Noções básicas segurança cibernética

GUIA

Co-funded by the Erasmus+ Programme of the European Union

O manual é um dos resultados do projecto Erasmus+ 'Cybersecurity Fundamentals'.

Coordenador do projecto:

Prof. Edward Lipiński Academy of Applied Sciences in Kielce

Parceiros:

Ambis vysoká škola, Praga, República Checa

Instituto Politécnico de Beja, Portugal

Co-funded by the Erasmus+ Programme of the European Union

O que é esta publicação?

Este é um manual para o instrutor do curso/semestre utilizar a colecção de materiais em linha encontrados na plataforma Cybersecurity Fundamentals. O manual também será útil para os estudantes, especialmente para aqueles que estudam por conta própria.

Os materiais foram desenvolvidos como parte do projecto "Fundamentos da Cibersegurança", financiado por fundos da UE ao abrigo do programa Erasmus+, de 2019 a 2022. O projecto foi coordenado pelo Prof. Edward Lipinski Academy of Applied Sciences em Kielce, e os parceiros eram universidades da República Checa e de Portugal.

Os materiais em linha (conferências em vídeo, manuais escolares específicos, vídeos instrucionais) são concebidos para melhorar a compreensão do amplo contexto da segurança cibernética e desenvolver competências para lidar com diferentes tipos de ameaças. O conjunto pode ser adaptado a diferentes contextos educacionais, dependendo das necessidades.

A publicação fornece materiais detalhados e orientação para a realização de seminários de *aprendizagem mista* ou *em linha*.

A escolha e a ordem em que os tópicos são apresentados devem ser adaptados às necessidades do grupo específico de participantes e, por conseguinte, é da responsabilidade de cada turma ou líder do curso. Não há nenhuma exigência de conduzir todos os módulos ou de os conduzir exactamente na ordem sugerida neste recurso.

A quem se destina esta publicação?

Esta publicação é destinada a académicos e formadores em segurança de sistemas informáticos. Sugere-se uma abordagem flexível: o curso pode ser integrado nos currículos existentes ou oferecido como um curso de formação autónomo. Embora o material se destine ao sector do ensino superior, também será útil para os formadores de pessoas que trabalham. Geograficamente, o contexto imediato do recurso são as audiências nos países parceiros, mas devido à abordagem transnacional e à natureza das questões apresentadas, o material é facilmente adaptável às necessidades dos educadores de outros países.

Quais são os objectivos desta publicação?

Os principais beneficiários do projecto "Fundamentos de Segurança Cibernética" são estudantes de várias faculdades, pois hoje em dia é difícil encontrar um campo de vida em que a ameaça de ataques aos sistemas informáticos não seja um problema. O curso é recomendado especialmente para estudantes de áreas principais como a segurança interna, pois os ataques cibernéticos a várias instituições são hoje incomparavelmente mais frequentes (e mais lucrativos) do que os ataques físicos. O objectivo desta publicação é ajudar o líder do curso/classe a seleccionar, entre os numerosos materiais em linha propostos, aqueles que são úteis para o seu grupo de estudantes e a conduzir actividades de *aprendizagem mista* (actividades em sala de aula e trabalho em linha independente do estudante) ou completamente *em linha.* No caso de *aprendizagem mista,* é aconselhável utilizar o método de *sala de aula folheada* onde os alunos vêm à aula depois de terem lido o material em linha pré-definido.

Abordagem pedagógica

"O conhecimento é criado pelos estudantes".

O curso adopta a abordagem de Kolb (1984) à aprendizagem experimental. De acordo com Kolb's Cycle, repete-se um ciclo de quatro etapas no processo de aprendizagem: experiência, reflexão, generalização e aplicação.

A formação de profissionais de cibersegurança baseia-se excepcionalmente na aprendizagem experiencial - experimentando tarefas cada vez mais difíceis ao mesmo tempo que desenvolve conhecimentos e competências.

Em todas as actividades propostas para utilização na sala de aula, tentamos mostrar a relação do tópico em discussão com a prática diária de trabalho dos participantes no curso, a fim de, de acordo com os princípios do Design Centrado no Homem, lhes proporcionar uma experiência de formação envolvente.

Notas para o formador

As notas do instrutor baseiam-se no conteúdo dos módulos em linha e seguem a ordem dos módulos na plataforma. Espera-se que cada sessão dure aproximadamente duas horas de aula. Uma descrição da carga horária é incluída no programa de cada módulo. As sessões podem também ser prolongadas ou encurtadas com alterações apropriadas nos materiais e tópicos.

Equipamento e materiais

O equipamento e materiais necessários para cada oficina estão geralmente disponíveis no sector do ensino superior. Estes incluem uma sala de informática adequada para trabalhos de grupo interactivos, projector, ecrã, acesso à Internet, colunas, flipchart, canetas, etc.

Utilização do curso

Ir para: https://moodle.cybersecurity-fundamentals.eu/

Seleccione a língua e o módulo do curso.

Seleccionar um estado (possível para entrar como 'Convidado', mas isto restringirá o acesso a algum material e funcionalidade). É possível criar uma conta você mesmo e iniciar sessão com uma conta Google ou Microsoft.

Este manual do professor diz respeito à versão polaca.

Os materiais do curso podem ser utilizados sequencialmente ou selectivamente, conforme as necessidades.

Informação para universidades

Qualquer universidade pode facilmente alojar o curso no seu servidor e utilizá-lo para educar os seus alunos. O LMS do curso é o Moodle, uma popular plataforma de e-learning de código aberto gratuita. O curso é também gratuito.

As universidades interessadas estão convidadas a contactar-nos em: erasmus@wsepinm.edu.pl . Aqueles que o desejarem receberão um curso embalado que poderão realizar no seu próprio servidor dentro de minutos. Isto aplica-se não só ao polaco, mas também às versões em inglês, checo e português. Gostaríamos particularmente de chamar a vossa atenção para a possibilidade de utilizar a versão inglesa do curso para ensinar nesta língua, que é difícil de navegar no ciberespaço, quanto mais não seja devido à prevalência da terminologia inglesa.

Conteúdo do curso

O conteúdo pedagógico do curso está organizado nos seguintes módulos:

Introdução

Módulo 1: Fundamentos de Redes de Computadores

Módulo 2: Lei e outros regulamentos

Módulo 3: Detectar e prevenir as ameaças cibernéticas

Módulo 4: CSIRT e CERT

Módulo 5: Fundamentos da perícia informática

Módulo 6: Segurança abrangente da rede

Módulo 1

Noções básicas de redes informáticas

1. Introdução

1.1 Resumo do módulo

O módulo centra-se nos conceitos básicos das redes informáticas (por exemplo, protocolos, endereços, topologias, etc.) e destina-se àqueles que não tiveram qualquer exposição prévia ao tema das redes informáticas. Os estudantes de ciências informáticas poderão provavelmente saltar este módulo.

1.2 Objectivos do curso

O módulo visa introduzir os conceitos básicos dos fundamentos da rede. Destina-se àqueles que ainda não foram expostos aos tópicos de configuração de rede, protocolos, topologia de rede, etc.

Ao concluir o curso no método de aprendizagem combinada, o aluno deve ter adquirido a capacidade de criar uma rede local simples, ligá-la à Internet, testar o desempenho da rede, resolver problemas de falhas.

O conhecimento adquirido desta forma é necessário para compreender o que é a Internet e os perigos de apenas estar ligado à rede.

1.3 Conteúdo do curso

As aulas individuais introduzem os alunos na camada física e na camada lógica da rede. Os alunos são introduzidos aos conceitos de protocolos, pacotes de dados, endereços físicos e lógicos e serviços básicos de rede.

1.4 Objectivos de aprendizagem

- Ganhar conhecimentos básicos de redes informáticas, infra-estruturas de rede.
- Familiarização com LAN, MAN, arquitectura de rede WAN.
- Familiarização com o modelo ISO/OSI de 7 camadas
- Familiarização com o modelo de valor da rede TCP/IP. Conhecimento das noções básicas dos protocolos TCP e UDP.
- Conhecimento das noções básicas da comunicação VoIP.
- Compreender a questão do desempenho da rede. Familiarização com os métodos de redução do tráfego na rede.
- Utilização de computadores, ferramentas digitais e redes informáticas, incluindo o conhecimento dos princípios dos dispositivos digitais e das redes informáticas e a realização de testes básicos de redes informáticas.

1.5 Programa de estudos

Efeito de aprendizagem	Estudantes que tenham passado no assunto sabe/conhece/cana:
NOVIDADES	
W1	Caracteriza os serviços de rede/servidor
W2	Tem um conhecimento amplo e estruturado dos serviços e aplicações utilizados nas redes informáticas. Está familiarizado com os sistemas operativos de rede
W3	Tem conhecimentos de configuração de equipamento de rede
W4	Tem conhecimentos sobre os riscos nas redes informáticas. Compreende a importância e o papel de protocolos de rede seleccionados com atribuição a camadas específicas de modelos de referência
W5	Tem conhecimentos de concepção de redes informáticas e dos seus componentes
W6	Descreve e analisa classes de endereços IP
W7	Pode nomear as camadas ISO/OSI
W8	Reconhece topologias de redes locais
W9	Conhece os endereços das portas TCP/UDP
W10	Conhece os conceitos relacionados com: administração e gestão de redes informáticas
W11	Conhece os princípios do equipamento de rede
HABILIDADES	
U1	Descreve e analisa classes de endereços IP
U2	Liga a rede informática local à Internet
U3	Ser capaz de analisar o tráfego nas redes informáticas. Ser capaz de configurar o endereçamento em rede e elementos de segurança seleccionados.
U4	Capaz de configurar dispositivos básicos de rede. Conhece e pode utilizar uma ferramenta de simulação na análise e concepção de redes informáticas.
U5	Capaz de configurar servidores de serviços web
U6	Ser capaz de configurar uma estação de trabalho para trabalhar em rede
U7	Pode verificar o desempenho da rede
U8	Ser capaz de conceber uma rede de área local
U9	Ser capaz de construir uma rede local simples utilizando equipamento de rede real. Ser capaz de preparar independentemente a cablagem estruturada.
U10	Capaz de gerir remotamente os postos de trabalho na rede
U11	Desenha a estrutura de endereços IP na rede
U12	Reconhece e aplica normas para a cablagem estruturada
U13	Reconhece protocolos de rede local e protocolos de acesso à rede de área ampla
U14	Reconhece os dispositivos de rede (descrição, símbolo, aparência)
U15	Efectua medições e testes da rede lógica
COMPETÊNCIAS SOCIAIS	
K1	Descreve a configuração das interfaces de rede
K2	Ser capaz de identificar as prioridades de acção
K3	Capaz de trabalhar e interagir num grupo no que diz respeito à configuração de endereçamento e serviços de rede seleccionados.
K4	Capaz de trabalhar em equipa, resolver tarefas em conjunto
K5	Explica os princípios dos protocolos de redes informáticas

Conteúdo do módulo (programa de palestras e outras actividades)		Referência aos resultados da aprendizagem
LECTURAS 1. Estrutura física da rede, tipos de equipamento de rede, cabos 2. Unidades de dados em redes 3. Estrutura de rede lógica, topologias 4. Modelos ISO/OSI, TCP/IP 5. Discussão sobre a utilização de camadas WORKSHOPS 1. Criação de uma rede física 2. Configuração de rede 3. Inquérito de rede 4. Ligação em rede à Internet		W 1-11 U1-15 K1-5
Saldo de crédito ECTS		
Forma de carga de trabalho dos estudantes		Número de horas
Número de horas com participação directa do professor académico		
1.1	Participação em conferências	6
1.2	Participação em seminários	
1.3	Participação em workshops	30
1.4	Participação em actividades laboratoriais	
1.5	Participação em projectos	
1.6	Participação em consultas (2-3 vezes por semestre)	
1.7	Participação na consulta do projecto	
1.8	Participação em exames/teste	2
1.9	Outros ...	
1.10	**Número de horas passadas com assistência directa de pessoal académico (soma 1.1 - 1.9)**	38
1.11	**Número de créditos ECTS obtidos pelo aluno em aulas que requerem a participação directa de um professor académico)**	1,5
Trabalho individual do estudante		
2.1	Estudos individuais (incluindo palestras de e-learning)	10
2.2	Preparação individual para workshops	10
2.3	Preparação do teste individual	
2.4	Preparação individual para aulas de laboratório	
2.5	Elaboração de relatórios	
2.6	Implementação de tarefas auto-realizadas (projectos, documentação)	
2.7	Preparação para o exame/teste final do seminário	10
2.8	Preparação para exame/teste final de conferências	
2.9	Outros	
2.10	**Número de horas de trabalho individual (soma de 2,1 - 2,9)**	30
2.11	**Número de créditos ECTS obtidos pelo estudante em actividades individuais de aprendizagem**	1
Carga de trabalho total (h)		**68**
Créditos ECTS para o módulo		**2,5**

Métodos de verificação dos resultados da aprendizagem									
Resultado da aprendizagem	**Formas de avaliação**								
	Exame oral	Exame escrito	Trabalho escrito parcial	Trabalho final escrito (ensaio, etc.)	Teste	Projecto/apresentação	Relatório	Actividades de sala de aula	Outros ...
NOVIDADES									
W1-11					x			x	
HABILIDADES									
U1-15					x			x	
COMPETÊNCIAS									
K1-5								x	

Critérios para avaliar a competência dos estudantes
Os requisitos mínimos para os três grupos de resultados de aprendizagem que um estudante deve atingir a fim de passar na disciplina são resumidos abaixo. Para que um estudante passe num módulo, todos os resultados de aprendizagem descritos no programa devem ser verificados positivamente pela(s) pessoa(s) que ensina(m) o módulo.

W - CONHECIMENTO
Avaliação:
Satisfatório - O aluno lembra-se e reproduz os conhecimentos a dominar dentro do módulo.
Bom - O estudante interpreta adicionalmente fenómenos/problemas e é capaz de resolver um problema típico
Muito bom - O estudante é capaz de resolver problemas mesmo complexos num determinado campo, é capaz de sintetizar, realizar uma avaliação abrangente, criar um trabalho que é original e inspirador para outros.

U - HABILIDADES
Avaliação:
Satisfatório - O aluno conhece a natureza das actividades e é capaz, sob a orientação do professor académico, de realizar actividades / resolver problemas relacionados com o conteúdo do módulo
Bom - O estudante é capaz de realizar actividades / tarefas / resolver problemas típicos relacionados com o conteúdo do módulo
Muito bom - O aluno dominou totalmente a capacidade / habilidade para realizar as actividades / tarefas / problemas previstos no conteúdo do módulo, também em casos mais complexos.

K - COMPETÊNCIA SOCIAL
Avaliação:
Satisfatório - O aluno assimila passivamente o conteúdo do módulo, demonstrando capacidade de concentração e escuta
Bom - O estudante participa activamente nas aulas, faz juízos de valor de acordo com os critérios aceites no domínio em questão, pode cooperar activamente num grupo
Muito bom - O estudante integra a atitude de acordo com o modelo proposto, desenvolve o seu próprio sistema de valores profissionais e sociais, é capaz de assumir a responsabilidade pelas acções do grupo, incluindo a liderança.

2. Material básico para o professor

Definições (glossário)

Rede informática - Uma colecção de dispositivos, tais como computadores, impressoras, telefones e televisores, que estão interligados para o intercâmbio de dados. Um meio de transmissão é utilizado para ligar os dispositivos e um protocolo de comunicação é utilizado para transmitir dados.

Endereço IPv4 - Este é um número de 32 bits, introduzido em forma decimal para facilidade de utilização (por exemplo 192.168.31.190), para identificar dispositivos e dados de endereço
na rede.

HOST - Este é um dispositivo com um endereço IP que é a fonte ou o destinatário dos dados transmitidos através da rede, ou seja, recebe dados de outros dispositivos ou envia tais dados. O termo hospedeiro é por vezes utilizado indistintamente com o termo dispositivo terminal, uma vez que normalmente se refere a um computador, tablet ou smartphone, ou seja, um dispositivo com o qual o utilizador da rede tem contacto directo.

Cliente - O dispositivo, ou mais precisamente o seu software, utiliza os serviços fornecidos pelo servidor. O cliente mais comum hoje em dia é o navegador web, que permite visualizar o conteúdo de páginas web alojadas por um servidor web. Exemplos de um cliente incluem também o FileZilla, que permite a troca de ficheiros através da Internet, e todo o tipo de software de correio electrónico para facilitar a utilização do correio. Consolas de jogos ou smartphones serão também clientes, desde que estejam ligados à Internet, é claro.

Servidor - Este é um computador com software especializado dedicado instalado para servir outros computadores. O serviço que um servidor pode fornecer é, por exemplo, um website, e-mail ou recurso de arquivo. Um servidor pode ser qualquer computador em que tal software esteja instalado e configurado, tal como APACHE, que é utilizado para manter e partilhar sítios web, ou MySQL, que é um sistema de gestão de bases de dados. Um servidor é normalmente um computador dedicado com elevado poder informático, capaz de lidar com múltiplas ligações e consultas em simultâneo.

Meio de transmissão - Por outras palavras, o meio que é o elemento de rede através do qual os dispositivos comunicam uns com os outros e trocam dados. Este meio pode ser cabo de cobre, cabo de fibra óptica e ondas de rádio (WiFi).

Protocolo de comunicação - Este é o método ou linguagem de comunicação e intercâmbio de dados entre dispositivos que define as regras e princípios dessa comunicação.

Internet - É um conjunto de redes de área ampla interligadas que formam uma rede informática global. As origens da Internet podem ser traçadas desde a criação da rede ARPANET no final da década de 1960, e a primeira ligação à Internet na Polónia foi lançada em Setembro de 1990. A Internet é vista por muitos como uma colecção de sites para navegar, mas não é o caso, uma vez que a Internet é uma colecção de muitas redes alargadas espalhadas por todo o mundo e os sites são serviços de rede específicos.

Intranet - Esta é uma rede interna privada que utiliza exactamente as mesmas normas de comunicação (protocolos) que a Internet, mas só tem acesso a utilizadores autorizados, tais como empregados de uma determinada empresa. Na maioria dos casos, o acesso a uma intranet, ou a esta rede interna da empresa, é através de um website, pelo que se diz que a comunicação utiliza as mesmas normas que a Internet.

Extranet - é uma extensa variedade de intranets que permitem o acesso aos seus recursos não só aos empregados de uma dada empresa, mas também a outros utilizadores.

DNS (Domain Name System) - Um serviço de rede cuja tarefa consiste em mudar um nome legível por humanos, o chamado nome mnemónico, para o endereço IP de um dispositivo na rede. É um serviço básico da Internet, alterando os endereços de websites para os endereços IP correspondentes dos servidores onde estes websites são armazenados, por exemplo, alterando o endereço Internet onet.pl para o endereço IP 214.180.141.140.

DHCP (Dynamic Host Configuration Protocol) é um protocolo de configuração automática que atribui um endereço IP, máscara de sub-rede ou endereço de gateway padrão a um anfitrião. É o método mais comum de atribuição de endereços IP a computadores numa rede, uma vez que não requer configuração manual de endereços IP em cada computador.

3. Durante as aulas

<u>Algumas ideias para actividades:</u>

WORKSHOPS

Com os estudantes, criar uma rede local no estúdio e ligá-la à Internet.

Juntamente com os estudantes, instalar uma ficha RJ45 no cabo UTP e verificar o desempenho do cabo.

PERGUNTAS DE REVISÃO

- Que protocolos são utilizados para o correio electrónico e quais para os sítios Web?

- Nomear as 7 camadas do modelo ISO/OSI?

- O que é um endereço MAC e o que é um endereço IP?

- O que significam os termos encapsulamento e decapsulamento?

- Como é que o IPv4 difere do IPv6?

- Quais são as principais vantagens e desvantagens das fibras ópticas em comparação com os cabos de par trançado?

TRABALHAR EM PARES/GRUPOS

Cenário 'telefone surdo' em diferentes configurações de rede:

1. dividir-se em grupos: Dividir os participantes em grupos, cada grupo deve ser composto por pelo menos três pessoas.

2. configuração linear: Na primeira configuração, a rede deve ser montada de forma linear. A primeira pessoa no grupo vem com uma frase curta e depois passa-a à pessoa seguinte através de um "telefone estúpido". A última pessoa do grupo passa a frase em voz alta. Comparar a frase recebida com a original e discutir com os participantes como é que a mensagem mudou.

3. Configuração em estrela: Na segunda configuração, a rede deve ser configurada de forma a ser uma estrela. Escolher uma pessoa para ser o início da entrega da frase. Esta pessoa passa a frase para uma pessoa, que a
passa para a pessoa seguinte e assim sucessivamente até que todas as pessoas do grupo tenham ouvido a frase. Comparar a frase recebida com a frase original e discutir com os participantes como é que a mensagem mudou.

4 Configuração da grelha: Na terceira configuração, a grelha deve ser estabelecida em forma de grelha. Cada pessoa do grupo deve ter dois vizinhos e passar a sentença a um deles. Ver como a frase muda à medida que passa por pessoas diferentes e discuti-la com os participantes.

Após cada configuração da grelha, discutir com os participantes que lições podem ser aprendidas com este exercício no contexto da topologia da rede informática. Exemplos de perguntas a fazer são:

- Como é que as diferentes configurações de rede afectam a qualidade da transmissão de informação?
- Que problemas podem ocorrer com diferentes configurações de rede?
- Quais são as vantagens e desvantagens das diferentes topologias de rede no contexto da transferência de informação?

TÓPICOS PARA DISCUSSÃO
- A quem pertence a Internet, quem a controla?
- Quais são os riscos de acesso aberto à web?
- Deve haver mais controlo sobre o conteúdo que aparece na Internet? Quem o deveria fazer?
- Que outras redes para além das redes informáticas podem ser reconhecidas? Como é que a abordagem à privacidade muda dependendo da dimensão da rede e de outros factores?
- Pode um restaurante ser um exemplo de uma cadeia? Quais são os papéis dos clientes, garçons, cozinheiros? Como é que são os protocolos e pacotes de dados?

4. Recursos da Internet

https://learn.microsoft.com/pl-pl/training/modules/network-fundamentals/
https://www.icann.org/
https://isportal.pl/
https://www.speedtest.net/
https://www.intgovforum.org/
https://www.whatismyisp.com/
https://uke.gov.pl/

5. Perguntas/testões adicionais

O que é que significa VoIP?
A. Voz no Protocolo Internet
B. Vício sobre Protocolo Internet
C. Posição da voz através da Internet
D. Voz sobre Protocolo Internet
RESPONSABILIDADE: D

O primeiro cibercriminoso 'técnico' foi Leonard Kleinrock, que em 1973 enviou uma mensagem através da ARPANET a respeito:
A. A sua máquina de barbear eléctrica desaparecida.
B. As suas namoradas
C. o livro de texto desejado
D. canções
RESPONSABILIDADE: A

Qual é o nome do programa que funciona como uma central telefónica?
A. IP-PBX
B. CVoIP
C. Skype
D. Equipas MS
RESPONSABILIDADE: A

Qual dos seguintes programas não utiliza a tecnologia VoIP?
A. Equipas de EM
B. Zoom
C. Google Meet
D. Photoshop
RESPONSABILIDADE: D

O que é o programa Asterix?
A. Servidor SIP
B. Servidor de ficheiros
C. servidor de fotografia
D. compressor de ficheiros
RESPONSABILIDADE: A

Qual dos seguintes aspectos não afecta o desempenho da rede informática?
A. Partes passivas de uma rede informática
B. Dispositivos activos
C. Interferência electromagnética
D. pressão atmosférica
RESPONSABILIDADE: D

De que material é feito o cabo de par trançado?
A. Cobre
B. Alumínio
C. aço
D. Fibra de vidro
RESPONSABILIDADE: A

O cabo de rede de par trançado de categoria 5 permite a transmissão até um máximo de:
A. 1 Gbps
B. 100 Mbps
C. 1 Mbps
D. 10 Gbps
RESPONSABILIDADE: A

Que meio transporta dados a uma maior distância?
A. Fibra óptica
B. Cabo de cobre (par torcido)
C. cabo de aço
D. cabo de alumínio
RESPONSABILIDADE: A
O que é um HOST numa rede informática?
A. Qualquer dispositivo ligado à rede
B. Anfitrião
C. um dispositivo central numa rede informática
D. drive externo
RESPONSABILIDADE: A

O que é um cartão de rede?
A. um dispositivo que permite a ligação de um anfitrião a uma rede informática
B. Parte do processador principal
C. dispositivo de fornecimento de energia
D. SSD
RESPONSABILIDADE: A

Que programa pode ser utilizado para medir a velocidade de descarga numa rede informática?
A. wget
B. ping
C. Equipas MS
D.
RESPONSABILIDADE: A

O endereço web através do qual pode verificar o desempenho da sua rede é:
A. teste de velocidade.net
B. google.com
C. yahoo.com
D. google.net
RESPONSABILIDADE: A

Um router de rede doméstica pode ser utilizado:
A. Restrições ao tráfego na rede
B. Procura de informação
C. vigilância por vídeo
D. playback mp3
RESPONSABILIDADE: A

Ao digitar "CMD" no MS Windows 10/11 na janela de pesquisa, vamos correr:
A. Linha de comando
B. Configuração do cartão de rede
C. Calculadora
D. Programa de compressão de ficheiros
RESPONSABILIDADE: A

Para que é utilizado o programa de ping?
A. indica o tempo de resposta ao pacote enviado
B. Altera a hora do sistema
C. apresenta o manual de ajuda
D. Encerrar todos os programas
RESPONSABILIDADE: A

Que programa devolve uma lista de routers consecutivos ao longo do percurso até ao computador de destino na rede?
A. Tracert
B. wget
C. ping
D. span
RESPONSABILIDADE: A

Módulo 2

Direito e outros regulamentos

3. Introdução

1.5 Resumo do curso

O curso foca conceitos legais básicos relacionados com a Internet e introduz o aluno ao tema da responsabilidade no ciberespaço. O conhecimento dos fundamentos legais de um Provedor de Serviços Internet (ISP) é também necessário para compreender o assunto na sua totalidade. Uma parte significativa do curso abrange a segurança cibernética e a legislação correspondente. Além disso, a protecção de dados pessoais no ciberespaço não pode ser negligenciada. A privacidade e segurança nas TIC e a protecção de dados no ciberespaço são também tópicos chave que constituem uma parte essencial do curso.

1.2 Objectivos do curso

Os estudantes aprenderão sobre a relação entre o direito e o ciberespaço. Estarão familiarizados com a base jurídica dos Provedores de Serviços Internet (ISPs). Para os seus estudos, concentrar-se-ão adicionalmente na segurança cibernética e na sua regulamentação. Para além disso, os estudantes estudarão o sistema de gestão da segurança da informação. Finalmente, descobrirão a importância da protecção de dados no ciberespaço.

O objectivo do módulo é familiarizar os estudantes com a aplicação da lei no domínio das tecnologias da informação e da comunicação. Um objectivo adicional é a identificação dos limites legais da segurança cibernética.

Após a conclusão do curso, o aluno deverá ter adquirido a capacidade de se orientar nas normas legais da União Europeia e dos países participantes que estejam directamente relacionadas com a questão da segurança cibernética.
Além disso, o estudante terá uma visão geral básica das questões de direito civil e público que são utilizadas no ciberespaço, com particular ênfase na aplicação prática dos conhecimentos adquiridos. O estudante não só será introduzido à teoria da aplicação do direito no ciberespaço e ao regulamento de lege lata, mas também à aplicação prática do direito na prática (de lege aplicata).

Os conhecimentos adquiridos serão ainda aplicados em módulos sobre ataques cibernéticos e como se defender contra eles, bem como num módulo sobre a construção e operação de equipas de segurança.

1.3 Conteúdo do curso

As aulas individuais introduzem os estudantes no sistema jurídico em questão, na norma jurídica, na lei e na Internet. Além disso, os estudantes são introduzidos à responsabilidade no ciberespaço e à base legal dos Provedores de Serviços de Internet (ISPs). Um dos tópicos chave é a segurança cibernética e a sua regulamentação legal. A privacidade e a segurança relacionada nas TIC, a protecção de dados no ciberespaço são também extremamente importantes e por isso a última parte das aulas é-lhes dedicada.

1.4 Objectivos de aprendizagem

1) Introdução ao tema do sistema jurídico, da norma jurídica, da lei e da Internet
2) Responsabilidade no ciberespaço
3) Compreender a base jurídica do negócio do ISP (Internet Service Provider)
4) Protecção de dados pessoais no ciberespaço
5) Privacidade e segurança nas TIC, protecção de dados no ciberespaço

3.5 Equipamento e materiais necessários

Leis e regulamentos sobre segurança cibernética - disponíveis online

Direito primário da UE

- Carta dos Direitos Fundamentais da União Europeia

Directivas do Parlamento Europeu e do Conselho

- 91/250/CEE sobre a protecção jurídica dos programas de computador
- 98/34/CE relativa a um procedimento de informação no domínio das normas e regulamentações técnicas, com a redacção que lhe foi dada pela Directiva 98/48/CE
- 1999/5/CE relativa aos equipamentos de rádio e equipamentos terminais de telecomunicações e ao reconhecimento mútuo da sua conformidade
- 2000/31/CE relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno (Directiva sobre o comércio electrónico)
- 2002/19/CE relativa ao acesso e interligação de redes de comunicações electrónicas e recursos conexos (Directiva Acesso)
- 2002/20/CE relativa à autorização de redes e serviços de comunicações electrónicas (Directiva Autorização), com a redacção que lhe foi dada pela Directiva 2009/140/CE
- 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (directiva-quadro), com a redacção que lhe foi dada pela Directiva 2009/140/CE
- 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (Directiva Serviço Universal)
- 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas
- 2006/24/CE relativa à conservação de dados gerados ou tratados no contexto da prestação de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações
- 2008/114/CE sobre a identificação e designação das infra-estruturas críticas europeias e a avaliação da necessidade de melhorar a sua protecção
- 2011/93/UE relativa à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil, em substituição da Decisão-Quadro 2004/68/JAI do Conselho
- 2013/11/UE relativa aos modos alternativos de resolução de litígios em matéria de consumo e que altera o Regulamento (CE) n.º 2006/2004 e a Directiva 2009/22/CE (Directiva relativa aos modos alternativos de resolução de litígios em matéria de consumo)
- 2013/40/EU sobre ataques contra os sistemas de informação e em substituição da Decisão-Quadro 2005/222/JAI do Conselho
- 2015/1535 sobre o procedimento para o fornecimento de informações no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação
- 2015/2366 relativa aos serviços de pagamento no mercado interno, que altera as Directivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010 e revoga a Directiva 2007/64/CE ("Directiva revista relativa aos serviços de pagamento")
- 2016/680 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou

repressão de infracções penais ou de execução de sanções penais, à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho

- 2016/1148 sobre medidas para um elevado nível comum de segurança das redes e sistemas de informação na União Europeia (NIS)

Regulamentos do Parlamento Europeu e do Conselho

- 460/2004/CE que cria a Agência Europeia para a Segurança das Redes e da Informação, com a redacção que lhe foi dada pelo Regulamento n.º 1007/2008
- 1077/2011/CE que cria uma Agência Europeia para a gestão operacional de sistemas informáticos de grande escala no domínio da liberdade, segurança e justiça
- 526/2013 sobre a Agência Europeia para a Segurança das Redes e da Informação (**ENISA)** e que revoga o Regulamento (CE) n.º 460/2004 Texto relevante para efeitos do EEE
- 910/2014 sobre serviços de identificação electrónica e de confiança para transacções electrónicas no mercado interno e que revoga a Directiva 1999/93/CE (**eIDAS)**[1]
- 679/2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados - **GDPR**)

Decisões do Conselho da Europa

- 92/242/CEE no domínio da segurança dos sistemas de informação
- **2005/222/JAI sobre ataques contra os sistemas de informação**
- 2011/292/UE sobre as regras de segurança para a protecção da informação classificada da UE

Outros documentos

- Convenção 185 do Conselho da Europa sobre Cibercriminalidade
- Conselho da Europa Protocolo Adicional 189 à Convenção sobre a Cibercriminalidade
- Convenção 196 do Conselho da Europa para a Prevenção do Terrorismo
- Regulamento de execução (UE) 2018/151 da Comissão que estabelece as regras de aplicação da Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho no que respeita a uma maior clarificação dos elementos que os fornecedores de serviços digitais devem ter em conta na gestão dos riscos para a segurança das redes e sistemas de informação, bem como os parâmetros para determinar se um incidente tem um impacto significativo

Normas internacionais

- ISMS série ISO/IEC 27000

Outros

- Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao mercado único digital dos serviços (Lei dos Serviços Digitais) e que altera a Directiva 2000/31/CE
- Responsabilidade privada e pública por acções de utilizadores ou empresas no ambiente online
- Características e definição dos diferentes FSI e dos seus direitos e obrigações em matéria de segurança cibernética
- O ISMS e a relação com a lei de segurança cibernética

1.6 Programa de estudos

[1] A seguir referido como "**eIDAS".**

Resultado da aprendizagem	O aluno que completar o módulo com sucesso saberá/ será competente no seguinte.
NOVIDADES	
W1	O estudante adquirirá conhecimentos profissionais e alargará a sua consciência legal das tecnologias de informação e comunicação.
W2	O estudante irá adquirir conhecimentos profissionais relacionados com a definição legal de segurança cibernética de acordo com o direito internacional (em particular o direito da UE) e o direito nacional dos países participantes.
HABILIDADES	
U1	É capaz de identificar os diferentes FSI, os seus direitos e obrigações e, com base nesta identificação, é capaz de argumentar áreas do direito relacionadas com a segurança cibernética.
U2	Ser capaz de analisar o quadro básico dos bens no ciberespaço (por exemplo, tecnologias, processos, dados, etc.) e identificar recomendações legais para a sua protecção.
COMPETÊNCIAS	
K1	O estudante domina parcialmente as disposições legais, é capaz de aplicar os institutos jurídicos individuais aos estudos de caso.

Conteúdo do módulo (programa de palestras e outras actividades)	**Referência aos resultados da aprendizagem**
LECTURAS 1. Normas jurídicas internacionais que regem a cibercriminalidade 2. Normas jurídicas nacionais que regem a cibercriminalidade WORKSHOPS 1. Análise de ataques cibernéticos individuais e sua subsunção nos termos das disposições da Convenção sobre o Cibercrime (TJCE nº 185) e do direito nacional (República Checa, Polónia, Portugal)	W1, W2 U1, U2, K1

Saldo de crédito ECTS		
Forma de carga de trabalho dos estudantes		Número de horas
Número de horas com participação directa do professor académico		
1.1	Participação em conferências	6
1.2	Participação em seminários	
1.3	Participação em workshops	14
1.4	Participação em actividades laboratoriais	
1.5	Participação em projectos	
1.6	Participação em consultas (2-3 vezes por semestre)	
1.7	Participação na consulta do projecto	
1.8	Participação em exames/teste	2
1.9	Outros ...	
1.10	**Número de horas passadas com assistência directa de pessoal académico (soma 1.1 - 1.9)**	22
1.11	**Número de créditos ECTS obtidos pelo aluno em aulas que requerem a participação directa de um professor académico)**	1
Trabalho individual do estudante		

2.1	Estudos individuais (incluindo palestras de e-learning)	25
2.2	Preparação individual para workshops	10
2.3	Preparação do teste individual	
2.4	Preparação individual para aulas de laboratório	
2.5	Elaboração de relatórios	
2.6	Implementação de tarefas auto-realizadas (projectos, documentação)	
2.7	Preparação para o exame/teste final do seminário	5
2.8	Preparação para exame/teste final de conferências	5
2.9	Outros	
2.10	**Número de horas de trabalho individual (soma de 2,1 - 2,9)**	45
2.11	**Número de créditos ECTS obtidos pelo estudante em actividades individuais de aprendizagem**	1,5
Carga de trabalho total (h)		**67**
Créditos ECTS para o módulo		**2,5**

Métodos de verificação dos resultados da aprendizagem

Resultado da aprendizagem	**Formas de classes de crédito**								
	Exame oral	Exame escrito	Trabalho escrito parcial	Trabalho final escrito (ensaio, etc.)	Teste	Desenho/apresentação	Relatório	Actividades de sala de aula	Outros ...
NOVIDADES									
W1		x	x		x			x	
W2		x	x		x			x	
HABILIDADES									
U1						x			
U2						x			
COMPETÊNCIAS									
K1								x	

Critérios para avaliar a competência dos estudantes
Os requisitos mínimos para os três grupos de resultados de aprendizagem que o Estudante deve atingir a fim de passar na disciplina são apresentados abaixo de forma sintética. Para que um Estudante passe num módulo, todos os resultados de aprendizagem descritos no programa devem ser verificados positivamente pela(s) pessoa(s) que ensina(m) o módulo.

W - CONHECIMENTO
Avaliação:
Satisfatório - O aluno lembra-se e reproduz os conhecimentos a dominar dentro do módulo.
Bom - O estudante interpreta adicionalmente fenómenos/problemas e é capaz de resolver um problema típico
Muito bom - O estudante é capaz de resolver problemas mesmo complexos num determinado campo, é capaz de sintetizar, realizar uma avaliação abrangente, criar um trabalho que é original e inspirador para outros.

U - HABILIDADES
Avaliação:
Satisfatório - O aluno conhece a natureza das actividades e é capaz, sob a orientação do professor

académico, de realizar actividades / resolver problemas relacionados com o conteúdo do módulo
Bom - O estudante é capaz de realizar actividades / tarefas / resolver problemas típicos relacionados com o conteúdo do módulo
Muito bom - O aluno dominou totalmente a capacidade / habilidade para realizar as actividades / tarefas / problemas previstos no conteúdo do módulo, também em casos mais complexos.

K - COMPETÊNCIA SOCIAL
Avaliação:
Satisfatório - O aluno assimila passivamente o conteúdo do módulo, demonstrando capacidade de concentração e escuta
Bom - O estudante participa activamente nas aulas, faz juízos de valor de acordo com os critérios aceites no domínio em questão, pode cooperar activamente num grupo
Muito bom - O estudante integra a atitude de acordo com o modelo proposto, desenvolve o seu próprio sistema de valores profissionais e sociais, é capaz de assumir a responsabilidade pelas acções do grupo, incluindo a liderança.

Forma de carga de trabalho dos estudantes		Número de horas
Número de horas com participação directa do professor académico		
1.1	Participação em conferências	6
1.2	Participação em seminários	
1.3	Participação em workshops	14
1.4	Participação em actividades laboratoriais	
1.5	Participação em projectos	
1.6	Participação em consultas (2-3 vezes por semestre)	
1.7	Participação na consulta do projecto	
1.8	Participação em exames/teste	2
1.9	Outros ...	
1.10	**Número de horas passadas com assistência directa de pessoal académico (soma 1.1 - 1.9)**	22
1.11	**Número de créditos ECTS obtidos pelo aluno em aulas que requerem a participação directa de um professor académico)**	1

Trabalho individual do estudante		
2.1	Estudos individuais (incluindo palestras de e-learning)	25
2.2	Preparação individual para workshops	10
2.3	Preparação do teste individual	
2.4	Preparação individual para aulas de laboratório	
2.5	Elaboração de relatórios	
2.6	Implementação de tarefas auto-realizadas (projectos, documentação)	
2.7	Preparação para o exame/teste final do seminário	5
2.8	Preparação para exame/teste final de conferências	5
2.9	Outros	
2.10	**Número de horas de trabalho individual (soma de 2,1 - 2,9)**	45
2.11	**Número de créditos ECTS obtidos pelo estudante em actividades individuais de aprendizagem**	1,5
Carga de trabalho total (h)		**67**
Créditos ECTS para o módulo		**2,5**

2. Material básico para o professor

Definições (glossário)

Lei natural *(ius naturale)* - existe independentemente do Estado. Ela surge e desenvolve-se na sociedade. Geralmente engloba um conjunto de regras correspondentes ao nível alcançado de desenvolvimento da sociedade.
Lei positiva *(ius positivum)* - é legislada pelo Estado ou sistema de governo. A lei positiva é, portanto, pré-determinada. Consiste em regras previsíveis que são aplicadas, ou seja, cuja violação é punida.
Direito - (ou direito objectivo) - um conjunto de normas jurídicas como regras de conduta de aplicação geral estabelecidas ou reconhecidas e aplicadas pelo Estado.
Direito - a possibilidade de as entidades jurídicas se comportarem como garantidas por uma norma legal. Um direito corresponde normalmente a uma obrigação legal de outra entidade jurídica.
Estrutura da norma legal - consiste em três partes, que são a **hipótese, a disposição** e a **sanção**.
Norma legal dispositivo - não estabelece de todo uma regra básica de conduta, ou define-a apenas como uma possibilidade. Deixa a determinação das regras ao critério dos destinatários. Se os destinatários não o fizerem, as regras da norma servem de guia para que o juiz saiba como decidir.
Norma jurídica cognitiva - estabelece a regra de conduta aplicável. Não deixa espaço para a vontade do destinatário.
Normas de direitos - as normas legais formulam explicitamente apenas os direitos.
Normas vinculativas - as normas legais formulam expressamente uma obrigação, sob a forma de uma injunção ou proibição.
Normas públicas - as normas legais aplicam-se onde o poder público é exercido. O poder público é exercido pelo Estado através dos gabinetes do legislativo, do executivo e do judiciário. Vemos o direito público como um campo do direito onde as relações se baseiam na desigualdade das partes, em que uma das partes representa a autoridade pública actuando contra indivíduos privados através de ordens, proibições e execução.
Normas privadas - as normas jurídicas aplicam-se no domínio do direito privado, ou seja, quando os sujeitos estão em posição de igualdade e nenhum deles pode decidir com autoridade sobre os direitos e obrigações do outro. Os sujeitos regulam os seus direitos e obrigações mútuos através de contratos e acordos.
Normas internacionais - normas jurídicas regulam as relações entre os Estados ou os seus povos, possivelmente a nível da União Europeia.
Normas nacionais - as normas jurídicas regulam as relações entre actores dentro da jurisdição de um Estado ou normalmente dentro do seu território.
Direito substantivo - as normas jurídicas definem as relações jurídicas em geral e estabelecem os direitos e obrigações dos sujeitos.
Direito processual - normas legais regulam a conduta das autoridades públicas na aplicação das normas de direito substantivo, o que pode resultar na emissão de um acto público.

As normas jurídicas gerais aplicam-se a todo o território do Estado ou da União Europeia. Além disso, aplicam-se a todas as entidades sem qualquer limitação no seu âmbito temporal.
Normas específicas - as normas legais funcionam apenas num determinado território. Caso contrário - aplicam-se apenas a uma determinada categoria de sujeitos ou durante um determinado período de tempo.
Eficácia de uma norma jurídica - significa que os destinatários em causa têm direito aos direitos e obrigações dela decorrentes.
Ciberespaço - pode ser definido como o espaço das actividades cibernéticas ou como o espaço criado pelas tecnologias de informação e comunicação em que um mundo virtual (ou espaço) paralelo ao espaço real é criado.
Ciberespaço - um ambiente digital que permite a criação, processamento e troca de informação, constituído por sistemas de informação e serviços e redes de comunicações electrónicas.
Ciberespaço - pode ser definido pela acessibilidade e rastreabilidade dos dados para o utilizador médio.
Ciberespaço - é um espaço constituído por três camadas: física, lógica e social
Camada física - inclui o termo **componente geográfica** e o termo **elementos físicos de rede**.
Camada lógica - contém os **elementos lógicos da rede**, ou seja, as ligações lógicas entre os nós da rede. Estes são implementados utilizando protocolos de comunicação de rede. Os nós podem ser computadores, telefones e outros dispositivos de rede.
Camada social - consiste em componentes chamados '**cyberness**' e **personalidade**.
Definição de normas - são criadas e implementadas por quem tem autoridade para definir o ambiente da rede de informação. São, na prática, normas *sui generis* que definem as redes de informação como tal. Vêm em camadas que são interdependentes.
Definir as autoridades - são os criadores das normas definidoras. Esta é a entidade que, através das suas acções, cria as regras do sistema lógico em que o organismo opera
A Internet só existe por causa das autoridades que a definem. Ela consiste em. Nenhuma operação terá lugar sem a participação (execução ou mediação da execução da operação) da autoridade que a define.
Fornecedor de serviços - qualquer entidade pública ou privada **que forneça aos seus utilizadores de serviços a capacidade de comunicar através de um sistema informático**
Fornecedor de serviços - qualquer outra entidade que processe ou armazene dados informáticos em nome de um serviço de comunicação ou utilizadores de um tal serviço
Por **serviço da sociedade da informação** entende-se qualquer serviço prestado por via electrónica a pedido individual de um utilizador notificado por via electrónica, normalmente prestado contra remuneração. Um serviço é fornecido electronicamente se for transmitido através de uma rede de comunicações electrónicas e recuperado pelo utilizador a partir de dispositivos electrónicos de armazenamento de dados.

Serviço de comunicações electrónicas significa um serviço normalmente prestado mediante remuneração e que se baseia na transmissão (total ou principalmente) de sinais através de uma rede de comunicações electrónicas.
Serviço de comunicações electrónicas publicamente disponível - é um serviço de comunicações electrónicas que ninguém está excluído de utilizar à partida.
Um operador - que fornece ou está autorizado a fornecer uma rede pública de comunicações ou recursos associados é referido pela lei como **um operador.**
Assinante - é qualquer pessoa que tenha celebrado um contrato para a prestação de tal serviço com uma empresa que preste serviços de comunicações electrónicas publicamente disponíveis.
Utilizador - é qualquer pessoa que utilize ou solicite serviços de comunicação electrónica publicamente disponíveis.
Teste de proporcionalidade - é um instrumento jurídico padrão tanto dos tribunais internacionais como constitucionais (domésticos) ao avaliar a colisão de regras de direito para proteger um direito ou interesse público constitucionalmente garantido com outro direito ou liberdade fundamental.
O princípio da aptidão - (fitness for purpose), segundo o qual uma **medida deve ser capaz de atingir o seu objectivo,** que é o de proteger outro direito fundamental ou bem público.
Princípio da necessidade - prevê a **utilização apenas dos meios mais amigos do ambiente para atingir o objectivo pretendido** (interferência nos direitos e liberdades fundamentais) **entre vários meios possíveis.**
Princípio da proporcionalidade - (num sentido mais restrito) **visa** evitar **danos a um direito fundamental desproporcionados em relação ao objectivo prosseguido,** ou seja, as medidas restritivas dos direitos e liberdades fundamentais não devem, em caso de conflito entre um direito ou liberdade fundamental e o interesse público, superar, através das suas consequências negativas, os aspectos positivos de interesse público dessas medidas.
GDPR/RODO - Regulamento Geral de Protecção de Dados
Information Security Management System (**ISMS**)[2] - **é um conjunto de políticas** concebidas para manter a confidencialidade, integridade e disponibilidade da informação, aplicando um processo de gestão de riscos e assegurando às partes interessadas que os riscos estão a ser devidamente geridos.[3]
ISMS - faz parte e está integrado nos processos da organização e no sistema de gestão global.
Ciclo PDCA - significa Plan-Do-Check-Act.
Variante **OPDCA** - estende o modelo original para incluir **uma** fase de **Observação** que precede a fase do Plano.
Avaliação de riscos - refere-se ao **processo global de identificação, análise e avaliação de riscos.**
Política de segurança - é um conjunto de princípios e regras que definem a forma de assegurar a protecção dos bens**.**

[2] A seguir referido como **SGSI**
[3] Cf. introdução de ČSN ISO/IEC 27001

Matriz RACI (**RACI matrix) - um acrónimo para responsável, responsável, consultado, informado.**
Um agente de apoio é um agente técnico, empregados e fornecedores envolvidos na operação, desenvolvimento, administração ou segurança de um sistema TIC.
O bem subjacente é a informação ou serviço processado ou fornecido pelo sistema TIC.
BCM - representa a gestão da continuidade do negócio.
Instalações - é um edifício ou outro espaço fechado.
Permissão significa o direito de acesso a qualquer activo (geralmente um computador ou sistema de comunicação, aplicação, etc.) Na prática, é uma ferramenta para "gerir utilizadores e grupos" e uma ferramenta para definir permissões em ficheiros e directórios. Estas ferramentas são um componente proprietário de todos os sistemas operativos padrão.
Servidor **central AAA** - um acrónimo para Autenticação, Autorização, Contabilidade.
SIEM - abreviatura de Security Incident and Event Management (Gestão de Incidentes e Eventos de Segurança).
Criptografia (encriptação) - é a disciplina científica preocupada em transformar a informação inteligível numa forma ininteligível para o destinatário se este não tiver as chaves com as quais desencriptar a informação.
Regulamento GDPR - é um **quadro jurídico geral para a protecção de dados pessoais que** é válido e eficaz em toda a UE e, em alguns casos, para além dela.
Dados pessoais - é **qualquer informação relativa a uma pessoa singular identificada ou identificável**. Uma pessoa singular identificável é aquela que pode ser identificada, directa ou indirectamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador em linha ou a um ou mais factores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.
Os dados pessoais são **qualquer informação** (por exemplo, pictórica, escrita, verbal, digital, genética, médica, etc.) que **esteja ligada** (através do conteúdo - por exemplo, nome, morada, posição, e-mail, etc.) **a um sujeito dos** dados**.**[4]
"Critério objectivo" - significa que dados como **endereços IP podem ser considerados como dados pessoais** processados por fornecedores de serviços sem ligação (por exemplo, por um operador de website), **mesmo que apenas um terceiro seja capaz de identificar um utilizador específico** (tipicamente um ISP de ligação).
Critério "**relativo**" **-** significa que **os endereços IP podem ser considerados dados pessoais para uma ligação ISP**, uma vez que permitem ao ISP estabelecer a identidade do utilizador, **mas já não para sítios ISP, que na realidade só têm informação sobre endereços IP e não sabem o nome do visitante.**

[4]De acordo com o artigo 4 (1) GDPR, a **pessoa em causa** é uma **pessoa singular** identificada ou identificável, **podendo ser identificada uma pessoa em causa:**

- **directamente,**
- **indirectamente (por exemplo, destaque, etc.)**

Tratamento de dados pessoais - significa **uma operação ou conjunto de operações** que se realiza sobre **dados pessoais** ou conjuntos de dados pessoais**, seja ou não por meios automatizados,** tais como recolha, registo, organização, organização, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.
DPIA - significa avaliação do impacto da protecção de dados pessoais
DPIA - é um instrumento a ser utilizado quando um tipo específico de **processamento, em particular utilizando novas tecnologias, é susceptível, dada a** natureza, âmbito, contexto e objectivos do processamento, de dar origem a **um elevado risco para os direitos e liberdades das pessoas singulares.**
RIR - abreviatura de **Regional Internet** Registry.
LIR - abreviatura de **Local Internet** Registry.

Citações chave de material em linha:

- O direito é um dos instrumentos mais importantes para estabilizar as relações sociais e regular a sociedade
- A lei é uma das suas possíveis regulamentações sob a forma de construções normativas imperfeitas, onde, mais do que em qualquer outro lugar, existe uma regra geral de que não há sobreposição entre a conduta no mundo real, ou seja, o que é realmente implementado no ambiente online, e a conduta normativa, ou seja, o que deve ser (pela vontade do regulador e pela nossa). A realidade da Internet e a sua regulação normativa são, portanto, duas categorias relativamente separadas. Este pressuposto também não será posto em causa nesta publicação. Pelo contrário, será um dos seus pilares
- O verdadeiro conceito de direito é relativamente difícil de definir, pois é um fenómeno multidisciplinar e não pode ser definido por uma única definição:
- **A lei natural** *(ius naturale* existe independentemente do Estado. Ela surge e desenvolve-se na sociedade. Compreende geralmente um conjunto de regras correspondentes ao nível de desenvolvimento alcançado pela sociedade.
- **Lei positiva** *(ius positivum)*. Esta lei é promulgada pelo Estado ou sistema de governo. A lei positiva é, portanto, pré-determinada. Consiste em regras previsíveis que são aplicadas, ou seja, onde a infracção é punida.
- **A lei** (ou lei objectiva) é entendida como um conjunto de normas legais como regras de conduta de aplicação geral estabelecidas ou reconhecidas e aplicadas pelo Estado.
- **Direito -** é a possibilidade de as entidades jurídicas se comportarem como garantidas por uma norma legal. Um direito corresponde geralmente a uma obrigação legal de outro sujeito jurídico. A afirmação de um sujeito que "este é o meu direito" é legal neste sentido.
- **Uma norma legal** é uma regra de conduta geralmente aplicável que regula os direitos e obrigações dos sujeitos. Esta norma de conduta é expressa numa forma jurídica específica reconhecida pelo Estado (ou pela União Europeia) e a sua observância é assegurada pela execução pelo Estado.
- As normas legais podem ser divididas de acordo com vários critérios. Estes incluem, em particular:

  1. *A natureza das regras estabelecidas por uma norma legal.* Devido à natureza das regras, as normas legais dividem-se em:
  - Dispositivo. Uma norma jurídica dispositiva não estabelece uma regra básica de conduta ou apenas a estabelece como uma possibilidade. Deixa a determinação das regras ao critério dos destinatários. Se os destinatários não o fizerem, as regras contidas na norma servem de guia para

que o juiz saiba como decidir. As normas de dispositivos são mais frequentemente utilizadas em direito civil ou em relações de direito civil, o que permite uma maior variabilidade na resolução de diferentes situações (auto-regulação).

- Cogent (categórico). Uma norma jurídica convincente estabelece uma regra de conduta vinculativa. Não deixa espaço para a vontade do destinatário.

- O **ciberespaço** é:
    - espaço de acção cibernética, ou seja, o espaço criado pelas tecnologias de informação e comunicação em que é criado um mundo virtual (ou espaço) paralelo ao real.
    - o ambiente digital que permite a criação, processamento e troca de informação, constituído por sistemas de informação e serviços e redes de comunicação electrónica.
    - um espaço composto por três camadas: física, lógica e social.

- **As características do ciberespaço** são a sua **descentralização, globalização, abertura, riqueza de informação, interactividade** e a possibilidade de o utilizador influenciar opiniões. Um importante atributo do ciberespaço é que a tecnologia e serviços relacionados desempenham um papel fundamental no mesmo. Recentemente, tornou-se cada vez mais claro que as manifestações do mundo virtual podem ter e têm consequências no mundo real.
- Uma das definições mais eficazes de *ciberespaço* encontra-se em *Cyberspace Operations: Concept Capability Plan 2016-2028*, que define o **ciberespaço como um espaço composto por três camadas:** [5]
    - físico,
    - lógico,
    - Social.
- **O ciberespaço também pode ser definido de acordo com a acessibilidade e rastreabilidade dos dados para o utilizador médio.** De acordo com esta divisão, o ciberespaço pode ser dividido em serviços e dados acessíveis através da Internet, serviços e dados acessíveis apenas dentro de redes e dispositivos específicos, e serviços e dados deliberadamente escondidos e acessíveis com ferramentas especiais.

Os seguintes nomes são normalmente utilizados para estas categorias:

- Web de Superfície
- Web profunda
- Teia Escura

- **A definição de normas** é criada e implementada pelas entidades com poderes para definir o ambiente da rede de informação. São, na prática, normas *sui generis* que definem as redes de informação como tal. Vêm em camadas que são interdependentes
- **As autoridades definidoras** são os criadores das normas definidoras. É a entidade que, através das suas acções, cria as regras do sistema lógico em que o organismo opera.
- O maior **corpo definidor**, mesmo que não seja a entidade que cria as regras do sistema lógico, **é o utilizador enquanto tal**.
- O conceito de prestação **por via electrónica é definido** na Directiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, no artigo 1(b)(ii), onde é definido como um serviço que é enviado

[5] TRADOC. Cyberspace Operations: Concept Capability Plan 2016-2028 [online]. [citado 18/02/2018], pp. 8-9 Disponível em: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

inicialmente e recebido no seu destino através de equipamento electrónico para o processamento (incluindo a compressão digital) e armazenamento de dados.

- **Um pedido individual do utilizador** significa que deve ser uma acção activa do utilizador
- A fim de determinar os direitos e obrigações individuais dos fornecedores de ligação, é necessário dividir estes fornecedores em dois grupos - **públicos e não públicos.** Ambos os grupos de fornecedores de ligação são abrangidos pela Lei sobre certos serviços da sociedade da informação, mas os fornecedores de ligação pública são também abrangidos pela Lei sobre comunicações electrónicas, que define outros direitos e obrigações destes fornecedores
- De acordo com o § 6 do ACISS, **o fornecedor da ligação não é obrigado** a supervisionar o conteúdo da informação transmitida ou a verificar activamente a ilegalidade da informação transmitida.
- **Serviço de comunicações electrónicas** [secção 2 (n) da ECA[6]]. De acordo com a secção 2 (n) do ECA, o termo significa um serviço normalmente prestado mediante remuneração e que se baseia na transmissão (total ou principalmente) de sinais através de uma rede de comunicações electrónicas.
- **Serviço de comunicações electrónicas publicamente disponível** [secção 2 (o) ECA]. Este serviço é um serviço de comunicações electrónicas do qual ninguém está anteriormente excluído de utilizar.
- **Uma empresa** que fornece ou está autorizada a fornecer uma rede pública de comunicações ou recursos conexos é referida pela presente lei como **um operador** [secção 2 (e) ECA].
- **Um assinante** [parágrafo 2(a) ECA] é qualquer pessoa que tenha celebrado um contrato para a prestação de tal serviço com uma empresa que preste serviços de comunicações electrónicas publicamente disponíveis.
- **Um utilizador** é qualquer pessoa que utilize ou solicite um serviço de comunicações electrónicas publicamente disponível.
- **O teste de proporcionalidade** é um instrumento jurídico padrão tanto dos tribunais internacionais como constitucionais (domésticos) ao avaliar a colisão de regras de direito destinadas a proteger um direito ou interesse público constitucionalmente garantido com outro direito ou liberdade fundamental.
- **O Information Security Management System** (**ISMS**)[7] **é um conjunto de princípios concebidos para** manter a confidencialidade, integridade e disponibilidade da informação, aplicando um processo de gestão de riscos e assegurando às partes interessadas que os riscos são devidamente geridos.[8]
- A solução ISMS requer uma abordagem sistémica e abrangente, respeitando os princípios e elementos de todo o ciclo de vida da segurança cibernética. O sistema de gestão do SGSI baseia-se no ciclo Deming, ou **ciclo PDCA** (**Plan-Do-Check-Act**).
- Um bem pode ser, de uma perspectiva de direito civil, uma coisa **tangível** (edifício, sistema informático, redes, energia, bens, etc.) ou **uma** coisa **intangível** (informação, conhecimento, dados, programas, etc.).
- Um bem pode também ser **qualidade** (por exemplo, disponibilidade e funcionalidade do sistema e dos dados, etc.) ou **bom nome,** reputação, etc.
- **As pessoas** (utilizadores, administradores, etc.), com os seus conhecimentos e experiência, são também uma mais-valia do ponto de vista da segurança cibernética.
- **Um agente de apoio** é um agente técnico, empregados e fornecedores envolvidos na operação, desenvolvimento, administração ou segurança de um sistema TIC.
- **O bem subjacente** é a informação ou serviço processado ou fornecido pelo sistema TIC.
- A Gestão da Continuidade de Negócios (**GCN**) é um processo baseado na identificação de elementos-chave (sistemas e processos) numa organização e depois estabelecer processos e procedimentos

[6] A seguir referido como ECA
[7] A seguir referido como **SGSI**
[8] Cf. introdução da ISO/IEC 27001

para assegurar a continuidade ou renovação desses elementos, a um nível pré-determinado em que ainda será possível executar as tarefas essenciais da organização.

- O termo **perímetro de segurança** física designa um espaço designado ou os limites desse espaço. Tal espaço pode ser, por exemplo, um conjunto de instalações, as próprias instalações ou parte das instalações.
- **As instalações** são um edifício ou outro espaço fechado.
- **Limite das instalações** significa uma divisória de edifícios, uma barreira física (cerca) ou outro limite de terreno visivelmente definido.
- **Uma área segura** significa um espaço num edifício que está estruturalmente ou de outra forma visivelmente separado.
- O termo **permissão** significa o direito de acesso a qualquer activo (geralmente um sistema informático ou de comunicação, aplicação, etc.) Na prática, é uma ferramenta para "gerir utilizadores e grupos" e uma ferramenta para definir permissões em ficheiros e directórios.
- Como parte da segurança física, alguns administradores são obrigados a realizar **testes de penetração do** sistema TIC, concentrando-se em bens importantes, nomeadamente:
    - antes de serem postos em serviço e
    - devido a uma mudança substancial.
- Como parte da segurança da aplicação, a empresa também assegura que os pedidos, informações e transacções são sempre protegidos contra:
    - acção não autorizada,
    - recusa de actuação.
- O valor do risco é mais frequentemente expresso em função do impacto, da ameaça e da vulnerabilidade. Por exemplo, a seguinte função pode ser usada para auto-avaliar o risco:

  Risco = impacto * ameaça * vulnerabilidade

- O Regulamento Geral de Protecção de Dados (UE) 2016/679 ou GDPR/ RODO[9] é um dos mais importantes documentos jurídicos internacionais que se relaciona directamente com a questão da segurança cibernética, embora não se destine principalmente ao campo das TIC.

  GDPR ≠ IT + software.

- **Os dados pessoais são sobretudo publicados nas redes sociais**, o que, pela sua própria natureza, pressupõe tal divulgação e consagra nos Termos e Condições as regras ao abrigo das quais tais dados são tratados
- De acordo com o artigo 4 (1) GDPR/RODO, os dados pessoais são "**qualquer informação relativa a uma pessoa singular identificada ou identificável".**
- De acordo com o n.º 2 do artigo 4.º do RODO, entende-se por tratamento de dados pessoais **qualquer operação ou** conjunto de **operações** efectuadas sobre **dados pessoais** ou conjuntos de dados pessoais, seja ou **não por meios automatizados, tais** como recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.
- Uma das áreas que a GDPR aborda explicitamente é a **segurança do processamento de dados pessoais**.
- A Avaliação de Impacto na Protecção de Dados (**DPIA**) é um instrumento a ser utilizado quando um tipo específico de **tratamento, em particular utilizando novas tecnologias, tendo em conta** a natureza, âmbito, contexto e objectivos do tratamento, é **susceptível de apresentar um risco elevado para os direitos e liberdades dos indivíduos.** É um instrumento que pode ajudar os

[9] [em linha]. Disponível em: http://eur-lex.europa.eu/legal-content/

responsáveis pelo tratamento a identificar riscos potenciais associados ao tratamento de dados pessoais e a implementar medidas adequadas.

- A avaliação do impacto da protecção de dados deve incluir:
    - descrição das operações de processamento planeadas,
    - avaliação da necessidade e da adequação das medidas tendo em vista o objectivo (**teste de proporcionalidade**),
    - avaliar os riscos para os direitos e liberdades dos sujeitos,
    - as medidas previstas para enfrentar estes riscos, incluindo garantias, medidas de segurança, etc.
- Os traços digitais, com base na possibilidade de serem influenciados pelo utilizador, podem ser amplamente **divididos em traços que podem ser influenciados (activos) e traços que não podem ser influenciados (passivos).**
- Por defeito, um endereço IP não é anónimo, e um sistema informático utiliza-o como um dos seus identificadores quando comunica com outros sistemas informáticos. Os endereços IP são atribuídos hierarquicamente, sendo o papel dominante desempenhado pela **ICANN,** que divide o mundo real em regiões geridas pelos **Registos Regionais** da Internet (**RIRs**).
- Os registos regionais dividem ainda mais os intervalos de IP atribuídos entre os Registos de Internet **Locais** (**LIR**). O registo local é normalmente um ISP - um fornecedor de ligação, público ou não público. Este registo pode então partilhar a sua gama de endereços IP com, por exemplo, partes da sua organização ou outras entidades.

3. Durante as aulas

<u>Algumas ideias para actividades:</u>

WORKSHOPS

1. Definição do alcance da lei no ciberespaço (fronteiras, possibilidades, etc.).
2. Responsabilidade privada e pública pelas acções de um utilizador ou empresa no ambiente online.
3. Características e definição dos diferentes FSI e dos seus direitos e obrigações em relação à segurança cibernética.
4. ISMS e a relação com a lei de segurança cibernética.
5. Direitos e obrigações básicos das entidades individuais da Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas para um elevado nível comum de segurança das redes e sistemas de informação na União, também da legislação nacional.
6. Aplicação dos direitos e obrigações da GDPR/RODO no ciberespaço.
7. Análise prática dos termos e condições de amostras de acordos de privacidade de ISP.

PERGUNTAS DE REVISÃO

1.

- O que é a lei?
- O que é uma norma legal e como está dividida?
- O que é o ciberespaço?
- Em que camadas consiste o ciberespaço?
- A lei aplica-se no ciberespaço e, em caso afirmativo, que normas jurídicas se aplicam?
- Como pode a lei ser aplicada no ciberespaço, incluindo possíveis sanções ou outras medidas?

- Dar alguns exemplos da aplicação da lei no ciberespaço.
- Definir ISMS.

2.

- Definir PSI.
- Como estão divididos os ISPs? De acordo com que critérios?
- Quais são as responsabilidades dos ISPs?
- O que é uma norma definidora?
- Quem é a autoridade definidora e qual é o seu papel?
- O que é a retenção de dados?

3.

- O que é o ciclo PDCA e qual é a sua aplicação?
- Que elementos podem ser incluídos na segurança física?
- O que é: Gestão da Continuidade do Negócio?
- Definir a ameaça.
- Definir o risco.
- Definir o impacto.
- Definir vulnerabilidade.
- Definir activos.
- O que é um bem, o que são os bens?

4.

- Qual é o âmbito territorial do GDPR?
- O que são dados pessoais?
- Um endereço IP é um dado pessoal?
- Quais são as responsabilidades do responsável pelo tratamento dos dados pessoais?
- O que se entende por tratamento de dados pessoais?
- O que significa uma avaliação do impacto da protecção de dados?

5.

- Definir o termo "pegada digital".
- Qual é a diferença entre as pegadas digitais?
- Em que componentes consiste uma pegada digital passiva?
- O que é um LIR?
- Que informação é que um endereço IP transporta sobre um utilizador?

- O que é um EULA?

Trabalhar em pares/grupos

- **Pares - mini-projecto**
  Em pares, os estudantes escolhem um dos tópicos discutidos. Eles escrevem as suas conclusões e apresentam-nas aos outros. Após a apresentação, os outros estudantes preparam perguntas adicionais para o grupo de apresentação.

- **Mapa de pensamentos**
  Os estudantes em pares escolhem um dos tópicos abordados e criam um mapa mental, que depois descrevem aos outros estudantes numa breve apresentação.

- **Palavras-chave**
  Os alunos em pares seleccionam individualmente palavras-chave a partir do glossário.

Eles escrevem as definições destas palavras em tiras de papel. Viram as tiras de papel com o lado em branco para cima. Um aluno escolhe uma tira, lê a definição e o outro aluno procura uma palavra-chave correspondente.
ou
Os alunos escrevem algumas palavras-chave do glossário num pedaço de papel. Eles viram as cartas com o lado em branco para cima. Um estudante pega no primeiro cartão e diz o que a palavra significa. O segundo aluno adivinha a palavra-chave.

- 10 palavras-chave
  Os estudantes escolhem 10 palavras-chave relacionadas com o tema escolhido. Estas 10 palavras-chave são dadas a outros pares. Os pares escrevem um texto que deve conter todas as palavras-chave. Uma frase só pode conter uma palavra-chave. Assim, o texto é composto de pelo menos 10 frases.

- Painel de discussão

  Os alunos escolhem 3 oradores. Cada orador escolhe um tópico para discutir. Os outros estudantes fazem perguntas sobre os tópicos. Cada orador pode usar um tipo de resposta - TRUE X FALSE. O estudante recebe um ponto para cada resposta verdadeira, por exemplo, GDPR significa Regulamento Geral de Protecção de Dados? - VERDADEIRO X FALSO.

4. Recursos da Internet

Ver bibliografia.

5. Perguntas/testões adicionais

SELECCIONAR A RESPOSTA CORRECTA:
(A resposta correcta foi sublinhada)

1. _____ é estabelecido pelo Estado ou sistema de governo e é, portanto, pré-determinado. Consiste em regras previsíveis que são aplicadas, ou seja, a sua violação é punida.

a) Direito positivo
b) Lei natural
c) Direito subjectivo
d) Lei objectiva

2. _____representa uma regra de conduta de aplicação geral que rege os direitos e obrigações dos actores.

a) Norma legal
b) Direito legal
c) Norma legal
(d) Linha jurídica

3. _____ - uma regra de conduta regula as relações sociais com efeito vinculativo

(a) uma decisão final
(b) legalmente conducente
(c) legalmente justificado
(d) juridicamente vinculativo

4. A estrutura padrão de uma norma jurídica é constituída por três partes, que são _____.

(a) hipótese, disposição e sanção
(b) Antecipação, disposição e sanção
(c) Hipótese, infracção e sanções
(d) Hipótese, disposição e penalização

5. _____ é a expressão das consequências de uma violação de uma obrigação legal decorrente da disposição de uma norma legal.

a) Repatriamento
(b) Julgamento
(c) Sanção
(d) Revisão

6. A norma _____ não especifica de todo uma regra básica de conduta ou apenas a define como uma possibilidade. Cabe aos destinatários determinar as regras. Se os destinatários não o fizerem, as disposições da norma servem de guia para o juiz ao decidir.

(a) Lógico
(b) Dispostivo
(c) categórica

(d) significativo

7. _____ normas legais regulam as relações entre actores dentro da jurisdição de um Estado ou normalmente dentro do seu território

a) Público
(b) Internacional
c) Particular
d) Nacional

8. _____ As normas legais aplicam-se a todo o território de um Estado ou da União Europeia. Além disso, aplicam-se a todas as entidades sem limitação do seu âmbito temporal.

(a) Internacional
b) Nacional
c) Substantivo
d) Civil

9. O ciberespaço também pode ser definido como o espaço das actividades cibernéticas ou como o espaço criado pelas tecnologias de informação e comunicação em que é criado um mundo (ou espaço) _____ paralelo ao espaço real.

(a) digital
(b) real
(c) virtual
(d) actual

10. O ciberespaço também pode ser definido de acordo com a disponibilidade e _____ dos dados para o utilizador médio.

(a) eficácia
(b) eficácia
(c) desempenho
(d) Rastreabilidade

11. O princípio_____ implica a utilização apenas dos meios mais amigos do ambiente para atingir o objectivo pretendido (interferência nos direitos e liberdades fundamentais) de entre vários possíveis.

(a) Necessidade
(b) Adequação
(c) proficiência
(d) Adequação

12. O que significa a abreviatura ISMS?

    (a) Sistema Seguro de Gestão de Informação

    (b) O Sistema de Gestão da Segurança da Informação

    (c) Gestão sistemática de informação segura

    (d) Equipa de Segurança da Informação do Sistema

13. Uma política de segurança é um conjunto de princípios e regras que _____políticas para assegurar/-e/-u a protecção dos bens.

    (a) determinar

    (b) afectar

    (c) prevenir

    (d) influência

14. O termo _____ significa o direito de acesso a qualquer bem (geralmente um sistema de informação ou comunicação, aplicação, etc.).

    (a) candidatura
    (b) a licença
    (c*) permissão)*
    (d) passe

15. O que significa a abreviatura DPIA?

    a) Avaliação do Impacto dos Dados Permitidos
    b) Avaliação do impacto da protecção de dados
    (c) Avaliação do impacto dos dados
    (d) Avaliação do impacto dos dados promissores

Bibliografia

ANGWIN, Julia. *Conheça o Dispositivo de Rastreio Online que é Virtualmente Impossível de bloquear.* [online]. [citado 10/06/2016].

BARLOW, Perry John. *Declaração de independência do ciberespaço.* [online]. [citado.23.09.2014]. Disponível em: https://www.eff.org/cyberspace-independence.

CAETANO, Lianne. *As suas aplicações estão a ser sobre-partilhadas? O Relatório de Segurança Móvel de 2014 diz tudo.* [online]. [citado 10/04/2015]. Disponível em: https://blogs.mcafee.com/consumer/mobile-security-report-2014/.

CNN sobre sexo pedófilo no Second Life. [online]. [citado 18.06.2009]. Disponível em: http://www.youtube.com/watch?v=AQM-SiiaipE
População mundial actual. [em linha]. [citado 10.08.2015]. Disponível em: http://www.worldometers.info/world-population/.

Estatísticas interessantes sobre estratégias móveis para a transformação digital. [em linha]. [citado 15/07/2016]. Disponível em: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

Retenção de dados inconstitucional na sua forma actual. [em linha]. [citado 16/07/2016]. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

Digital, Social & Mobile no mundo em 2015. [em linha]. [citado 09/08/2015]. Disponível a partir de:http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

ENGLEHARDT, Steven e Ardvin NARAYANANAN. *Seguimento em linha: Medição e análise de 1 milhão de sítios.* [em linha]. [citado.05.08.2016]. Disponível em: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

O Facebook poderá em breve identificá-lo em cada fotografia. [online]. [citado 09.08.2015]. Disponível a partir de: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

O FBI explora a vulnerabilidade do Flash para quebrar a segurança da rede Tor. [online]. [citado.23/07/2016]. Disponível em: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/.

Primeira Emenda. [em linha]. [citado 10/07/2016]. Disponível a partir de: https://www.law.cornell.edu/constitution/first_amendment.

O Bundestag alemão aprova nova lei de retenção de dados. [em linha]. [citado 16/07/2016]. Disponível em: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

HAINES, Lester. *Jogador online apunhalado por palavras cibernéticas 'roubadas'.* [online]. [citado 03/10/2006]. Disponível em: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praga: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, pp. 101-102.

Censura na Internet. [em linha]. [citado 10.08.2016]. Disponível em: http://www.deliveringdata.com/2010_10_01_archive.html.

História da Internet dos anos 80 [online]. [citado 07.06.2016]. Disponível em: http://www.computerhistory.org/internethistory/1980s/.

JOHNSON, David R. e David POST. *A Ascensão da Lei no Ciberespaço.* [online]. [citado 10/07/2016].

KOLOUCH, Jan e Andrea KROPÁČOVÁ. Responsabilidade pelo seu próprio dispositivo e pelos dados e aplicações nele armazenados. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14).* [B.m.], c2014, pp. 321-324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

KOLOUCH, Janeiro. *Cibercriminalidade.* Praga: CZ.NIC, 2016, p. 78 e seguintes. e pp. 109 e seguintes.

Redes sociais líderes no mundo, a partir de Abril de 2016, classificadas por número de utilizadores activos (em milhões) [online]. [citado 10.08.2015]. Disponível em: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

LESSIG, Lawrence. *Código v. 2. p.* 6 Disponível na íntegra (eng) [online]. [cit.13/03/2008]. Disponível: http://pdf.codev2.cc/Lessig-Codev2.pdf

MAISNER, Martin e Barbora VLACHOVÁ. *Zákon o kybernetickébezpečnosti. Komentář.* Praga: Wolters Kluwer, 2015. p. 85

MATEJKA, Ján. *Internet jakoobjektpráva: hledánírovnováhyautonomie a soukromí.* Praga: CZ.NIC, 2013. ISBN 978-80-904248-7-6 pp. 25

Desafios jurídicos nacionais à Directiva de Retenção de Dados. [em linha]. [citado 16/07/2016]. Disponível em: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html.

O ciclo PDCA. [em linha]. [citado 06/07/2018]. Disponível em: https://www.creativesafetysupply.com/glossary/pdca-cycle/.

PETERKA, Jiří. *Uchovávatprovozní a lokalizačníúdajenámuž EU nenařizuje. My to v tom ale pokračujeme.* [online]. [citado 10/11/2015]. Disponível em: http://www.earchiv.cz/b14/b0428001.php3

REED, Chris. *Direito da Internet*. Cambridge: Cambridge University Press, 2004, p. 218.
Registos regionais em linha. [em linha]. [citado 04.08.2015]. Disponível em: https://*www.nro.net/about-the-nro/regional-internet-registries.*

ROSER, Christoph. *The Many Flavors of the PDCA.* [em linha]. [citado 06/07/2018]. Disponível em: https://www.allaboutlean.com/pdca-variants/.

SMITH, Craig. *Pelos Números: 100 estatísticas e factos surpreendentes da pesquisa do Google.* [online]. [citado 04/08/2016]. Disponível a partir de: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/.

Tribunal de Justiça da União Europeia. Comunicado de imprensa n.º 54/14, 8 de Abril de 2014. Acórdão nos processos apensos C-293/12 e C-594/12 [online]. [citado 15/07/2016]. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf.

Conclusões do Advogado-Geral Pedro Cruz Villalón. Processo C-293/12 e C-594/12 [online]. [citado.15/07/2016]. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

Conclusões do Advogado-Geral SAUGMANDSGAARD ØE, datadas de 19/07/2016. Nos processos apensos C-203/15 e C-698/15 [em linha]. [citado 10/8/2016]. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

Surface Web, Deep Web, Dark Web - qual é a diferença? [em linha]. [citado 20/07/2016]. Disponível a partir de: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference.

Módulo 3

Detecção e prevenção de ameaças cibernéticas

1. Introdução

1.1 Resumo do curso

O curso centra-se inicialmente numa visão geral das normas legais básicas da cibercriminalidade. É também necessário compreender o conceito de cibercrime a fim de se compreender toda a questão. Uma parte significativa do curso trata da classificação dos cibercrimes. O curso analisa os vários cibercrimes, que são descritos em grande detalhe. A parte principal do curso é dedicada aos ciberataques e às suas sanções.

1.2 Objectivos do curso

Os estudantes são introduzidos às normas legais que regem o crime cibernético. O objectivo do curso é familiarizar os alunos com a questão dos ciberataques, que podem ter as características de comportamentos ilegais, bem como a possível qualificação legal de tais comportamentos. A parte principal do curso é identificar as formas e métodos de cometer cibercrimes. O curso também se concentra em spam, fraude, hoaxes e botnets. Além disso, os alunos estudarão os ataques cibernéticos, especificamente os relacionados com finanças (pharming, spearphishing, mobile phishing), mas também os ataques relacionados com a sociedade (cyberbullying, perseguição, sexting, cyber grooming, etc.). A prevenção destes fenómenos negativos é um conteúdo importante deste módulo.

1.3 Conteúdo do curso

Palestras individuais introduzem os estudantes às normas legais que regem o cibercrime. Além disso, os estudantes são introduzidos à engenharia social, spam, fraude, hoax e botnet. Durante as aulas, os alunos são introduzidos a diferentes tipos de ataques cibernéticos, tais como hacking, cracking, malware, ransomware. Não só são mencionados ataques cibernéticos, tais como ataques contra as finanças (phishing, pharming, spearphishing, mobile phishing), mas também ataques cibernéticos sociais (cyberbullying, perseguição, sexting, cybergrooming, etc.).

1.4 Objectivos de aprendizagem

1) Introdução à terminologia da cibercriminalidade
2) Conhecer os regulamentos nacionais sobre a cibercriminalidade
3) Conhecer os regulamentos internacionais sobre cibercriminalidade
4) Compreender a importância da engenharia social no contexto dos ciberataques
5) Consciência das manifestações de cibercriminalidade
6) Compreender os ciberataques

1.5. Equipamento e materiais necessários

Detecção e prevenção de ataques informáticos - disponível online

1.6 Syllabus

Resultado da aprendizagem	O aluno que completar o módulo com sucesso saberá/ será competente no seguinte.
NOVIDADES	
W1	O estudante obterá uma visão geral das normas jurídicas nacionais e internacionais que definem as actividades ilegais no ciberespaço.
W2	O aluno aprenderá a terminologia técnica básica que está relacionada com ataques cibernéticos, incidentes cibernéticos, crimes cibernéticos, etc. Será capaz de distinguir que norma legal ou disposições especiais se aplicam a um determinado ataque e porquê.
HABILIDADES	
U1	Após a conclusão do curso, o aluno será capaz de identificar ataques cibernéticos básicos, o seu modus operandi, as consequências causadas, etc.
U2	Com base na identificação acima referida, o estudante poderá aplicar instâncias legais específicas à violação em questão. O estudante será capaz de tomar medidas preventivas básicas para possivelmente eliminar comportamentos negativos no futuro.
COMPETÊNCIAS	
K1	O estudante é capaz de distinguir entre diferentes ciberataques, controla parcialmente as disposições legais relacionadas com a protecção contra estes ataques e é capaz de aplicar medidas básicas de prevenção.

Conteúdo do módulo (programa de palestras e outras actividades)	**Referência aos resultados da aprendizagem**
LECTURAS 1. Engenharia social 2. Spam, burla, fraude 3. Botnet 4. Ataques cibernéticos - Hacking, cracking, malware, ransomware 5. Ataques cibernéticos - ataques de natureza financeira (phishingpharming, spearphishing, mobile phishing) 6. Ataques cibernéticos - ataques sociais (cyberbullying, perseguição, sexting, cybergrooming, etc.). WORKSHOPS 1. Análise de ataques individuais - modus operandi 2. Teste de segurança contra ataques seleccionados. 3. Definição de opções para prevenir determinados tipos de ataque 4. Concepção de uma solução personalizada para proteger contra ataques cibernéticos individuais. 5. Testes de segurança de certos sistemas, aplicações e dados. Os estudantes tentarão conceber as suas próprias soluções para aumentar a segurança destes sistemas, aplicações ou dados. 6. Familiarize-se com ferramentas e recursos para armazenamento seguro de dados e estabelecimento de comunicação segura em linha (por exemplo, administração e definições de VPN, PGP, gestor de senhas, etc.).	W1, W2 U1, U2, K1

Saldo de crédito ECTS		
Forma de carga de trabalho dos estudantes		Número de horas
Número de horas com participação directa do professor académico		
1.1	Participação em conferências	6
1.2	Participação em seminários	
1.3	Participação em workshops	14
1.4	Participação em actividades laboratoriais	
1.5	Participação em projectos	
1.6	Participação em consultas (2-3 vezes por semestre)	
1.7	Participação na consulta do projecto	
1.8	Participação em exames/teste	2
1.9	Outros ...	
1.10	**Número de horas passadas com assistência directa de pessoal académico (soma 1.1 - 1.9)**	22
1.11	**Número de créditos ECTS obtidos pelo aluno em aulas que requerem a participação directa de um professor académico)**	1
Trabalho individual do estudante		
2.1	Estudos individuais (incluindo palestras de e-learning)	25
2.2	Preparação individual para workshops	10
2.3	Preparação do teste individual	
2.4	Preparação individual para aulas de laboratório	
2.5	Elaboração de relatórios	
2.6	Implementação de tarefas auto-realizadas (projectos, documentação)	
2.7	Preparação para o exame/teste final do seminário	5
2.8	Preparação para exame/teste final de conferências	5
2.9	Outros	
2.10	**Número de horas de trabalho individual (soma de 2,1 - 2,9)**	45
2.11	**Número de créditos ECTS obtidos pelo estudante em actividades individuais de aprendizagem**	1,5
Carga de trabalho total (h)		**67**
Créditos ECTS para o módulo		**2,5**

Métodos de verificação dos resultados da aprendizagem									
Resultado da aprendizagem	**Formas de classes de crédito**								
	Exame oral	Exame escrito	Trabalho escrito parcial	Trabalho final escrito (ensaio,	Teste	Desenho/apresentação	Relatório	Actividades de sala de aula	Outros ...
NOVIDADES									
W1, W 2		x	x		x			x	
HABILIDADES									
U1						x		x	
U2						x		x	
COMPETÊNCIAS									
K1						x		x	

Critérios para avaliar a competência dos estudantes
Os requisitos mínimos para os três grupos de resultados de aprendizagem que o Estudante deve atingir a fim de passar na disciplina são apresentados abaixo de forma sintética. Para que um Estudante passe num módulo, todos os resultados de aprendizagem descritos no programa devem ser verificados positivamente pela(s) pessoa(s) que ensina(m) o módulo.

W - CONHECIMENTO
Avaliação:
Satisfatório - O aluno lembra-se e reproduz os conhecimentos a dominar dentro do módulo.
Bom - O estudante interpreta adicionalmente fenómenos/problemas e é capaz de resolver um problema típico
Muito bom - O estudante é capaz de resolver problemas mesmo complexos num determinado campo, é capaz de sintetizar, realizar uma avaliação abrangente, criar um trabalho que é original e inspirador para outros.

U - HABILIDADES
Avaliação:
Satisfatório - O aluno conhece a natureza das actividades e é capaz, sob a orientação do professor académico, de realizar actividades / resolver problemas relacionados com o conteúdo do módulo
Bom - O estudante é capaz de realizar actividades / tarefas / resolver problemas típicos relacionados com o conteúdo do módulo
Muito bom - O aluno dominou totalmente a capacidade / habilidade para realizar as actividades / tarefas / problemas previstos no conteúdo do módulo, também em casos mais complexos.

K - COMPETÊNCIA SOCIAL
Avaliação:
Satisfatório - O aluno assimila passivamente o conteúdo do módulo, demonstrando capacidade de concentração e escuta
Bom - O estudante participa activamente nas aulas, faz juízos de valor de acordo com os critérios aceites no domínio em questão, pode cooperar activamente num grupo
Muito bom - O estudante integra a atitude de acordo com o modelo proposto, desenvolve o seu próprio sistema de valores profissionais e sociais, é capaz de assumir a responsabilidade pelas acções do grupo, incluindo a liderança.

2. Material básico para o professor

Definições (glossário)

Cibercrime - é mais comummente utilizado para se referir a crimes cometidos utilizando a tecnologia da informação, e a utilização do termo também passou do campo normativo para o vocabulário profissional.
Cibercrime - é um crime em que meios de informação e tecnologia de comunicação são **utilizados como instrumento para cometer um crime e como alvo de um ataque do perpetrador**, **e o referido ataque é um crime, desde que estes dispositivos sejam utilizados ou abusados num ambiente de informação, sistema, software ou comunicação (isto é, ciberespaço).**
O cibercrime pode ser definido como um comportamento dirigido contra um computador ou, em alguns casos, uma rede informática, ou como um comportamento em que um computador é utilizado como um instrumento para cometer um crime. Um critério indispensável para aplicar a definição de cibercrime é que o ambiente em que a actividade tem lugar seja então uma rede informática, ou seja, o ciberespaço.
Cibercrime - qualquer crime em que o perpetrador tenha utilizado tecnologias de informação e comunicação

FP TERMINAL - Fraude de pagamento. Grupo dedicado à prestação de apoio em matéria de fraude em linha.

FP Cyborg - Crimes de alta tecnologia. Um grupo que lida com e presta apoio a vários ataques cibernéticos que afectam infra-estruturas críticas e sistemas de informação. Em particular, estes incluem ataques como malware, resgates, hacking, phishing, roubo de identidade, etc.
Gémeos FP - Exploração Sexual Infantil. Um grupo que se ocupa e dá apoio na investigação do abuso sexual de crianças
Incidente de segurança informática (que pode ser entendido como um ataque informático ou crime informático) - uma acção ilegal, não autorizada e inaceitável que afecta um sistema ou rede informática.
Ataque cibernético[10] - pode, portanto, ser definido como **qualquer comportamento ilegal de um agressor no ciberespaço que seja dirigido contra os interesses de outra pessoa.**
Um incidente de cibersegurança - é um evento que pode causar uma violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas.
Incidente de cibersegurança - é uma violação da segurança da informação nos sistemas de informação, ou uma violação da segurança da prestação de serviços, ou uma violação da segurança e integridade das redes de comunicação electrónica como resultado de um evento cibernético.
Dados informáticos - significa qualquer expressão de factos, informações ou conceitos de uma forma adequada ao processamento num sistema informático, incluindo um programa capaz de levar um sistema informático a executar uma função.
Informação - são dados que foram processados num formulário que é útil para o destinatário. Portanto, qualquer informação é informação, mas qualquer dado armazenado não se torna necessariamente informação.
Engenharia social - envolve influenciar, persuadir ou manipular as pessoas a fim de as levar a tomar uma determinada acção ou de obter deles informações que de outra forma não dariam.
Uma botnet pode ser definida muito simplesmente como uma rede de bots ligados por software[11] , que executam alguma acção baseada num comando do 'proprietário' (ou administrador) dessa rede. Uma rede construída desta forma pode ser utilizada para actividades legítimas (por exemplo, computação distribuída) ou para actividades ilegais.
Arquitectura descentralizada - é normalmente construída sobre uma arquitectura peer-to-peer (P2P). Esta arquitectura permite a partilha de recursos e comandos dentro de uma rede P2P.
O malware - serve como um meio de acesso, controlo e propagação de malware ou outras tarefas conforme as instruções do atacante, e não apenas no caso de botnets. Contudo, se o malware está actualmente a infectar o sistema informático de um utilizador, é altamente provável que se tenha tornado parte de uma rede de botnets
Malware (derivado de *software malicioso*) pode ser qualquer programa utilizado para perturbar o funcionamento padrão de um sistema informático, obter informações (dados) ou ser utilizado para obter acesso a um sistema informático. O malware pode assumir muitas formas, com muitos tipos de malware a serem nomeados de acordo com a actividade que realiza.
Adware significa "*software suportado por publicidade".* É a forma menos perigosa mas rentável de malware.[12]

[10] É necessário distinguir o conceito de um ataque informático do de um **incidente de segurança,** que constitui uma violação da segurança SI/TI e das regras estabelecidas para a sua protecção (política de segurança).

[11]**Bot** (abreviatura de robot). Este é um programa que pode executar os comandos do atacante introduzidos a partir de outro sistema informático. A forma mais comum de o fazer é infectar o computador com um vírus como um verme, um cavalo de Tróia, etc. Um sistema informático que é controlado remotamente desta forma é então referido como um **zombie**. No entanto, algumas fontes até se referem a um sistema informático infectado como um bot.
O bot pode recolher dados, processar pedidos, enviar mensagens, comunicar com o elemento de controlo, etc.

[12] Há empresas especializadas em "pagar por instalação" (*PPI*). *O "PPI" resulta então numa miríade de acções que levam à instalação de add-ons ou outro software indesejado que (no caso menos prejudicial) lista anúncios em websites sem o conhecimento do utilizador ou insere-os onde não há anúncios no website....* ***A PPI confia no facto de que aqueles que oferecem estes serviços não se importam se o utilizador quiser instalar alguma coisa. Recebem até US$1,50 por***

Spyware é uma combinação das palavras inglesas '*spy*' e '*software'*. Spyware é utilizado para obter dados estatísticos[13] sobre o funcionamento de um sistema informático e enviá-los para a caixa de dados do atacante sem o conhecimento ou consentimento do utilizador. Estes dados podem também incluir informações de natureza pessoal ou informações sobre a pessoa do utilizador, bem como informações sobre websites visitados, aplicações executadas, etc.
Vírus - são um programa ou código malicioso que se liga a outro ficheiro executável existente (por exemplo, software, etc.) ou documento. O vírus é replicado quando esse software é executado ou quando o documento infectado é aberto. Mais frequentemente, os vírus propagam-se através da partilha de software entre sistemas informáticos; não é necessária a cooperação do utilizador para os espalhar.
Os vermes informáticos também são **referidos** como vírus. A razão para a associação mais estreita com vírus é que os vermes não precisam de nenhum hospedeiro, ou seja, não têm um ficheiro executável (como os vírus). Ao contrário dos vírus, que são incluídos como parte de outro programa, estes programas geralmente propagam-se separadamente.
Os cavalos de Tróia são geralmente os programas informáticos que contêm funções ocultas com as quais o utilizador não concorda ou não tem conhecimento, e que são potencialmente perigosos para a continuação do funcionamento do sistema.
Backdoor - alguns Trojans, quando lançados sem o conhecimento do utilizador, abrem as portas de comunicação do computador, tornando muito mais fácil para outros malware infectar ainda mais o sistema atacado ou facilitar o controlo directo do computador infectado remotamente.
Scanning[14] **programas** ('*port scanners*') - ou seja, programas utilizados principalmente para determinar quais as portas de uma rede de comunicações de um computador estão abertas, que serviços estão a correr nelas e se é possível lançar um ataque a um tal sistema.
Rootkits- refere-se não só a programas informáticos, mas também a toda a tecnologia utilizada para mascarar a presença de malware (por exemplo, vírus informáticos ou cavalos de Tróia, worms, etc.) num sistema infectado. Na maioria das vezes, assumem a forma de programas de computador não muito grandes. Os rootkits não são prejudiciais em si mesmos, mas são explorados pelos criadores de programas maliciosos, tais como vírus, spyware, etc.[15]
Keylogger- é um software que regista toques de teclas específicos num sistema informático infectado. Mais frequentemente, um keylogger é utilizado para registar detalhes de login (nome de utilizador e palavra-passe) para contas que são acedidas a partir do sistema informático. A informação obtida é então geralmente enviada ao atacante.
Ransomware - é um malware que impede ou restringe os utilizadores de utilizar correctamente um sistema informático até que o atacante receba um "resgate". O Ransomware entra frequentemente num computador através de malware (cavalo de Tróia ou worm) que se encontra num website ou é um anexo de correio electrónico. Uma vez que o malware se tenha 'estabelecido' em segurança no sistema informático, o seu próprio 'resgate' será descarregado.
Crypto-ransomware - o objectivo deste malware é encriptar o disco rígido ou tipos de ficheiros seleccionados no sistema informático. Visa principalmente encriptar os ficheiros privados do utilizador, tais como imagens, documentos de texto ou folhas de cálculo, vídeos, etc.
Resgate policial - depois bloqueia o acesso à conta do utilizador no Windows[16] notificando o utilizador de

***instalação**, pelo que é mais do que certo que as instalações fraudulentas e automatizadas são uma parte essencial do seu 'modelo de negócio'".*

[13] Por exemplo, uma visão geral dos websites visitados, os seus endereços IP, uma visão geral dos programas instalados e utilizados, registos de downloads de ficheiros da Internet, dados sobre a estrutura e o conteúdo dos directórios armazenados no disco rígido, etc.

[14] Estes programas são por vezes referidos como programas de digitalização ou scanners.

[15]Para mais detalhes ver BALIGA, Arati, Liviu IFTODE e Xiaoxin CHEN. Contenção automatizada de ataques de Rootkits. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 323-334.

[16] A candidatura foi definida para "StayOnTop". O utilizador não pode ver outras aplicações escondidas sob este "diálogo de resgate" e é incapaz de invocar o gestor de tarefas. O próprio Ransomware foi registado nos registos Run e RunOnce e efectuava uma verificação a cada 500 ms e escondia o gestor de tarefas dentro do mesmo intervalo de tempo. A única outra aplicação em execução era a comunicação com o servidor C&C (mascarada no processo do navegador).

que foi encontrado no seu computador material que viola as leis do país (por exemplo, violação dos direitos de autor, pornografia infantil, etc.). Ao mesmo tempo, o utilizador foi convidado pela 'polícia' a pagar a quantia necessária, após o que o computador será desbloqueado e todo o assunto será 'resolvido'.

Spam - pode basicamente ser entendido a dois níveis. Num **sentido restrito, é a** difusão em massa de mensagens não solicitadas, geralmente de natureza publicitária através da Internet, e na maioria das vezes através da comunicação electrónica. Num **sentido lato,** spam são todas as mensagens não solicitadas recebidas, e portanto também mensagens contendo vírus, cavalos de Tróia, etc. . [17]

Spam - é uma **mensagem enviada electronicamente, em massa e especialmente sem um pedido.**

Fraude - O spam contendo conteúdo criminoso ou outro conteúdo fraudulento é referido como **fraude**. As burlas constituem agora uma proporção significativa de spam e o seu objectivo é, geralmente utilizando engenharia social, ganhar a confiança do utilizador e forçá-lo a realizar certas acções necessárias

Scam 419 - esta é a designação para e-mails, mais conhecidos como **Cartas Nigerianas.** Estes esquemas são um exemplo da transferência do crime comum (fraude) do mundo real para o mundo virtual.

Hoax(ficção, piada, boato de imprensa) - é outra forma de spam ou hoax. O rótulo "hoax" é utilizado para mensagens em cadeia (como por exemplo: "*passe-o*", "*se não enviar isto a outras 20 pessoas.... tornar-se-á...*" etc.) que contenham informações distorcidas, falsas, enganosas ou outras informações falsas. O embuste inclui frequentemente avisos de ataque, descrições de ameaças, pedidos de ajuda, apelos, petições, declarações de celebridades, cartas em cadeia de boa sorte, mensagens engraçadas, imagens e vídeos em apresentações, brincadeiras com gatos e outros animais, etc.

Ofertas fraudulentas - esta é uma forma muito eficaz de fraude. As ofertas fraudulentas podem ser enviadas em massa ou de uma forma direccionada. Hoje em dia, tais ofertas são enviadas não só por correio electrónico, mas também através de todo o tipo de mensagens instantâneas, redes sociais, sites de leilões, etc.

Phishing- é mais comummente definido como comportamento fraudulento ou enganoso destinado a obter informações do utilizador tais como nome de utilizador, palavra-chave, número de cartão de crédito, PIN, etc.

Phishing - num **sentido restrito, o phishing** é uma acção que requer que o utilizador visite um site fraudulento (exibindo, por exemplo, um site bancário online, loja online, etc.) e depois preencha 'informação de login' ou a informação é solicitada directamente (por exemplo, ao preencher um formulário, etc.). **Phishing - num sentido lato, o** phishing pode ser definido como qualquer comportamento fraudulento concebido para incutir confiança num utilizador, reduzir a sua vigilância ou forçá-lo a aceitar um cenário preparado antecipadamente pelo atacante.

Pharming[18] - é uma forma mais sofisticada e perigosa de phishing. É um ataque ao servidor DNS (Domain Name System), que traduz um nome de domínio para um endereço IP. O ataque ocorre quando um utilizador digita o endereço de um servidor web a que pretende aceder num navegador web.

A pesca com lanças é uma forma de ataque de phishing, mas a diferença é que a pesca com lanças é um ataque precisamente direccionado, em oposição à pesca com lanças, que é um ataque (aleatório) bastante comum. O alvo do ataque - é geralmente um grupo, organização ou indivíduo específico, e especificamente a informação e dados contidos dentro dessa organização (por exemplo, propriedade intelectual, dados pessoais e financeiros, estratégias empresariais, informação classificada, etc.).

Vishing[19] - refere-se ao phishing telefónico, em que o atacante usa uma técnica de engenharia social e tenta extrair informações sensíveis do utilizador (por exemplo, números de conta, detalhes de login - nome e senha, números de cartões de pagamento, etc.). O atacante tenta deliberadamente falsificar a identidade do utilizador. Os atacantes apresentam-se frequentemente como representantes de bancos reais ou outras instituições, a fim de suscitar o mínimo de suspeitas possíveis no utilizador. O Vishing é utilizado na telefonia VoIP (Voice over Internet Protocol).

[17] Para classificar spam, cf. forexample GONZÁLES-TALAVÁN, Guillermo. Um simples filtro de spam SMTP configurável: Greylists. *Computers& Security*, 2006, vol. 25, No. 3, pp. 229-236.

[18] É uma combinação das palavras farmingi **phreaking**.

[19] É uma combinação das palavras 'voz' e 'phishing'.

Smishing[20] - funciona com base num princípio semelhante ao vishing ou phishing, mas utiliza mensagens SMS para distribuir mensagens. Smishing é essencialmente uma tentativa de levar o utilizador a pagar uma quantia de dinheiro (por exemplo, ligar para uma linha gratuita, enviar um SMS a um doador, etc.) ou clicar em ligações URL suspeitas. Se o utilizador visitar tal URL, é redireccionado para uma página que explora alguma vulnerabilidade no sistema informático, ou o utilizador é solicitado a fornecer informações sensíveis ou malware.[21]
Business Email Compromise[22] - é um tipo de ataque fraudulento em que um atacante faz-se passar por um executivo (geralmente o CEO) e tenta fazer com que um empregado, cliente ou fornecedor entregue dinheiro ou informação sensível ao atacante.
CEO FRAUD (uma forma de fraude BEC) - Os atacantes apresentam-se como CEO de uma empresa ou outro executivo da empresa e enviam um e-mail falso aos empregados com a capacidade de enviar transferências electrónicas e instruí-los a enviar fundos aos atacantes.
INVOICE (uma forma de fraude BEC) - uma empresa, que frequentemente tem uma relação de longa data com um fornecedor, é solicitada a transferir fundos para pagar uma factura para outra conta falsa. O agressor contacta normalmente a vítima por correio electrónico ou telefone. Um ataque via correio electrónico tem normalmente um código fonte (cabeçalho) e uma linha de assunto do pedido, o que o faz parecer muito semelhante a um pedido legítimo.
ACCOUNT COMPRISE (uma forma de fraude BEC) - Este ataque é semelhante ao da Factura Falsa. O atacante utiliza a conta de e-mail de um empregado (pirateada ou falsificada) e depois envia um e-mail aos clientes para os informar de que houve um problema com o seu pagamento e que precisam de reenviar o mesmo para outra conta.
Business Executive and Attorney Impersonation (uma forma de fraude BEC) - as vítimas são contactadas por atacantes que se fazem passar por advogados ou representantes de escritórios de advocacia. O agressor pede uma grande transferência de fundos para ajudar a resolver uma disputa legal ou pagar uma factura pendente. O agressor tenta convencer as vítimas de que a transferência é confidencial e sensível ao tempo, pelo que é menos provável que o funcionário tente confirmar se devem transferir fundos.
DATA THEFT (uma forma de BEC scam) - Um tipo de BEC que não visa a transferência directa de dinheiro. As vítimas típicas deste ataque são os departamentos / empregados financeiros ou de RH. O agressor pede-lhes que enviem dados muito sensíveis para a sua conta. A engenharia social é utilizada e o ataque de roubo de dados pode ser o ponto de partida para os ataques BEC acima mencionados, orientados para a transferência financeira.
Sítios Web (empresas) fraudulentos - Na Internet pode encontrar muitas actividades ou sítios Web[23] apresentando prémios surpreendentes ou oferecendo vários bens a preços muito acessíveis. Os atacantes utilizam engenharia social e confiam principalmente na desconfiança e no descuido das pessoas. As próprias actividades do agressor podem então normalmente assumir duas formas.
Hacking - é agora visto pejorativamente pelo público como qualquer acção de uma pessoa para obter acesso ilegal ao sistema ou computador pessoal de outra pessoa.[24]
Chapéus brancos - Chapéus brancos: são hackers que se infiltram num sistema explorando vulnerabilidades na segurança do sistema precisamente para detectar essas vulnerabilidades e criar tais mecanismos e barreiras que devem impedir tais ataques. Muitas vezes, são empregados ou colaboradores

[20] É uma combinação das palavras 'SMS' e 'phishing'.

[21] Por exemplo, o Xshqi- *Android Worm no Dia dos Namorados chinês.* [online]. [citado 14.8.2016]. Disponível a partir de: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
Selfmite- *O verme SMS do Android Selfmite está de volta, mais agressivo do que nunca.* [online]. [citado 14.8.2016]. Disponível em: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

[22] A fraude BEC é também conhecida como "fraude do CEO" ou "Man-in-the-Email".

[23] Na maioria das vezes são websites, portais de publicidade, mas também podem ser contas nos meios de comunicação social, etc.

[24] Para mais detalhes ver, por exemplo, GRIFFITHS, Mark. Criminalidade Informática e Hacking: uma questão séria para a Polícia? *The Police Journal,* 2000, vol. 73, no. 1, pp. 18-24.
YAR, Majid. Computer Hacking: Apenas mais um caso de Delinquência Juvenil? *The Howard Journal*, 2005, vol. 44, no. 4, pp. 387-399.

externos de empresas conceituadas que operam no campo da tecnologia da informação. A sua intrusão num sistema não causa danos ou outros danos aos utilizadores; pelo contrário, em muitos casos, alertam o administrador de tal sistema infectado para vulnerabilidades de segurança. As suas actividades são essencialmente de natureza não destrutiva.

Chapéus pretos - Chapéus pretos: basicamente o oposto dos hackers de chapéus brancos. A sua motivação é tentar causar danos ou outros danos ao utilizador de um sistema infectado, ou obter propriedades ou outras vantagens. Para além de conseguirem efectivamente uma violação do sistema pirateado, outro elemento criminoso é evidente nas suas acções.

Chapéus cinzentos - chapéus **cinzentos:** esta é a zona cinzenta dos hackers, ou seja, pessoas que não se perfilaram na direcção destes dois grupos. Ocasionalmente podem violar alguns direitos de outros ou princípios morais, mas as suas acções não são ditadas principalmente por um desejo de causar danos, como é o caso dos chapéus pretos.

O termo **cracking** - está associado ao termo hacking, por vezes até estes termos são confundidos pelo público ou nos meios de comunicação social. Em termos de conteúdo, o termo cracking significa quebrar ou contornar os elementos de protecção de um sistema informático, programas ou aplicações, com a intenção da sua posterior utilização não autorizada.

Cracking de senha - é uma forma de cracking utilizada para estabelecer uma senha de acesso a um sistema informático, sistema ou programa licenciado. No que diz respeito ao cracking de direitos de autor, o cracker geralmente cria um keygen ou crack[25] , o que permite a utilização subsequente do programa. Tais programas modificados são geralmente disponibilizados em fóruns warez ou redes P2P.

Pirataria na Internet - é um termo geral que abrange crimes que violam os direitos de propriedade intelectual (muitas vezes limitado aos direitos de autor). É apenas com a expansão dos sistemas informáticos e especialmente com o advento da Internet que podemos falar de pirataria em massa como uma das formas mais generalizadas de cibercriminalidade.

Direito de propriedade intelectual - é um bem intangível, um bem chamado material, que é **o resultado da actividade criativa de uma pessoa.** Este direito é **independente do substrato material** (pode portanto ser utilizado em qualquer altura e em qualquer parte do mundo) desde que seja **único, não repetitivo e suficientemente original.**

Direitos de autor - protege, por exemplo, obras literárias e artísticas originais, composições musicais, emissões televisivas, programas informáticos, bases de dados, criações publicitárias, multimédia, etc.

Direitos industriais - proteger, por exemplo, patentes sobre invenções, desenhos, modelos industriais, marcas, origens geográficas, etc.

Pirataria de software - violação dos direitos de autor em relação a programas informáticos.

Pirataria audiovisual - violação dos direitos de autor em obras audiovisuais - música e cinema.

A difusão de uma obra por correio electrónico (um caso de violação dos direitos de autor no ciberespaço) - é a forma mais fácil de divulgar pequenos ficheiros (especialmente obras literárias ou gráficas protegidas por direitos de autor).

Interferência com programas de computador (um caso de violação dos direitos de autor no ciberespaço) - para derrotar os meios técnicos do proprietário dos direitos de autor para impossibilitar cópias de tais programas protegidos (o chamado crack)

Divulgação de uma obra utilizando dados (um caso de violação dos direitos de autor no ciberespaço) - suportes directamente entre utilizadores (empréstimo e subsequente cópia de dados de DVD, HDD, etc., venda de suportes e outros).

Gravação directa durante uma sessão e subsequente distribuição da gravação (por exemplo, gravação de uma obra cinematográfica directamente do ecrã) - gravação de um caso de violação dos direitos de autor no ciberespaço) - gravação.

Demonstrações não autorizadas de obras audiovisuais (um caso de violação dos direitos de autor no ciberespaço) - a aquisição efectiva de uma obra informática. Um programa de computador é

[25]**Keygen-** Gerador de **chaves.** Um programa que gera números de série ou outros dados. **Crack** - Um programa utilizado para remover ou reduzir a funcionalidade de elementos de protecção de outro programa.

particularmente protegido e não é possível fazer cópias de tal obra, mesmo para uso pessoal, sem o consentimento dos titulares dos direitos de autor ao abrigo da lei dos direitos de autor.
Utilização de um programa de computador em violação de uma licença.
A colocação de uma obra (quer audiovisual ou software) no ciberespaço (**uploading**) constitui distribuição da obra na acepção da lei de direitos de autor e (a menos que autorizada pelo autor ou outra pessoa autorizada) pode ser punível. **É também uma utilização não autorizada de uma obra para publicar uma ligação a um local no ciberespaço a partir do qual a obra pode ser obtida.**
Warez - é, em termos simples, **uma forma de pirataria de software** em que a tecnologia da informação é apenas um meio de acelerar a distribuição de cópias ilegais de obras protegidas por direitos de autor através da Internet. Os fóruns Warez são actualmente utilizados principalmente para descarregar fendas e keygen, bem como programas completos modificados, filmes e música.
Sniffing - é um método de intercepção ilegal de dados passando por uma rede informática durante a comunicação entre o serviço fornecido e um sistema informático utilizando um **sniffer.**[26]
DoS - representa a ***negação de serviço***. É uma forma de ataque a um serviço (Internet) que visa desactivar ou degradar o desempenho de equipamento técnico infectado.[27] Este ataque é implementado através da inundação do sistema informático comprometido (ou elemento de rede) com pedidos repetidos para que o sistema informático tome medidas. Este ataque também pode ser implementado através de canais de informação de inundação entre o servidor e o computador do utilizador ou através de recursos do sistema sem inundação.
Negação de Serviço Distribuída (DDoS) - o sistema informático alvo é sobrecarregado pelo **envio de pacotes de múltiplos sistemas informáticos em diferentes locais, o que dificulta a defesa e a identificação do atacante**. Este tipo de ataque tem sido utilizado, por exemplo, contra Yahoo! Inc, comércio electrónico, etc.[28]
DRDoS (Distributed Reflected Denial of Service), é um ataque de DoS distribuído falsificado que utiliza o que é conhecido como mecanismo de reflexão. O ataque envolve o envio de pedidos de ligação falsificados a um grande número de sistemas informáticos, que depois respondem a estes pedidos, mas não ao iniciador da ligação, mas à vítima. Isto porque os *pedidos de ligação falsificados* têm como endereço de origem o endereço da vítima, que é depois inundada com respostas a estes pedidos.
Ping-Flood - graças ao Protocolo de Mensagem de Controlo da Internet e à ferramenta Ping (Packet Internet Groper), é possível utilizar o comando "ping" para determinar a "vida" de um sistema informático com um dado endereço IP e para detectar o tempo de resposta de tal sistema. Num ataque Ping-Flood, a vítima é inundada por um grande número dos chamados pacotes de pedido de eco ICMP, aos quais a vítima começa a responder - enviando os chamados pacotes de resposta de eco ICMP.
Inundação de recursos livres do sistema (*SYN-Flood*) - é um tipo de ataque em que o atacante tenta sobrecarregar a sua vítima com um grande número de pedidos de ligação. O atacante envia uma sequência de pacotes de comando SYN (pacotes SYN) para o sistema informático alvo (vítima), com o sistema alvo a responder a cada pacote SYN enviando um pacote SYN-ACK, mas o atacante já não responde. O sistema informático alvo espera por um reconhecimento final, um chamado pacote ACK, por parte do iniciador da ligação (o atacante) e atribuiu recursos para esta ligação, mas tem um número limitado.
Falsificação do **endereço de origem** (*IP spoofing*) - é a acção de forjar o endereço de origem dos pacotes

[26]Sniffing **é** a palavra inglesa para bisbilhotar ou espiar. Um farejador é, portanto, alguém que bisbilhotar ou espiar.

[27] Para mais detalhes, por exemplo MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO e Pedro GARCÍA-TEODORO. Avaliação de um ataque de baixa taxa de DoS contra Servidores de Aplicação. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 335-354.

CARL, Glenn, Richard BROOKS e Rai SURESH. Detecção de Negação de Serviço com Base em Ondas. *Computers & Security*, 2006, vol. 25, no. 8, pp. 600-615

RAK, Roman e Radek KUMMER. Informačníhrozby v letech 2007-2017. *revista de segurança*, 2007, vol. 14, no. 1, p. 3.

[28] Por exemplo, ataques do DoS aos sítios web da Presidência, Parlamento, ministérios, meios de comunicação social e dois bancos estónios - Estónia (2007). *A Estónia recupera de um ataque maciço de DDoS.* [em linha]. [cit. 4. 3.2010] Disponível em: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

enviados, quando um atacante que inicia uma ligação a partir da máquina A com endereço IP **a.b.c.d** insere, por exemplo, o endereço IP d**.c.b.a** como endereço de origem e o envia para o alvo B. O alvo B responde então a este endereço de origem, isto é, a resposta não é dirigida ao endereço IP a.b.c.d, mas ao endereço IP **d.c.b.a.**
O ataque Smurf - é realizado através de uma má configuração do sistema para enviar pacotes para todos os computadores ligados à rede informática através de um endereço de difusão
Divulgação de tipos de pornografia proibidos - trata-se principalmente da divulgação de material pornográfico que retrata o contacto com animais e a divulgação (ou posse) de "pornografia infantil" (material que retrata ou explora de outra forma uma criança - uma pessoa com menos de 18 anos ou uma pessoa que parece ser uma criança).
Disseminação de conteúdos odiosos e extremistas - a ofensa inclui, em particular, apoiar e promover um movimento que visa claramente suprimir os direitos humanos e as liberdades, expressar simpatia por tal movimento, pregar o ressentimento racial, étnico e nacional, religioso ou de classe ou o ressentimento de outro grupo.
Agressão - no mundo real, envolve uma tentativa de um agressor de prejudicar, humilhar, ridicularizar ou insultar outra pessoa, quer física ou mentalmente
Cyberbullying - depois move 'bullying clássico' para o mundo virtual e permite ao agressor utilizar ferramentas e recursos que podem ter um impacto muito maior na vítima do que seria o caso no mundo real.
Ciberespaço - é um acto de manipulação psicológica de uma pessoa (geralmente utilizando engenharia social), realizado através da Internet ou de tecnologias de informação e comunicação (por exemplo, telemóveis, etc.). O objectivo do ciberespaço é criar uma falsa confiança na vítima e assim induzi-la a encontrar-se pessoalmente. O resultado de um tal encontro pode ser qualquer ataque físico, sexual ou outro ataque à vítima. Tanto as crianças como os adultos podem ser vítimas de cibercontrolo. De acordo com as estatísticas, as raparigas dos 13 aos 17 anos são as vítimas mais comuns.
Sexting - é uma forma de comportamento perigoso, especialmente no ambiente das redes sociais, é conhecida como sexting. O termo sexting foi cunhado a partir de uma combinação das palavras sexo e texturização, o que torna o seu significado claro. É a disseminação electrónica de mensagens de texto, fotografias ou vídeos com conteúdo sexual. Este material sexualmente explícito pode ser colocado em redes sociais ou outros repositórios de dados directamente pelos próprios autores ou por outro utilizador que tenha obtido acesso a tal material. Isto é feito na maioria das vezes através do upload voluntário de ficheiros com conteúdo sexual, que são descarregados pelos próprios remetentes.
Cyberstalking é um composto das palavras cyberstalking e stalking. Originalmente, a palavra perseguição era utilizada por caçadores que caçavam caça e significava seguir a caça até ser morta.
Cyberstalking é a acção de contactar repetidamente a vítima, por exemplo, através de mensagens de texto, e-mails, chamadas telefónicas, VoIP, mensagens instantâneas, etc. As acções do agressor normalmente aumentam e normalmente suscitam preocupações sobre a privacidade, saúde ou vida da vítima.
Os ciberstaladores caracterizam-se pela sua persistência e natureza sistemática, e não é raro um ciberstalador criar múltiplas identidades falsas, que utilizam para contactar a vítima. Um ciberinstalador pode também demonstrar o seu poder e força, por exemplo, publicando informações sobre a vida da vítima, que pode obter de várias fontes online.
Roubo de identidade - é um ataque em que uma identidade virtual é roubada[29] , ou é a tomada de controlo (permanente ou temporária) dessa identidade. O motivo do atacante pode ser um ganho financeiro, mas também outros benefícios relacionados com o facto de o atacante estar a agir em nome de outra pessoa, por exemplo, acesso a informações sobre outras pessoas, acesso a dados da empresa, etc.
APT - representa uma ameaça avançada e persistente.
APT - é um ciberataque sustentado e sistemático centrado num sistema informático alvo ou nas TIC de uma

[29] Uma identidade virtual refere-se a qualquer identidade ou avatar utilizado por uma pessoa para interagir no ciberespaço (por exemplo, e-mail, conta de rede social,jogos, vários mercados online, sistema informático, etc.) Não importa se a identidade virtual é real ou falsa, ou seja, se representa uma pessoa real ou se é uma identidade completamente criada artificialmente e sem base real.

organização alvo. São utilizadas diferentes técnicas e recursos relativamente grandes para tal ataque, e normalmente alvos secundários (por exemplo, sistemas informáticos, tais como ataques repetidos de DoS ou outros ataques) podem ser atacados para distrair a atenção do alvo principal (infiltração da empresa por malware), que é depois atacado.
Ciberterrorismo - é essencialmente a má utilização das TIC (incluindo a Internet) como meio e ambiente para levar a cabo um ataque. Como um ataque terrorista clássico convencional, é uma actividade planeada, geralmente motivada política ou religiosamente e levada a cabo por pequenas estruturas organizadas em vez de militarmente. O objectivo destes grupos é principalmente o de influenciar a opinião pública. Devido à rápida proliferação das tecnologias de informação e comunicação em todo o mundo, o ciberterrorismo representa uma ameaça significativa e é cada vez mais utilizado por grupos terroristas.[30]
Terrorismo dos meios de comunicação social - o uso indevido planeado dos meios de comunicação social e de outras armas psicológicas para influenciar as opiniões da população no seu conjunto ou das populações visadas.

Citações chave de material em linha:

- A fim de compreender os ciberataques e a cibercriminalidade, é necessário conhecer a terminologia básica directamente relacionada com o campo escolhido. Este capítulo apresenta termos técnicos bem como jurídicos seleccionados.
- É impossível encontrar uma área de actividade humana em que a tecnologia informática, ou melhor, a tecnologia da informação ou da comunicação, não seja directa ou indirectamente utilizada.
- Pode argumentar-se que, em **princípio, é impossível encontrar uma área de actividade humana em que a tecnologia informática, ou um sistema de informação ou tecnologia de informação ou comunicação, não seja directa ou indirectamente utilizada.**
- A Decisão-Quadro 2002/584/JAI do Conselho da UE sobre o Mandado de Detenção Europeu define "**criminalidade informática"** como a conduta dirigida contra um computador ou conduta em que um computador é o meio para cometer uma infracção penal. A definição de cibercrime baseia-se também na redacção do Mandado de Detenção Europeu.
- Nas convenções internacionais, o termo "**cibercrime**" é mais frequentemente utilizado para se referir a crimes cometidos através das tecnologias da informação, e a utilização do termo foi também transferida do campo normativo para o vocabulário profissional. O conceito de cibercrime é de natureza semelhante aos termos *"crime violento", "crime juvenil", "crime económico", etc. Tais termos referem-se a grupos de crimes que têm algum factor comum, como o método de execução, a pessoa do perpetrador (pelo menos em termos de tipo), etc. na sua essência, pode ser uma mistura muito diversificada de crimes, ligados por um factor comum (computador, programa, dados).*[31]
- Ao definir o conteúdo do conceito de **cibercrime**, é importante perceber que à medida que aumenta a possibilidade de utilização de dispositivos TIC, aumenta também a possibilidade de os utilizar (utilização indevida) para cometer um crime. Por conseguinte, em princípio, não existe uma definição universal e universalmente aceite que afecte plenamente o âmbito e a profundidade do conceito.
- "Actividade criminosa em que um computador aparece de alguma forma como um agregado de hardware e software (incluindo dados), ou apenas alguns dos seus elementos podem aparecer, ou por vezes um número maior de computadores isolados ou ligados em rede informática, e quer como objecto de interesse dessa actividade criminosa (excepto para essa actividade criminosa cujos objectos são os dispositivos descritos tratados como bens imóveis), ou como um ambiente (objecto), ou como um instrumento de actividade criminosa (Ver Criminalidade Informática)".

[30] JIROVSKÝ, Václav. *Kybernetickákriminalitanejen o hacking, cracking, virech a trojskýchkoních bez tajemnic.* Praga: Grada, 2007, p. 129

[31]Smejkal, Vladimír. *Kybernetickákriminalita.* Plzeň: AlešČeněk, 2015, p. 19.

- ***Crime informático / Cibercrime -*** "Um crime cometido utilizando ou directamente relacionado com um sistema de processamento de dados ou rede informática".
- Nos termos mais gerais, o cibercrime pode ser definido como um **comportamento dirigido contra um computador, ou uma rede informática, ou como um comportamento em que um computador é utilizado como uma ferramenta para cometer um crime.** Um critério indispensável para aplicar a definição de cibercrime é que a rede informática, ou ciberespaço, seja então o ambiente em que a actividade tem lugar.
- Ao definir o conceito de cibercrime, é primeiro necessário **definir o conceito de crime em geral.** No que diz respeito à utilização de sistemas de informação, tecnologia informática ou dispositivos de comunicação, há uma série de actividades que são certamente indesejáveis mas não puníveis ao abrigo do direito penal, embora possam ser muito perigosas (prejudiciais) para a sociedade.
- Na definição do conceito de criminalidade (e esta definição pode ser dada de vários pontos de vista - sociológico, forense, etc.), baseamo-nos na definição de criminalidade como uma **compilação de todos os actos que se qualificam no âmbito do elemento objectivo regulado pelo direito penal.** Com **base nesta definição, a criminalidade não inclui, portanto, tais actos que não satisfaçam qualquer elemento objectivo do crime, ou seja, nem sequer um delito ou outra infracção administrativa.** Esta definição do conceito de criminalidade é relativamente precisa e pode ser aplicada no domínio das tecnologias da informação e da comunicação.
- O cibercrime, portanto, é um crime que envolve os meios da tecnologia da informação e da comunicação:
  a) ***utilizado como instrumento para cometer um crime,***
  b) ***são o alvo de um ataque do perpetrador*, e esse *ataque* é** uma infracção penal,
- **Sob o termo cibercrime, os crimes enquadram-se em três categorias diferentes:**
  - **infracções em que o objecto individual que caracteriza a finalidade é directamente a protecção do sistema informático, dos seus dispositivos e componentes contra certos tipos de ataques ou os legítimos interesses das pessoas na utilização desimpedida destes dispositivos técnicos,**
  - **crimes que são cometidos através das tecnologias da informação e comunicação,**
  - **outras infracções qualificadas que não se enquadram na primeira ou segunda categoria, mas que, no caso em questão, também podem ser cometidas utilizando tecnologias de informação e que satisfazem a definição acima referida, porque podem ser utilizados procedimentos de detecção semelhantes para as detectar e esclarecer como os utilizados para investigar infracções na primeira e segunda categorias (por exemplo, pareceres de peritos com objectivos semelhantes).**
- **<u>Classificação de acordo com a Convenção sobre o Cibercrime e de acordo com o Protocolo Adicional.</u>**

  A Convenção sobre o Cibercrime divide o cibercrime em quatro categorias:

  1. **Ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos**;
  2. **Crime informático**;
  3. **Infracções relacionadas com o conteúdo**;
  4. **Infracções relacionadas com a violação dos direitos de autor e direitos conexos**.

- Um protocolo adicional define então outros cibercrimes:
  1. **Divulgação de material racista e xenófobo através de sistemas informáticos***;*

2. **Uma ameaça por motivos raciais e xenófobos***;*
3. **Insulto de motivação racista e xenófoba***;*
4. **Negar, minimizar grosseiramente, perdoar ou justificar o genocídio ou crimes contra a humanidade.**

- **<u>Classificação do Comité de Peritos em Cibercriminalidade</u>**

De acordo com o Estatuto de 2000 do Comité de Peritos em Cibercriminalidade do Conselho da Europa, a cibercriminalidade pode ser dividida em:

1. **De acordo com a posição do computador no momento da infracção:**
   - *alvo de ataque;*
   - *meios* (ferramenta) *de ataque.*
2. **Consoante o tipo de acto:**
   - *infracções tradicionais* (tais como contrafacção, etc.)
   - *novas infracções* (tais como phishing, DDoS, etc.)

- **<u>Classificação de acordo com a eEurope+</u>**

  O documento dividiu o crime informático em:

1. **Ofensas contra a privacidade**
   - Recolha, armazenamento, modificação, divulgação e divulgação ilegais de dados pessoais.
2. **Crime de conteúdo informático**
   - Pornografia infantil, racismo, incitamento à violência, etc.
3. **Crimes económicos**
   - Acesso não autorizado, sabotagem, hacking, transmissão de vírus, espionagem informática, falsificação informática e fraude.
4. **Infracções de propriedade intelectual**[32]

- **<u>Classificação do crime informático segundo a criminologia</u>**

  Porada a Konrád[33] divide o cibercrime em cinco grupos básicos.

1. **Interferência não autorizada com a introdução de dados**
   - alterar o documento de entrada para processamento informático,
   - criação de um documento contendo dados falsos para tratamento posterior por um computador,
2. **Alterações não autorizadas aos dados armazenados**
   - manipulação de dados, manipulação não autorizada de dados e posterior regresso à normalidade,
3. **Instruções não autorizadas para operações informáticas**
   - instrução directa para executar a operação ou instalar software que executa a operação automaticamente,
4. **Intrusão não autorizada em computadores, no sistema informático e nas suas bases de dados**

[32]Mais detalhes: JIROVSKÝ, Václav. *Kybernetickákriminalitanejen o hacking, cracking, virech a trojskýchkoních bez tajemnic.* Praga: Grada, 2007, p. 92

[33]Mais detalhes: STRAUS, Jiří et al. *Kriminalistickámetodika*.Plzeň: AlešČeněk, 2006, pp. 272-274

- acesso informativo a uma base de dados, sem utilização de informação,
- utilização não autorizada de informações para uso pessoal,
- alteração, destruição ou substituição de informação por outros,
- intercepção" ilegal e registo do tráfego de comunicações electrónicas.

5. **Ataque ao computador, software e ficheiros e dados de outra pessoa em bases de dados**
   - desenvolvimento de programas de ataque,
   - a introdução de um vírus no software informático,
   - infecções com vírus ou outros programas.

- **<u>O foco da Europol em certos tipos de cibercriminalidade por grau de dano</u>**

A Europol adere à Convenção sobre o Cibercrime e cumpre a divisão das infracções nela contidas. Para apoiar a luta contra a cibercriminalidade e ajudar os Estados-Membros, foi criado o Centro Europeu de Cibercriminalidade (EC3) no seio da Europol[34] . Esta equipa definiu claramente o seu âmbito de acção na luta contra a cibercriminalidade e identificou as três áreas seguintes (pontos focais - PFs) com que lida:

FP TERMINAL - Fraude de pagamento. Grupo dedicado à prestação de apoio em matéria de fraude em linha.

FP Cyborg - Crimes de alta tecnologia. Um grupo que lida e presta apoio a vários ataques cibernéticos que afectam infra-estruturas críticas[35] e sistemas de informação. Em particular, estes incluem ataques tais como malware, resgate, hacking, phishing, roubo de identidade, etc.

---

[34] *Combate ao cibercrime na era digital.* [em linha]. [citado 7.5.2018]. Disponível em: https://www.europol.europa.eu/ec3.

[35] Relativamente à definição do conceito de infra-estruturas críticas, na República Checa (no caso do ciberespaço) deve começar com a Lei sobre Segurança Cibernética e Alterações a Leis Relacionadas (Lei sobre Segurança Cibernética). A seguir referida como a Lei de **Segurança Cibernética** ou **AoCS.** No artigo 2(b), esta lei define o conceito de infra-estrutura de informação crítica e um elemento ou sistema de infra-estrutura crítica.
A definição do termo "infra-estrutura de informação crítica" baseia-se na legislação que rege a área da gestão de crises. A infra-estrutura de informação crítica é uma parte da infra-estrutura crítica, que é definida pela Lei n.º 240/2000 Coll. sobre gestão de crises e alterações a certas leis (a Lei de Gestão de Crises), tal como alterada (doravante referida como a Lei de Gestão de Crises). Para ser considerado como uma infra-estrutura de informação crítica, um sistema ou serviço de informação específico e uma rede de comunicações electrónicas devem satisfazer os critérios de definição de infra-estrutura crítica, bem como o elemento de infra-estrutura crítica definido na Lei de Gestão de Crises, e os critérios transversais e sectoriais definidos no Regulamento do Governo n.º 432/2010 Coll. sobre os critérios de definição do elemento de infra-estrutura crítica.
A Secção VI introduz critérios da indústria para definir um elemento crítico da infra-estrutura desde a eficácia da Lei e da segurança cibernética. "*Sistemas de comunicações e de informação", G: segurança cibernética.* Foram aqui estabelecidos critérios específicos para a definição de um determinado sistema de informação, serviço ou rede de comunicações electrónicas como um elemento crítico de infra-estrutura de informação.
No entanto, esta definição só se aplica à área da segurança cibernética. Em geral, **as infra-estruturas críticas podem ser definidas da seguinte forma**:

1. Infra-estrutura crítica significa um elemento de infra-estrutura crítica ou um sistema de elementos de infra-estrutura crítica, cujo funcionamento teria um impacto significativo na segurança do Estado, na satisfação das necessidades básicas de vida da população, na saúde humana ou na economia do Estado.
2. Elemento de infra-estrutura crítica significa um edifício, instalação, ferramenta ou infra-estrutura pública designada de acordo com os critérios transversais e sectoriais, que estão estabelecidos no Regulamento Governamental n.º 432/2010 Coll. sobre Critérios de Designação de Elementos de Infra-estruturas Críticas.
3. O critério transversal para a designação de um elemento de infra-estrutura crítico é o aspecto de
   (a) baixas com um limiar de mais de 250 mortos ou mais de 2.500 pessoas com hospitalização subsequente por mais de 24 horas,
   (b) um impacto económico com um limiar de perda económica no país de mais de 0,5% do produto interno bruto, ou
   (c) Impacto na sociedade com um limiar de redução significativa na prestação de serviços essenciais ou outras

Gémeos FP - Exploração Sexual Infantil. Um grupo que se ocupa e dá apoio na investigação do abuso sexual de crianças.

- **<u>Classificação do cibercrime de acordo com a sua "relação" com o ambiente digital</u>**

  Com o desenvolvimento do cibercrime como tal, surgiu nos últimos anos uma opinião que postula a possibilidade de ver o cibercrime como um acto que pode ser descrito como 'puro' ou 'verdadeiro' cibercrime.

  De acordo com a divisão acima referida, seria então possível compreender o cibercrime como tal:

  - Conceito estreito ("puro" cibercrime);
  - Conceito amplo (comportamento criminoso "ordinário" num novo ambiente).

- **O ataque cibernético**[36] pode ser definido como **qualquer comportamento ilegal de um agressor no ciberespaço que seja dirigido contra os interesses de outra pessoa.** Estes actos nem sempre assumem a forma de um crime.
- O sucesso de um ataque cibernético baseia-se geralmente na violação de um dos elementos que compõem a segurança cibernética (**pessoas, processos e tecnologia**). **Estes elementos devem ser aplicados ou modificados ao longo de todo o ciclo de vida**. **Em particular, relacionam-se com a prevenção, detecção e resposta a um ataque.**
- **Um evento de cibersegurança** é "um evento *que pode causar uma violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas*". Na realidade, é um evento sem consequências negativas reais para o sistema de comunicação ou de informação em questão. No fundo, é apenas uma ameaça, mas deve ser real.
- **Um incidente de cibersegurança** é "uma *violação da segurança da informação nos sistemas de informação ou uma violação da segurança da prestação de serviços ou uma violação da segurança e integridade das redes de comunicações electrónicas como resultado de um evento cibernético*".
- Dados informáticos significa *"qualquer expressão de factos, informações ou conceitos de uma forma adequada ao processamento num sistema informático, incluindo um programa capaz de levar um sistema informático a executar uma função".*
- Informação *"são dados que foram processados num formulário que é útil para o destinatário. Portanto, qualquer informação é informação, mas qualquer dado armazenado não se torna necessariamente informação".*

Convenção sobre a Cibercriminalidade

- **A Convenção sobre o Cibercrime e o respectivo Protocolo Adicional** devem ser mencionados em primeiro lugar, **uma vez que estes são dois dos mais importantes documentos legais** que contribuem para a protecção da sociedade contra o cibercrime, estabelecendo o quadro básico para o cibercrime ao mesmo tempo que fornecem os meios para o detectar e investigar. Serão também apresentados documentos jurídicos da UE e da CE relacionados com a cibercriminalidade
- A Convenção sobre o Cibercrime foi aprovada pelo Comité de Ministros do Conselho da Europa na sua 109ª reunião de 8th de Novembro de 2001. A Convenção sobre o Cibercrime foi aberta para assinatura a 23rd de Novembro de 2001 em Budapeste.[37] A Convenção entrou em vigor a 1st de Julho de 2004.

perturbações graves na vida quotidiana de mais de 125.000 pessoas.

[36] É necessário distinguir o conceito de um ataque informático do de um **incidente de segurança,** que constitui uma violação da segurança SI/TI e das regras estabelecidas para a sua protecção (política de segurança).

[37] Uma lista dos países que assinaram e ratificaram a Convenção sobre o Cibercrime pode ser encontrada em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D.

- A Convenção sobre o Cibercrime[38] **é constituída por um preâmbulo** e **48 artigos,** que estão divididos em 4 capítulos:

  Termos utilizados

  Medidas a tomar a nível nacional

  Parte 1 - Direito penal substantivo (artigos 2º a 13º)

  Parte 2 - Direito processual (Artigos 14-21)

  Parte 3 - Jurisdição (Artigo 22)

  Cooperação internacional

  Parte 1 - Princípios gerais (artigos 23-28)

  Parte 2 - Disposições específicas (artigos 29º a 35º)

  Disposições finais

- Um passo importante para a unificação da lei é a identificação de quatro grupos básicos de infracções (ver Capítulo II; Artigos 2-13) e a ancoragem neles de outras disposições gerais de direito penal substantivo

  Ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos. (Artigos 2-6),

  Infracções informáticas. (Artigos 7-8),

  Infracções relacionadas com o conteúdo. (Artigo 9º),

  Infracções relacionadas com a violação dos direitos de autor e direitos conexos. (Artigo 10º).

- **Protocolo Adicional 189 do Conselho da Europa à Convenção sobre Cibercriminalidade**[39] , adoptado a 28th de Janeiro de 2003.[40] , define o âmbito das infracções que não são abrangidas pela Convenção sobre a Cibercriminalidade. A Convenção sobre a Cibercriminalidade não abrange as infracções relacionadas com a divulgação de determinado "*material nocivo*".[41]

- O Protocolo Adicional é constituído por um **preâmbulo** e **16 artigos,** que estão divididos em 4 capítulos:

1. **Disposições comuns**
2. **Medidas a tomar a nível nacional**
   - Artigo 3 - Divulgação de material racista e xenófobo através de sistemas informáticos
   - Artigo 4 - Ameaças motivadas pelo racismo e xenofobia
   - Artigo 5 - Insultos com motivações raciais e xenófobas
   - Artigo 6º - Negação, minimização grosseira, apologia ou justificação de genocídio ou crimes contra a humanidade

[38] O texto completo da Convenção pode ser encontrado em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[39] *Protocolo adicional à Convenção sobre Cibercriminalidade, relativo à criminalização de actos de natureza racista e xenófoba cometidos através de sistemas informáticos* [em linha]. [citado.20.8.2016]. Disponível a partir de: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f

[40] Uma lista dos países que assinaram e ratificaram o Protocolo Adicional pode ser encontrada em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D

[41] Com excepção da pornografia infantil, que está directamente incluída no artigo 9º da Convenção sobre o Cibercrime.

3. **Relação entre a Convenção sobre Cibercriminalidade e o Protocolo Adicional**
4. **Disposições finais**

- Se quiséssemos definir o conceito de engenharia social, poderíamos dizer que se trata de influenciar, persuadir ou manipular as pessoas a fim de as obrigar a tomar uma determinada acção ou a obter deles informações que de outra forma não dariam
- No caso da engenharia social, um dos factores-chave é obter o máximo de informação possível sobre o alvo do ataque (quer seja um sistema informático, uma entidade jurídica ou um indivíduo). Muitas vezes há uma interacção prolongada com uma pessoa chave e a construção de "confiança" entre o agressor e a vítima antes do ataque, enquanto que o agressor explora normalmente o descuido, a confiança, o desejo de ajudar os outros, a preguiça, a fraqueza, o medo (por exemplo, de se meter em problemas), a irresponsabilidade, a estupidez, etc.
- Os ataques de engenharia social são geralmente realizados de três maneiras, e estes métodos são combinados:
    1. **Recolha de dados livremente** (publicamente) **disponíveis** sobre o alvo do ataque
    2. **Ataque físico** (por exemplo, o atacante finge ser funcionário de uma agência de serviços - por exemplo, um técnico de serviço de impressão, técnico de manutenção, etc.), em que o atacante tenta obter o máximo de informação possível "de dentro" da empresa, ou informação sensível sobre funcionários individuais (por exemplo, através de buscas no caixote do lixo - mergulho no contentor do lixo)
    3. **Ataque psicológico**

  Os métodos mais comuns de ataques de engenharia social incluem:

    1. **E-mail fraudulento** ou **site falso**
    2. **Chamada telefónica**
    3. **Ataque cara-a-cara**
    4. **Mergulho em contentores de lixo,** bem como "esforço de dados".
    5. **Pesquisa de websites, redes sociais, etc.** (Esta é uma fonte de dados facilmente acessível e aberta para os atacantes da engenharia social para ajudar a identificar ou verificar informações sobre um alvo potencial). **Informação pública disponível online** (por exemplo, CVs publicados online, teses, artigos, propostas, etc.) **Relatórios anuais e outra informação pública disponível sobre a empresa**
    6. **Fornecimento de publicidade ou outro material em CD, DVD ou outros suportes de armazenamento**
    7. **Deixar um portador de dados** (USB, etc.) num **local de interesse** (por exemplo, na empresa, na casa de um empregado, etc., tal portador contém, normalmente, malware)
    8. **Oferta para experimentar um serviço online** (por exemplo, oferta de armazenamento em nuvem, ou um serviço interessante de graça, etc.).
    9. **Fornecimento ou descoberta de equipamento** (sistema informático)
    10. **Técnico de serviço falso**
    11. **Outros**
- Uma botnet pode muito simplesmente ser definida como uma rede de bots ligados por software[42] , que executam alguma acção baseada num comando do 'proprietário' (ou administrador) dessa rede.

[42]**Bot** (abreviatura de robot). Este é um programa que pode executar os comandos do atacante introduzidos a partir de outro sistema informático. A forma mais comum de o fazer é infectar o computador com um vírus como um verme, um

Uma rede construída desta forma pode ser utilizada para actividades legítimas (por exemplo, computação distribuída) ou para actividades ilegais.

- Típico de **um botnet** é que se um **sistema informático alvo for infectado, esse sistema,** conhecido como 'zombie' ou 'bot', **liga-se a um servidor de controlo central** [chamado servidor de comando e controlo (C&C)]. **Todo o sistema** (contendo o zombie e o C&C) **é controlado por um atacante** (referido como botmaster ou botherder) **que controla os bots através do servidor C&C**.[43]
- Os seguintes elementos são característicos (essenciais) de uma botnet:

1. **Infra-estrutura de Comando e Controlo (C&C)**

   É uma infra-estrutura que consiste num elemento (ou elementos) de controlo e robots (controlados por sistemas informáticos).

2. **Instalação e controlo do bot**

   Isto é normalmente malware que se propaga através de uma botnet ou outros meios. O objectivo principal de tal malware é incluir outros sistemas informáticos na rede de bots. O malware explora várias vulnerabilidades em sistemas informáticos.

3. **Controlo de robots através de infra-estruturas C&C**

   Um bot é um software que opera furtivamente e utiliza canais de comunicação populares (IRC, IM, RFC 1459, etc.) para comunicar com um servidor C&C. Os novos bots tentam obter o máximo de informação possível do ambiente e promover-se a outros sistemas informáticos.

- Com base na arquitectura, é possível distinguir botnets de botnets:

1. **Arquitectura centralizada**

   Esta arquitectura é tipicamente construída sobre o princípio da comunicação cliente-servidor. Os sistemas informáticos finais (zombies/bots) comunicam directamente com o servidor C&C (o elemento de controlo central) e executam instruções e utilizam recursos deste servidor.

2. **Arquitectura descentralizada**

   É normalmente construído sobre uma arquitectura peer-to-peer (P2P). Esta arquitectura permite a partilha de recursos e comandos dentro de uma rede P2P. Na sua forma 'clássica', não existe um elemento de controlo central, o que torna este sistema mais resistente a tentativas de assumir o controlo através deste elemento de controlo

- É possível classificar uma botnet como uma estrutura de **crime como serviço** (onde **um** serviço é oferecido: **botnet-as-a-service**), ou como uma economia de malware[44] , onde fornece a plataforma técnica básica necessária para realizar uma série de ataques informáticos.

---

cavalo de Tróia, etc. Um sistema informático que é controlado remotamente desta forma é então referido como um **zombie**. No entanto, algumas fontes até se referem a um sistema informático infectado como um bot.
O bot pode recolher dados, processar pedidos, enviar mensagens, comunicar com o elemento de controlo, etc.

[43] Para mais detalhes ver PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. *Botnets: Detecção, Medição, Desinfecção e Defesa.* ENISA, 2011 [online]. [citado.17.5.2015], p. 14. Disponível em: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence
Outras definições e informações sobre botnet podem ser encontradas, por exemplo, em:
Que je para botnet a jak sešíří?[online]. [citado 15.7.2016]. Disponível a partir de: https://www.youtube.com/watch?v=ywXqDon5Xtg
Botnets: nováinternetováhrozba. [online]. [citado 15.7.2016]. Disponível a partir de: http://www.lupa.cz/clanky/botnety-internetova-hrozba/.
Válkysíťovýchrobotů - jak fungujísítěbotnets. [online]. [citado 15.7.2016]. Disponível a partir de: http://tmp.testnet-8.net/docs/h9_botnet.pdf.
Botnets. [online]. [citado 15.7.2016]. Disponível em: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6.

[44] Gestão de malwares. Mais detalhes podem ser encontrados em: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. *Botnets: Detecção, Medição, Desinfecção e Defesa.* ENISA, 2011 [online]. [citado.17.5.2015], p. 21. Disponível em: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

- **Possíveis sanções penais na Polónia**

  Acesso ilegal a um sistema (hacking) Art. 267 § 1 e 2 do Código Penal. Esta infracção é processada a pedido da vítima. É punível com uma multa, restrição da liberdade ou prisão até 2 anos.

- **Possíveis sanções penais na República Checa**
  Quanto à actividade do próprio agressor de instalar software malicioso com o objectivo de posteriormente assumir o controlo de um sistema informático, é possível avaliar este comportamento ao abrigo da **secção 230 do** Código Penal (acesso não autorizado a um sistema informático e meio de armazenamento). Se o atacante tivesse colocado o malware no sistema informático com a intenção de causar danos ou outros danos a outra pessoa ou de obter um benefício não autorizado para si ou para outra pessoa, as suas acções poderiam ser qualificadas ao abrigo do artigo 230 (2) (d) do Código Penal.

- **Possíveis sanções penais em Portugal**
  De acordo com o artigo 6(2) da *Lei sobre o Cibercrime,* é criminalizado como acesso ilegal a um ou mais dispositivos informáticos para introduzir ilegalmente qualquer programa informático, instrução executável, código ou dados destinados a serem executados ilegalmente num sistema informático. O mesmo se aplica às infracções de danos a programas informáticos ou outros dados informáticos [Interferência de Dados] (Artigo 4(3)), sabotagem informática [Interferência Ilegal] (Artigo 5(2)), e intercepção ilegal (Artigo 7(3)).
- **Malware** (um composto de software malicioso) pode ser qualquer software utilizado para interferir com o funcionamento normal de um sistema informático, adquirir informações (dados) ou ser utilizado para obter acesso a um sistema informático. O malware pode assumir muitas formas, e muitos tipos de malware são nomeados em função das actividades que executam

    1. **Adware**
    2. **Spyware**
    3. **Vírus**
    4. **Minhocas**
    5. **Cavalos de Tróia**
    6. **Backdoor**
    7. **Rootkits**
    8. **Keylogger**
    9. **Ransomware**
- O termo adware é uma abreviatura para "*software suportado por* publicidade". É a forma menos perigosa mas rentável de malware.[45] O adware exibe anúncios no sistema informático do utilizador (por exemplo, pop-ups no sistema operativo[46] ou em websites, anúncios exibidos juntamente com software, etc.).

[45] Há empresas especializadas em "pagar por instalação" (*PPI*). *O "PPI" resulta então numa pletora de acções que levam à instalação de suplementos ou outro software indesejado que (no caso menos prejudicial) lista anúncios em websites sem o conhecimento do utilizador ou insere-os onde não há anúncios no website.... **A PPI confia no facto de que aqueles que oferecem estes serviços não se importam se o utilizador quiser instalar alguma coisa**. **Recebem até US$1,50 por instalação**, pelo que é mais do que certo que as instalações fraudulentas e automatizadas são uma parte essencial do seu 'modelo de negócio'".*

[46] Um desenho destes pop-ups. Para mais detalhes, ver *Adware.* [Online]. [citado 10.8.2016]. Disponível a partir de: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

- Spyware é uma combinação das palavras inglesas '*spy*' e '*software'*. Spyware é utilizado para obter dados estatísticos[47] sobre o funcionamento de um sistema informático e enviá-los para a caixa de dados do atacante sem o conhecimento ou consentimento do utilizador. Estes dados podem também incluir informações de natureza pessoal ou informações sobre a pessoa do utilizador, bem como informações sobre websites visitados, aplicações executadas, etc.
- O spyware pode ser instalado como malware autónomo, bem como muitas vezes como parte de outro software gratuito e de outra forma perfeitamente seguro. Neste caso, a instalação e outras actividades de spyware são normalmente tratadas nos termos do EULA, e o utilizador geralmente concorda voluntariamente, sem o saber, em monitorizar a sua própria actividade.
- O spyware representa uma ameaça tanto porque envia várias informações do sistema informático do utilizador para o "atacante" (que é posteriormente processado e correlacionado com dados e informações obtidas de outras fontes)
- Há um grande número de vírus cuja finalidade é destrutiva, enquanto outros são concebidos para "se estabelecerem" no maior número possível de sistemas informáticos e depois utilizá-los para lançar um ataque direccionado. Típico destes programas é a capacidade de se espalhar entre sistemas sem intervenção do utilizador no sistema informático.
- Dependendo em que ficheiros os vírus infectam, eles podem ser divididos:
    - vírus de arranque (só infectam as partições do sistema)
    - ficheiros de vírus (apenas infectar ficheiros)
    - vírus multicomponentes (infectam tanto ficheiros como áreas do sistema)
    - Macro-vírus (aplicações de ataque que utilizam macros)
- Os chamados worms **informáticos** também são **referidos** como vírus. A razão para a associação mais estreita com vírus é que os vermes não precisam de nenhum hospedeiro, ou seja, não têm um ficheiro executável (como os vírus). Ao contrário dos vírus, que são incluídos como parte de outro programa, estes programas geralmente propagam-se separadamente. O sistema danificado é então utilizado pelo worm para continuar a enviar cópias de si mesmo a outros utilizadores através da comunicação em rede.
- **Os cavalos de Tróia** são geralmente os programas informáticos que contêm funções ocultas que o utilizador não consente ou não tem conhecimento, e que são potencialmente perigosos para a continuação do funcionamento do sistema. Tal como acontece com os vírus, estes programas podem ser agrupados com outro programa ou aplicação segura, ou podem parecer-se com um programa informático inofensivo. Os cavalos de Tróia, ao contrário dos vírus clássicos, são incapazes de se replicarem ou propagarem sem a "ajuda" do utilizador. Se activado, um cavalo de Tróia pode ser utilizado, por exemplo, para apagar, bloquear, modificar, copiar dados ou perturbar um sistema informático ou redes informáticas.
- Alguns Trojans, quando lançados sem o conhecimento do utilizador, abrem as portas de comunicação do computador, o que torna muito mais fácil para outros programas maliciosos infectar ainda mais o sistema atacado ou facilitar o controlo directo do computador infectado, dito à distância. Tais Trojans são referidos como **backdoors**.[48]
- **Rootkits -** este termo refere-se não só a programas informáticos, mas também a toda a tecnologia utilizada para mascarar a presença de malware (por exemplo, vírus informáticos ou cavalos de Tróia, vermes, etc.) num sistema infectado. Na maioria das vezes, assumem a forma de programas de

[47] Por exemplo, uma visão geral dos websites visitados, os seus endereços IP, uma visão geral dos programas instalados e utilizados, registos de downloads de ficheiros da Internet, dados sobre a estrutura e o conteúdo dos directórios armazenados no disco rígido, etc.

[48] Uma visão geral dos Trojans mais comuns, incluindo uma lista das suas funções e portas de comunicação, pode ser obtida a partir de várias páginas disponíveis na Internet. Para mais pormenores, ver, por exemplo, http://www.test.bezpecnosti.cz/full.php.

computador não muito grandes. Os Rootkits não são prejudiciais em si mesmos, mas são utilizados pelos criadores de programas maliciosos, tais como vírus, spyware, etc.[49]

- Um programa rootkit altera o comportamento de todo o sistema operativo, partes do mesmo ou aplicações adicionais de modo a que os utilizadores não tenham conhecimento da existência de programas maliciosos no seu sistema informático. Em geral, os rootkits podem ser divididos em rootkits de **sistema** (que modificam o núcleo) e rootkits de **aplicação** (que modificam a configuração da aplicação).[50]
- Um keylogger é um software que regista toques de teclas específicos num sistema informático infectado. Mais frequentemente, um keylogger é utilizado para registar detalhes de login (nome de utilizador e palavra-passe) para contas que são acedidas a partir do sistema informático. A informação obtida é então geralmente enviada ao atacante.
- O serviço de resgate será descrito em mais pormenor num capítulo separado.

Distribuição de malware

Há muitas maneiras de se entregar malware a um sistema informático alvo.

Vários métodos de propagação de malware.

Os malwares podem ser difundidos:

Meios de armazenamento portáteis

Por exemplo, utilizando CDs, DVDs, USBs, um disco externo, etc. Esta é a forma mais antiga mas ainda eficaz de distribuir malware, na qual os utilizadores passam ficheiros infectados uns aos outros ou **redes informáticas** contendo **ficheiros infectados** (partilhando tais ficheiros dentro de redes informáticas, geralmente redes P2P).

Drive-by-download

Uma das formas mais comuns de ser infectado com malware é descarregá-lo da Internet e depois executar o ficheiro, geralmente com uma extensão .exe (ficheiro executável), a partir de uma fonte desconhecida. Estes podem ser programas falsos ou falsificados (por exemplo, imitações de Flapp Bird, falsos codecs multimédia, etc.), programas utilizados para contornar a protecção dos direitos de autor (crackers, keygenes, etc.**), programas infectados reais, etc.**

- **O malware pode ser instalado em quase todos os sistemas informáticos.** Um exemplo de instalações específicas é quando o **micromalware é instalado.** Este é um código malicioso que se espalha num número relativamente pequeno de sistemas informáticos.
- **A maioria dos dispositivos Android não permite que o sistema operativo seja actualizado para a versão mais recente, que é normalmente modificado para suportar vulnerabilidades de segurança conhecidas e já tem bugs corrigidos de versões anteriores deste sistema operativo. De facto, estima-se que 77% das ameaças que atacam o sistema operativo Android poderiam ser eliminadas através da utilização da versão mais recente deste sistema operativo**
- Para dispositivos móveis, os atacantes utilizam principalmente:
    - **versão desactualizada do sistema operativo do dispositivo móvel** (vulnerabilidades conhecidas de sistemas individuais);
    - **protecção mínima do dispositivo móvel** com medidas anti-vírus;

[49]Para mais detalhes ver BALIGA, Arati, Liviu IFTODE e Xiaoxin CHEN. Contenção automatizada de ataques de Rootkits. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 323-334.

[50] Cf. RAK, Roman e Radek KUMMER. Informačníhrozby v letech 2007-2017. *revista de segurança*, 2007, vol. 14, no. 1, p. 5.

- **ignorância do utilizador** (muitos utilizadores instalam imprudentemente aplicações "a partir de uma fonte desconhecida" ou aplicações que requerem acesso e permissões excessivas dentro do dispositivo);
- **engenharia social e "ondas de interesse" em aplicações de um tipo particular.**

- **Possíveis sanções penais na Polónia**
  Violação da integridade dos dados (vírus, trojans) - 268 do Código Penal, Art. 268a do Código Penal. Esta infracção diz respeito, entre outras coisas, ao roubo de dados pessoais, à sua disponibilização a terceiros sem o consentimento do proprietário, e à sua utilização não autorizada. Existem sanções financeiras (até PLN 100.000) pela prática destes actos.
- **Possíveis sanções penais na República Checa**
  Na República Checa, um ataque utilizando malware pode ser punido ao abrigo do § **230** (Acesso não autorizado ao sistema informático e ao portador de informação) do Código Penal. A posse de malware, com a intenção de cometer uma infracção ao abrigo do §182 (Violação do segredo das mensagens transportadas) ou uma infracção ao abrigo do § 230 do Código Penal, é uma infracção ao abrigo do § 231 (Obtenção e posse de senhas de acesso a dispositivos e sistemas informáticos e outros dados deste tipo) do Código Penal. Se o objectivo do vírus fosse, por exemplo, obter informações classificadas ou apoiar um grupo terrorista, o agressor poderia, por exemplo, cometer infracções ao abrigo da **Secção 311 (Ataque terrorista), da Secção 316 (Inteligência) ou da Secção 317 (Ameaça a informações classificadas) do Código Penal na fase de preparação**.
- **Possíveis sanções penais em Portugal**
  De acordo com o Artigo 6(2) da *Lei sobre o Cibercrime,* é criminalizado como acesso ilegal criar, distribuir ou divulgar qualquer programa informático, instrução executável, código ou dados destinados a executar o acesso ilegal a um sistema informático. O mesmo se aplica às infracções de danos a programas informáticos ou outros dados informáticos [Interferência de Dados] (artigo 4(3)), sabotagem informática [Interferência Ilegal] (artigo 5(2)) e intercepção ilegal (artigo 7(3)), uma vez que o legislador português não optou por uma única disposição sobre a má utilização de dispositivos, como fez a Convenção de Budapeste (artigo 6).

Ransomware

- O grupo malware também inclui o chamado malware de extorsão, para o qual o termo "**ransomware" foi cunhado**[51] (por vezes também referido como rogueware ou scareware). Ransomware é um malware que impede ou restringe os utilizadores de utilizar correctamente um sistema informático até que o atacante receba um "resgate". O Ransomware entra frequentemente no computador de um utilizador através de malware (cavalo de Tróia ou worm) que se encontra num website ou é um anexo de correio electrónico. Uma vez que o malware se tenha 'estabelecido' em segurança no sistema informático, o seu próprio 'ransomware' é descarregado.
- **O primeiro tipo é o de resgate que restringe a funcionalidade de todo o sistema informático** e não permite que o utilizador utilize o sistema (por exemplo, impedindo o sistema operativo de arrancar ou bloqueando o ecrã do sistema). Um exemplo típico deste tipo é o '*Ransomware policial*' - ver abaixo).
- **O segundo tipo é o software de resgate, que deixa o sistema informático funcional mas bloqueia os dados do utilizador e torna-os inacessíveis.**
- Um segundo tipo de serviço de resgate, conhecido como **crypto-ransomware,** está actualmente a ser utilizado. O objectivo deste malware é encriptar o disco rígido ou tipos seleccionados de ficheiros no sistema informático. O seu principal objectivo é encriptar os ficheiros privados do utilizador, tais como imagens, documentos de texto ou folhas de cálculo, vídeos, etc.
- O surgimento maciço de resgates pode ser datado de cerca de 2011, quando um ataque de resgate começou a espalhar-se pelo mundo bloqueando o acesso à conta de um utilizador do Windows, anunciando que o computador tinha sido bloqueado pela polícia estatal.
- Diferentes versões (aparência da página) do serviço de resgate da polícia apareceram gradualmente na Europa. A primeira versão foi gravada no final de 2011, mostrou o endereço IP da ligação, a ligação ISP e a localização [onde o endereço IP do fornecedor de ligação específica (ISP) foi dado], se o utilizador tivesse uma webcam ligada, foi criada e mostrada uma imagem.
- **Desde 2013, tem havido uma mudança significativa no serviço de resgate. Os atacantes reduziram os ataques que envolveram a redução da funcionalidade de todo um sistema informático e concentraram-se principalmente no bloqueio de dados dos utilizadores.**
- O crime como um serviço tem oferecido **um resgate como um serviço** desde 2016**. O** utilizador (ou seja, o atacante) tem a possibilidade de definir o seu próprio "ransomware" de acordo com as suas ideias. Ao mesmo tempo, ele ou ela recebe instalações técnicas sob a forma de servidores C&C, carteiras de bitcoin, suporte online 24/7, etc. Um exemplo de resgate como um serviço é o software **Ransom32.**
- **Possíveis sanções penais na Polónia**
  As leis que se aplicam na Polónia são as seguintes:
  Artigo 267º Obtenção ilícita de informações
  Artigo 269a. Interferência com um sistema ou rede de TIC
- **Possíveis sanções penais na República Checa**
  Na República Checa, um ataque com malware como o resgate pode ser punido ao abrigo do § 230 (Acesso não autorizado ao sistema informático e ao portador de informação) do Código Penal. A posse de malware, com a intenção de cometer uma infracção ao abrigo do § 182 (Violação do sigilo

[51]Por exemploReventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, JigSawetc. Mais detalhes podem ser encontrados, por exemplo, em:
Ransomware. [online]. [citado 14.8.2016]. Disponível em: https://www.trendmicro.com/vinfo/us/security/definition/ransomware.

das mensagens transportadas) ou uma infracção ao abrigo do § 230 do Código Penal, é uma infracção ao abrigo do § 231 (Obtenção e posse de senhas de acesso a dispositivos e sistemas informáticos e outros dados deste tipo) do Código Penal.

No caso de resgate, é também possível aplicar as disposições do artigo 230 (3) do Código Penal quando o agressor comete tal infracção com a intenção de obter um benefício injustificado para si próprio ou para outra pessoa. Também é possível considerar a aplicação do artigo 175 (chantagem) do Código Penal quando uma pessoa é coagida a pagar um montante, ameaçando causar-lhe outros danos graves (por exemplo, através da apresentação de uma queixa criminal[52]]).

- **Possíveis sanções penais em Portugal**

  Como em quase todas as jurisdições, os ataques de resgate não são particularmente puníveis, embora tais acções possam ser processadas como extorsão. Uma alternativa, de um ponto de vista estritamente cibercrime, seria a fraude informática (artigo 221º do Código Penal), uma vez que o seu âmbito material é bastante amplo, seguindo a redacção da infracção análoga no texto da *Convenção de Budapeste* (artigo 8º).

Spam

- Do ponto de vista das tecnologias de informação e comunicação, o conteúdo do conceito de spam pode basicamente ser compreendido a dois níveis. Num sentido **restrito,** é a difusão em massa de mensagens não solicitadas, geralmente de natureza publicitária através da Internet, e na maioria das vezes através da comunicação electrónica. Num **sentido lato, spam são** todas as mensagens não solicitadas recebidas, e portanto também mensagens contendo vírus, cavalos de Tróia, etc. [53]
- Uma característica do spam é que é uma **mensagem enviada electronicamente, em massa e, acima de tudo, sem pedido.**
- O esquema 419 é a designação para e-mails, mais conhecido como **Cartas Nigerianas.** Estes esquemas são um exemplo da transferência do crime comum (fraude) do mundo real para o mundo virtual.
- Um embuste (ficção, piada, boato de imprensa) é outra forma de spam ou hoax. O rótulo "hoax" é utilizado para mensagens em cadeia (como por exemplo: "*passe-o*", "*se não enviar isto a outras 20 pessoas.... tornar-se-á...*" etc.) que contenham informações distorcidas, falsas, enganosas ou outras informações falsas. O gancho inclui frequentemente avisos de ataque, descrições de ameaças, pedidos de ajuda, apelos, petições, declarações de celebridades, cartas em cadeia de boa sorte, mensagens engraçadas, imagens e vídeos em apresentações, brincadeiras com gatos e outros animais, etc.
- Uma forma muito eficaz de fraude são as várias ofertas fraudulentas que podem ser enviadas em massa ou de uma forma direccionada. Hoje em dia, tais ofertas são enviadas não só por correio electrónico, mas também através de todo o tipo de mensagens instantâneas, redes sociais, sites de leilões, etc.

---

[52] Para o conceito de outros danos graves, ver SÁMAL, Pavel et al. *Trestnízákoník II. § 140 až 421 (Código Penal II. § 140 a 421). Komentář. (Comentário.)* 2ª Edição. Praga: C. H. Beck, 2012, pp. 1752-1753

Especificamente, "a *ameaça de causar outro dano grave pode consistir numa ameaça de danos materiais, danos graves à honra ou reputação de alguém, etc.". Outro tipo de dano grave pode consistir na instauração de um processo penal em resultado da denúncia de um crime em que o perpetrador ameaça a vítima forçando-a a fazer, a abster-se de fazer ou a tolerar algo. Ao mesmo tempo, é irrelevante se a vítima cometeu ou não o crime de que a denúncia a ameaça (cf. R 27/1982). "*

[53] Para classificar spam, cf. forexample GONZÁLES-TALAVÁN, Guillermo. Um simples filtro de spam SMTP configurável: Greylists. *Computers& Security*, 2006, vol. 25, No. 3, pp. 229-236.

- No que diz respeito à **distribuição em massa de** ofertas fraudulentas, pode-se imaginar uma série de actividades em "pirâmide" ou "avião", ofertas de trabalho favoráveis em casa[54] , métodos de valor "garantido" (com as taxas de juro mais altas), ofertas de empréstimo (com as taxas de juro mais baixas), ofertas de trabalho "grandes", etc.
- **O envio direccionado de** ofertas **fraudulentas** deve também incluir comportamentos que não sejam apenas spam, mas que sejam, por exemplo, uma combinação de licitação para um determinado tipo de bens em portais de leilão e subsequente comunicação com utilizadores que tenham aceite a licitação. Estes são conhecidos como "fraude em leilão".
- **Possíveis sanções penais na Polónia**
  Na Polónia, o envio de informação comercial não solicitada através de comunicação electrónica é considerado uma infracção e é punível com uma multa. Isto é regulado pela Lei de 18 de Julho de 2002 sobre a prestação de serviços por meios electrónicos (Dz. U. de 2002, n.º 144, item 1204):
- **Possíveis sanções penais na República Checa**
  No que diz respeito a sanções criminais para spam e spammers, estas não estão actualmente totalmente (re)resolvidas na República Checa. Não existe protecção legal nacional ou internacional contra este comportamento indesejável. Mesmo a Convenção sobre o Cibercrime não inclui uma definição de spam como um crime.
- **Possíveis sanções penais em Portugal**
- Também em Portugal, em geral, o spam em si não é considerado um crime. Contudo, de acordo com o Artigo 14(1)(f)(g)(h)(i)(j) da Lei 41/2004, sobre protecção de dados e privacidade nas comunicações electrónicas, os spammers para fins comerciais têm de pagar multas administrativas, desde um mínimo de 1.500 euros até um máximo de 50.000 euros.

Phishing

- O termo phishing é mais comummente definido como uma conduta fraudulenta ou enganosa destinada a obter informações do utilizador tais como nome de utilizador, palavra-chave, número de cartão de crédito, PIN, etc.
- Num **sentido restrito, o** phishing é uma actividade que requer que o utilizador visite um website fraudulento (exibindo, por exemplo, uma página bancária online, uma loja online, etc.) e depois preencha 'informação de login' ou a informação é solicitada directamente (por exemplo, ao preencher um formulário, etc.).
- Num **sentido lato, o** phishing pode ser definido como qualquer comportamento fraudulento que vise incutir confiança num utilizador, reduzir a sua vigilância ou forçá-lo a aceitar um cenário preparado antecipadamente pelo atacante.
- O princípio de um ataque "*clássico" de* phishing consiste geralmente no envio do chamado e-mail de phishing à vítima, que à primeira vista não suscita qualquer suspeita de que possa ser uma mensagem fraudulenta. Uma mensagem de correio electrónico deste tipo contém geralmente um link no qual o utilizador é persuadido a clicar.

[54] Por um lado, estas ofertas podem consistir de um pedido como por exemplo: "*envie-nos $10 para a nossa conta e enviar-lhe-emos instruções sobre como ganhar $8.847 por mês*". A segunda possibilidade é que estas ofertas de emprego não requerem qualquer pagamento adiantado, apenas exigem o registo do utilizador. Ao registar-se, o atacante obtém informações pessoais sobre o utilizador. Um e-mail desta empresa pode então ser enviado para o endereço de e-mail do utilizador, contendo, por exemplo, malware, etc.

- **Planear um ataque de phishing**

  Nesta fase do ataque de phishing, o alvo (grupo de utilizadores) é seleccionado e o método a ser utilizado para o ataque é escolhido. É avaliado o tipo de segurança técnica que o alvo utiliza, o risco de o atacante revelar a sua identidade, etc.

- **Criar as condições para um ataque de phishing**

  Nesta fase, a solução técnica para o ataque de phishing tem lugar. O atacante adquire listas de endereços de correio electrónico dos utilizadores a quem o correio electrónico de phishing deve ser enviado, é criada uma caixa de dados para a qual o sistema envia os dados de utilizador adquiridos, é criada uma mensagem de confiança que é depois distribuída aos utilizadores

- **Ataque de Phishing**

  O e-mail de phishing é entregue ao utilizador individual e, dependendo da qualidade do processamento deste e-mail e de outros factores (experiência do utilizador, sensibilização do utilizador para questões de phishing, software anti-phishing do alvo, etc.), o e-mail de phishing é entregue ao utilizador. Nesta fase do ataque de phishing, o utilizador encontra o e-mail de phishing pela primeira vez.

- **Recolha de dados**

  O atacante obtém dados que foram introduzidos por utilizadores individuais do sistema comprometido num ambiente de site falso

- **Retirada de fundos ou outros ganhos de um ataque de phishing**

  Utilizando os dados obtidos, o atacante acede às contas bancárias reais de utilizadores individuais e retira fundos. Ao transferir para outras contas, especialmente estrangeiras, diluindo estes fundos e utilizando outras técnicas, os fundos levantados tornam-se praticamente indetectáveis.

- **Possíveis sanções penais na Polónia**

  Violação do segredo de comunicação (sniffing) Art. 267 § 3 Código Penal. Este tipo de infracção envolve a obtenção de informação de propriedade, por exemplo, através de sniffers, ou seja, programas que interceptam dados (passwords e IDs de utilizadores).

- **Possíveis sanções penais na República Checa**

  No caso de formas combinadas de ataques de phishing, em que o malware é utilizado para infectar um computador, tal comportamento por parte do perpetrador deve também ser punido ao abrigo da **Secção 230** (Acesso não autorizado ao sistema informático e portador de informação) do Código Penal. Se o objectivo do ataque de phishing for obter uma vantagem indevida para si próprio ou para outra pessoa, as disposições do Artigo **230 (3) do** Código Penal podem também ser aplicáveis.

- **Possíveis sanções penais em Portugal**

  Uma vez que a divulgação de software malicioso é punível (artigo 6(2) da Lei sobre o Cibercrime), como mencionado, a mera criação de dados não autênticos seria considerada uma infracção de falsificação informática (artigo 3 da Lei sobre o Cibercrime). Além disso, se a finalidade de tal criação for uma intenção fraudulenta ou desonesta de obter, ilegalmente, um benefício pecuniário para si próprio ou para outra pessoa, a expensas da vítima, isto também seria considerado como fraude informática (artigo 221 § 1 do Código Penal).

Pharming

- **O Pharming**[55] é uma forma mais sofisticada e perigosa de phishing. É um ataque ao servidor DNS (DomainName System), que traduz um nome de domínio para um endereço IP. O ataque ocorre quando um utilizador digita o endereço do servidor web a que pretende aceder no seu navegador. No entanto, ele ou ela não se ligará ao endereço IP correcto do servidor web original, mas a um endereço IP diferente, forjado.
- **A caça submarina** é uma forma de ataque de phishing, mas a diferença é que a caça submarina é um ataque precisamente direccionado, ao contrário da caça submarina, que é um ataque (aleatório) bastante comum. O alvo do ataque é geralmente um grupo, organização ou indivíduo específico, e especificamente informação e dados dentro dessa organização (por exemplo, propriedade intelectual, dados pessoais e financeiros, estratégias empresariais, informação classificada, etc.).
- **Possíveis sanções penais na Polónia**
  Aplicam-se as mesmas leis que para o phishing.
- **Possíveis sanções penais na República Checa**
  O castigo para um pescador de lanças é semelhante ao castigo para o phishing. Uma organização terrorista, por exemplo, pode estar por detrás de um ataque de caça submarina. Nesse caso, a responsabilidade por uma infracção ao abrigo da **secção 311** (ataque terrorista) do Código Penal não é excluída.
- **Possíveis sanções penais em Portugal**
  A conclusão é a mesma que para o phishing em geral, incluindo a relacionada com o terrorismo.

Vishing

- O termo vishing[56] refere-se ao phishing telefónico, no qual o atacante usa uma técnica de engenharia social e tenta extrair informações sensíveis do utilizador (por exemplo, números de conta, detalhes de login - nome e senha, números de cartões de pagamento, etc.). O atacante tenta deliberadamente falsificar a sua identidade. Os atacantes apresentam-se frequentemente como representantes de bancos reais ou outras instituições, a fim de suscitar o mínimo de suspeitas possível no utilizador. O Vishing é utilizado na telefonia de Voz sobre Protocolo Internet (VoIP).

Smishing

- Smishing[57] funciona segundo um princípio semelhante ao vishing ou phishing, mas utiliza mensagens SMS para distribuir mensagens. Smishing é essencialmente uma tentativa de levar o utilizador a pagar uma quantia de dinheiro (por exemplo, ligar para uma linha gratuita, enviar um SMS a um doador, etc.) ou clicar em ligações URL suspeitas. Se o utilizador visitar tal URL, é redireccionado para uma página que explora alguma vulnerabilidade no sistema informático, ou o utilizador é solicitado a fornecer informações sensíveis ou malware.[58]

[55] É uma combinação das palavras farmingi **phreaking**.
[56] É uma combinação das palavras 'voz' e 'phishing'.
[57] É uma combinação das palavras 'SMS' e 'phishing'.
[58] Por exemplo, o Xshqi- *Android Worm no Dia dos Namorados chinês.* [online]. [citado 14.8.2016]. Disponível a partir de: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
Selfmite- *O verme SMS do Android Selfmite está de volta, mais agressivo do que nunca.* [online]. [citado 14.8.2016]. Disponível em: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-

- **Possíveis sanções penais na Polónia**
  Aplicam-se as mesmas leis que para o phishing.
- **Possíveis sanções penais na República Checa**
  As sanções penais por vishing e smishing são semelhantes às sanções por phishing.
- **Possíveis sanções penais em Portugal**
  Mais uma vez, a conclusão sobre a criminalização é a mesma que para o phishing em geral, incluindo o phishing relacionado com o terrorismo.

Compromisso de e-mail comercial

- Business Email Compromise[59] é um tipo de ataque fraudulento em que um agressor se faz passar por um executivo (geralmente o CEO) e tenta conseguir que um empregado, cliente ou fornecedor entregue dinheiro ou informações confidenciais ao agressor.
- Tanto as pequenas empresas como as grandes corporações são vítimas do esquema da BEC. A fraude do BEC está ligada a outras formas de fraude, incluindo mas não se limitando a: romance, lotaria, emprego e esquemas de contratação.
- Os atacantes da BEC dependem fortemente de tácticas de engenharia social para enganar empregados e gestores insuspeitos. Algumas das amostras de e-mails têm linhas de assunto contendo palavras como ***pedido***, ***pagamento***, ***transferência*** e ***urgente, entre outras.***

  A fraude BEC assume tipicamente uma das seguintes formas:

  1. **"esquema "CEO**

     Os atacantes fingem ser o CEO da empresa ou outro membro da equipa de gestão da empresa e enviam um e-mail falso aos funcionários com a opção de enviar transferências electrónicas e instruí-los a enviar fundos aos atacantes.

  2. **Facturas falsas**[60]

     A empresa, que frequentemente tem uma relação de longa data com o fornecedor, é solicitada a transferir os fundos para pagar a factura para outra conta falsa. O agressor contacta normalmente a vítima por correio electrónico ou telefone. O ataque por correio electrónico tem normalmente um código-fonte (cabeçalho) e uma linha de assunto do pedido, de modo a parecer muito semelhante a um pedido legítimo.

  3. **Danos na conta**

     Este ataque é semelhante ao da Factura Falsa. O atacante utiliza a conta de e-mail de um empregado (pirateada ou falsificada) e depois envia um e-mail aos clientes para os informar de que houve um problema com o seu pagamento e que precisam de reenviar o mesmo para outra conta.

  4. **Personificação de empresários e advogados**

     As vítimas são contactadas por atacantes que se identificam como advogados ou representantes de firmas de advogados. O agressor pede uma grande transferência de fundos para ajudar a resolver uma disputa legal ou pagar uma factura pendente. O agressor tenta convencer as vítimas

more-aggressive-than-ever.html

[59] A fraude BEC é também conhecida como "fraude do CEO" ou "Man-in-the-Email".

[60] O ataque também é referido como: "The Bogus Invoice Scheme", "The Supplier Swindle" e "Invoice Modification Scheme".

de que a transferência é confidencial e sensível ao tempo, pelo que é menos provável que o funcionário tente confirmar se devem transferir fundos.

5. Roubo de dados

Um tipo de BEC que não tem como objectivo a transferência directa de dinheiro. As vítimas típicas deste ataque são os departamentos/empregados financeiros ou de RH. O agressor pede-lhes que enviem dados muito sensíveis para a sua conta. A engenharia social é utilizada e o ataque de roubo de dados pode ser o ponto de partida para os referidos ataques BEC orientados para a transferência financeira.

- **Possíveis sanções penais na Polónia**

Na Polónia, isto é regulado pelo Artigo 286 (fraude), que estabelece que:

§ 1. quem, a fim de obter um lucro material, levar outra pessoa a uma disposição desvantajosa dos seus próprios bens ou dos bens de outra pessoa por meio de engano ou exploração de um erro ou incapacidade de apreender a acção pretendida, será sujeito à pena de privação de liberdade por um período compreendido entre 6 meses e 8 anos

- **Possíveis sanções penais na República Checa**

Na República Checa, é possível punir a conduta acima descrita na **Secção 209** (Fraude) do Código Penal. A fraude complementar é um enriquecimento. A criação de uma réplica do website e a aquisição de logins e palavras-passe poderiam então ser classificadas como preparação ou tentativa de infracção, nos termos do § 209 do Código Penal. Se o agressor tentasse (§ 21 do Código Penal) obter acesso não autorizado à conta de outro utilizador utilizando os dados de acesso obtidos, tal comportamento poderia também ser classificado sob **§ 230** (Acesso não autorizado a um sistema informático e a um suporte de informação) do Código Penal.

- **Possíveis sanções penais em Portugal**

Mais uma vez, tal como explicado em relação ao phishing em geral, tais actos seriam puníveis como falsificação informática (Artigo 3 da Lei sobre o Cibercrime), bem como fraude informática (Artigo 221 do Código Penal).

Hacking

- O termo hacking é actualmente entendido pejorativamente pelo público como qualquer acção de uma pessoa para obter acesso ilegal ao sistema ou computador pessoal de outra pessoa.[61] Nos meios de comunicação social em particular, o termo é geralmente utilizado para descrever qualquer atacante cujas acções são dirigidas contra a tecnologia da informação ou cujas actividades se baseiam na utilização de tal tecnologia
- Actualmente, os próprios hackers utilizam o termo hacker para pessoas que têm excelentes conhecimentos de sistemas TIC, sistemas informáticos, os seus sistemas operativos e outro software, os princípios e mecanismos das redes, e são também excelentes programadores capazes de criar o seu próprio software em muito pouco tempo.

[61] Para mais detalhes ver, por exemplo, GRIFFITHS, Mark. Criminalidade Informática e Hacking: uma questão séria para a Polícia? *The Police Journal,* 2000, vol. 73, no. 1, pp. 18-24.
YAR, Majid. Computer Hacking: Apenas mais um caso de Delinquência Juvenil? *The Howard Journal*, 2005, vol. 44, no. 4, pp. 387-399.

- **<u>Discriminação de hackers</u>**

  É a motivação para obter acesso invulgar (não necessariamente ilegal), o método para cometer tal intrusão, a sua motivação e o seu eventual tratamento dos dados obtidos, que são os factores-chave para categorizar estes indivíduos nos três grupos principais seguintes:

  White Hats *(Chapéus Brancos)* - estes são hackers que se infiltram num sistema explorando vulnerabilidades na segurança do sistema precisamente para detectar essas vulnerabilidades e criar tais mecanismos e barreiras que devem impedir tais ataques. Muitas vezes, são empregados ou colaboradores externos de empresas conceituadas que operam no campo das tecnologias de informação. A sua intrusão num sistema não causa danos ou outros danos aos utilizadores; pelo contrário, em muitos casos, alertam o administrador de tal sistema infectado para vulnerabilidades de segurança. As suas actividades são essencialmente de natureza não destrutiva.

  Black Hast *(Black Hats)*- basicamente o oposto dos hackers de chapéus brancos. A sua motivação é tentar causar danos ou outros danos ao utilizador de um sistema infectado, ou ganhar propriedades ou outras vantagens. Para além de conseguirem realmente uma violação do sistema hacked, outro elemento criminoso é evidente nas suas acções.

  Grey Hats*(Grey Hats)*- esta é a área cinzenta dos hackers, ou seja, pessoas que não se perfilaram na direcção destes dois grupos. Ocasionalmente podem violar alguns direitos de outros ou princípios morais, mas as suas acções não são ditadas principalmente por um desejo de causar danos, como é o caso dos chapéus pretos.

- **Formas de hacking**

  As actividades reais dos hackers consistem numa série de acções. As actividades típicas utilizadas pelos hackers incluem:

  1. Engenharia social
  2. Quebrar palavras-passe[62]
  3. Escaneamento de portos[63]
  4. Utilização de malware para se infiltrar num sistema informático
  5. Phishing
  6. Roteiro Cruzado de Sítios[64]

[62] Este é o processo de obtenção de uma senha para um sistema informático. As seguintes são normalmente utilizadas para decifrar palavras-passe:

- Adivinhação de senha Bruteforce (teste de senha. uma senha suficientemente forte é prevenção);
- Adivinhar uma palavra-passe com base em algum conhecimento do utilizador (obtido, por exemplo, a partir de redes sociais, etc.);
- Utilização de um dicionário de palavras-chave comummente utilizadas (ataque de dicionário);
- Solicitar uma palavra-passe ao administrador do sistema fazendo-se passar por um utilizador autorizado (O atacante imita uma palavra-passe esquecida e tenta recuperá-la).
- Interceptar palavras-passe de comunicações em rede não encriptadas ou insuficientemente encriptadas entre o sistema informático e o utilizador
- Procura de palavras-passe em ficheiros de dados armazenados pelo sistema

[63] Este é um método que detecta portas de rede abertas num sistema informático que está ligado a uma rede informática. Com base nesta descoberta, é possível determinar que serviços estão a correr no sistema informático (por exemplo, servidor web, servidor ftp, etc.). O ataque real é então centrado nos serviços em execução detectados, com base nas suas vulnerabilidades.

[64] Este é um ataque que envolve a invasão de um website. Este tipo de ataque utiliza elementos activos (scripts) num website em que é inserido código malicioso e depois oferecido à vítima.
Uma das actividades menos comuns, mas ainda mais perigosas, é a exploração de uma vulnerabilidade numa aplicação web para executar malware no browser da vítima. A vítima é então incapaz de detectar este comportamento. O código malicioso funciona da mesma forma que o resto do website, e o agressor tem a capacidade de assumir os privilégios do navegador do sistema.

7. Escutas nas comunicações

- Provavelmente, o grupo hacker mais conhecido hoje em dia é o Anónimo.

- **Possíveis sanções penais na Polónia**
  A infracção de hacking é regulada no Artigo 267§1 do Código Penal.
- **Possíveis sanções penais na República Checa**
  Como mencionado acima, há uma série de actividades ou ataques que podem ser categorizados como hacking (que vão desde o cracking de senhas a sofisticados ataques de phishing que são combinados com engenharia social e a utilização de malware).
  As acções de um hacker, que consistem unicamente em utilizar as suas capacidades para ultrapassar medidas de segurança e obter acesso a um sistema informático ou parte dele, podem ser punidas ao abrigo da Secção 230(1)(Acesso não autorizado a um sistema informático e a um suporte de informação) do Código Penal.

Rachadura

- O termo **cracking está** associado ao termo hacking, por vezes até estes termos são erradamente confundidos pelo público ou nos meios de comunicação social. Em termos de conteúdo, o termo cracking significa quebrar ou contornar os elementos de protecção de um sistema informático, programas ou aplicações, com a intenção da sua posterior utilização não autorizada.
- **Possíveis sanções penais na Polónia**
  Aplicam-se as mesmas leis que no caso de hacking

Possíveis sanções penais na República Checa

- As acções do perpetrador através das quais a protecção de um sistema ou programa informático é violada, com a intenção de obter informações e a sua subsequente utilização não autorizada, cumprem os elementos objectivos de uma infracção nos termos da Secção 230 (1) ou (2) (Acesso não autorizado a um sistema informático e a um portador de informações) do Código Penal. Se o objectivo do ataque de cracking for a obtenção de um benefício injustificado para si próprio ou para outra pessoa, as disposições do artigo 230 (3) do Código Penal podem também ser aplicáveis.
- **Possíveis sanções penais em Portugal**
  O acesso ilegal a um sistema informático é em si mesmo punível (artigo 6(1) da Lei sobre o Cibercrime). Além disso, a derrota das medidas de segurança e/ou a obtenção de uma vantagem indevida não são necessárias como elementos objectivos, sendo consideradas infracções agravantes (Artigo 6(3) e (4)).
  Como mencionado, a criação, distribuição ou divulgação ilegal de qualquer programa informático, instrução executável, código ou dados destinados a efectuar o acesso ilegal a um sistema informático é criminalizada como Acesso Ilegal (Artigo 6(2) da Lei sobre o Cibercrime), como uma infracção agravada se o perpetrador tivesse acesso a segredos comerciais ou dados confidenciais, o mesmo acontecendo no caso de obter uma vantagem indevida relevante (Artigo 6(4) da Lei sobre o Cibercrime).

Pirataria na Internet

- O termo pirataria na Internet é um termo geral que abrange crimes que violam os direitos de propriedade intelectual (muitas vezes limitado aos direitos de autor). É apenas com a expansão dos

Mais detalhes podem ser encontrados, por exemplo, em *OWASP, XSS* [online] [citado 15.7.2016]. Disponível em: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

sistemas informáticos e especialmente com o advento da Internet que podemos falar de pirataria em massa como uma das formas mais generalizadas de cibercriminalidade.

- Um direito de propriedade intelectual é um bem intangível, um bem chamado tangível, que é **o resultado da actividade criativa de uma pessoa.** Este direito é **independente de um substrato material** (pode portanto ser utilizado em qualquer altura e em qualquer parte do mundo) desde que seja **único, não reprodutível e suficientemente original.**
- Os direitos de propriedade intelectual podem ser divididos em duas áreas:

  1) **Direitos de autor** (protege, por exemplo, obras literárias e artísticas originais, composições musicais, emissões televisivas, programas informáticos, bases de dados, criações publicitárias, multimédia, etc.).

  2) **Direitos industriais** (proteger, por exemplo, patentes sobre invenções, desenhos, modelos industriais, marcas, origem geográfica, etc.).
- Os termos mais frequentemente utilizados são **pirataria de software** (com referência à violação dos direitos de autor em relação a programas informáticos) e **pirataria audiovisual** (com referência à violação dos direitos de autor em obras audiovisuais - música e filme). **No entanto, a base da pirataria de software e audiovisual é sempre a violação de um dos direitos de autor ou direitos relacionados com os direitos de autor.**
- Os crimes contra a propriedade intelectual expandiram-se consideravelmente com o surgimento maciço da Internet. Os casos mais comuns de violação dos direitos de autor no ciberespaço incluem:
  - *distribuição de uma obra por correio electrónico*, que é a forma mais fácil de distribuir pequenos ficheiros (especialmente obras literárias ou gráficas de autoria),
  - *publicação de uma obra num sítio web* sem o consentimento do autor. Esta é outra forma muito simples de infringir os direitos de autor. Os ficheiros mais pequenos (em termos de tamanho dos dados) são publicados e este comportamento ilegal é normalmente detectado muito cedo.
  - *distribuição de uma obra carregando-a para um servidor especializado a* partir do qual as obras podem ser descarregadas livremente (por exemplo, Megaupload, Rapidshare),
  - *divulgação de um trabalho através de redes peer-to-Peer (P2P)*.[65] Estas redes são capazes de transferir/partilhar enormes quantidades de dados (na ordem de alguns GB a dezenas de TB). Estes são os casos mais flagrantes de violação dos direitos de autor.
  - *adulteração de programas de computador a fim de derrotar os meios técnicos do detentor dos direitos de autor para impedir a criação de cópias de tais programas protegidos* (o chamado crack),
  - *divulgação do trabalho através de suportes de dados directamente entre utilizadores* (empréstimo e subsequente cópia de dados de DVD, discos rígidos, etc., venda de suportes de dados, etc.),
  - *gravação directamente durante a projecção e subsequente disseminação da gravação* (por exemplo, gravação de um trabalho cinematográfico directamente do ecrã) - camcording,
  - *demonstrações não autorizadas de obras audiovisuais,*
  - *a aquisição efectiva de um trabalho informático*. Um programa de computador é particularmente protegido e não é possível fazer cópias de tal obra, mesmo para uso pessoal, sem o consentimento dos proprietários dos direitos de autor ao abrigo da lei dos direitos de autor,

[65] Ao ligar-se a um P2P, o utilizador, por defeito, começa a partilhar automaticamente o seu conteúdo com outros utilizadores (geralmente desconhecidos para eles). Normalmente, ao descarregar, o carregamento do material descarregado é automaticamente definido.

- *utilização de um programa de computador em violação de uma licença,*

- **A colocação de uma obra** (quer audiovisual ou software) no ciberespaço (**uploading**) constitui distribuição da obra na acepção da lei de direitos de autor e (a menos que autorizada pelo autor ou outra pessoa autorizada) pode ser punível. **É também uma utilização não autorizada de uma obra para publicar uma ligação a um local no ciberespaço a partir do qual a obra pode ser obtida.**

Warez

- O termo 'Warez' surge frequentemente em ligação com a pirataria na Internet. Warez **é**, em termos simples, **uma forma de pirataria de software** em que a tecnologia da informação é apenas um meio de acelerar a distribuição de cópias ilegais de obras protegidas por direitos de autor através da Internet. Os fóruns Warez são actualmente utilizados principalmente para descarregar crack e keygen, bem como programas completos modificados, filmes e música. O produto final da cena warez chama-se um **lançamento**.
- **Possíveis sanções penais na Polónia**
  As questões de propriedade intelectual na Polónia são reguladas por dois actos jurídicos básicos: a Lei dos Direitos de Autor e Direitos Conexos e a Lei da Propriedade Industrial.
- **Possíveis sanções penais na República Checa**
  A partilha de ficheiros, seja em redes warez ou P2P, pode ser punida ao abrigo da secção **270** (violação de direitos de autor, direitos relacionados com direitos de autor e direitos de base de dados) ou da **secção 231** (meios e armazenamento de dispositivos de acesso ao sistema informático e senhas e outros dados do género) do Código Penal.
- **Possíveis sanções penais em Portugal**
  Em geral, tais actos são puníveis como cópia não autorizada, distribuição e venda de obras e/ou como contrafacção de obras protegidas por direitos de autor (artigos 195 e 196 do Código dos Direitos de Autor e Direitos Conexos).

Sniffing

- Sniffing é um método de intercepção ilegal de dados que passa através de uma rede informática durante a comunicação entre o serviço fornecido e um sistema informático utilizando **um sniffer.**[66]
- **Possíveis sanções penais na Polónia**
  Na Polónia, farejar (sniffing) é um delito punível de acordo com a lei:
  Violação do segredo de comunicação (farejar) Art. 267 § 3 CC.
- **Possíveis sanções penais na República Checa**
  Tal acção pode praticamente ser descrita como **intercepção e registo ilegal do tráfego de telecomunicações**. O comportamento acima descrito irá certamente interferir com os direitos humanos e liberdades fundamentais, em particular o **Artigo 13 da Carta, e é completamente indiferente se a intercepção ilegal é realizada por um atacante externo ou por um administrador de rede. De acordo com** as normas do direito penal, seria possível subsumir tal comportamento ao abrigo do **Artigo 182(1)** (Violação do sigilo das comunicações) do Código Penal, e no caso de utilização abusiva da informação assim obtida, poderia ser uma infracção ao abrigo do **Artigo 182(2) do** Código Penal
- **Possíveis sanções penais em Portugal**

[66]Sniffing é a palavra inglesa para bisbilhotar ou espiar. Sniffer é, portanto, alguém que bisbilhotar, farejar ou espiar.

Tal acção é abrangida pelo âmbito da Intercepção Ilegal (Artigo 7 da Lei sobre o Crime Cibernético), mas também a partilha e disponibilização de qualquer conteúdo pode ser considerada uma Violação do Segredo da Correspondência ou das Telecomunicações (Artigo 194 do Código Penal).

DoS

- O termo DoS é uma abreviatura para "***negação de serviço***". É uma forma de ataque a um serviço (Internet) que visa desactivar ou reduzir o desempenho de equipamento técnico infectado.[67] Este ataque é levado a cabo inundando o sistema informático comprometido (ou elemento de rede) com pedidos repetidos para que este tome medidas.
- A diferença entre ataques DoS, DDoS e DRDoS reside principalmente na forma como o ataque é levado a cabo. Para maior clareza, os diferentes tipos de ataque são acompanhados por desenhos que demonstram como o ataque é levado a cabo.
- No caso da **DoS (Negação de Serviço), a** fonte do ataque é uma só. Este tipo de ataque é relativamente fácil de defender, uma vez que é possível bloquear o tráfego da fonte do ataque.
- Com a **Negação Distribuída de Serviço (DDoS),** o sistema informático alvo é sobrecarregado pelo **envio de pacotes de múltiplos sistemas informáticos em diferentes locais, o que dificulta a defesa e a identificação do atacante**. Este tipo de ataque tem sido utilizado, por exemplo, contra Yahoo! Inc, comércio electrónico, etc.[68] Botnets ou as acções dos utilizadores que apoiam uma campanha específica na Internet (ver abaixo - Anónimo e LOIC) são muito frequentemente utilizados para este tipo de ataque. No caso do **DRDoS (Distributed ReflectedDenial of Service),** é o spoofedDoSattack, que utiliza um chamado mecanismo de reflexão. O ataque consiste em enviar falsos pedidos de ligação a um grande número de sistemas informáticos, que depois respondem a estes pedidos, mas não ao iniciador da ligação, mas à vítima.
- Os ataques DoS, DDoS, DRDoS exploram muito frequentemente falhas tais como o sistema operativo, programas em execução ou protocolos de rede - UDP, TCP, IP, http, etc.
- Existem vários métodos básicos de ataque DoS ou DDoS, sendo o mais conhecido o mais conhecido:

  Inundação com o comando ping (*Ping-Flood*)

  Graças ao Protocolo de Mensagem de Controlo da Internet e à ferramenta Ping (Packet Internet Groper), é possível utilizar o comando 'ping' para determinar a 'vida' de um sistema informático com um dado endereço IP e para detectar o tempo de resposta de tal sistema.

  Inundação de recursos livres do sistema (*SYN-Flood*)

  SYN-Flood é um tipo de ataque em que o atacante tenta sobrecarregar a sua vítima com um grande número de pedidos de ligação. O atacante envia uma sequência de pacotes de comando SYN (pacotes SYN) para o sistema informático alvo (vítima), com o sistema alvo a responder a cada pacote SYN enviando um pacote SYN-ACK, mas o atacante já não responde.

---

[67] Para mais detalhes, por exemplo MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO e Pedro GARCÍA-TEODORO. Avaliação de um ataque de baixa taxa de DoS contra Servidores de Aplicação. *Computers & Security*, 2008, vol. 27, no. 7-8, pp. 335-354.
CARL, Glenn, Richard BROOKS e Rai SURESH. Detecção de Negação de Serviço com Base em Ondas. *Computers & Security*, 2006, vol. 25, no. 8, pp. 600-615
RAK, Roman e Radek KUMMER. Informačníhrozby v letech 2007-2017. *revista de segurança*, 2007, vol. 14, no. 1, p. 3.

[68] Por exemplo, ataques do DoS aos sítios web da Presidência, Parlamento, ministérios, meios de comunicação social e dois bancos estónios - Estónia (2007). *A Estónia recupera de um ataque maciço de DDoS.* [em linha]. [cit. 4. 3.2010] Disponível em: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

Falsificação do **endereço de origem** (*IP spoofing*)

IP Spoofing é a acção de forjar o endereço de origem dos pacotes enviados, quando um atacante que inicia uma ligação a partir da máquina A com o endereço IP a**.b.c.**dw define como endereço de origem, por exemplo, o endereço IP **d.c.b**.ai envia-o para o alvo B. O alvo B responde a este endereço de origem, isto é, a resposta não é dirigida ao endereço IP a.b.c.d, mas ao endereço IP **d.c.b.a.**

Ataque de Smurf

Este ataque é realizado através de uma má configuração do sistema para enviar pacotes para todos os computadores ligados à rede informática através de um endereço de difusão.

- O objectivo dos ataques DoS/DDoS **não é** geralmente **infectar um computador** ou sistema informático**,** nem **derrotar as características de segurança da palavra-passe** que o protege**,** mas sim **sobrecarregá-lo ou desactivá-lo temporariamente com uma** série de pedidos repetidos. Isto geralmente resulta em acesso restrito ou bloqueado a serviços.
- **Possíveis sanções penais na Polónia**

  Neste caso, aplica-se o Artigo 268 do Código Penal.
- **Possíveis sanções penais na República Checa**

  Decorre da redacção das disposições do Artigo **230(2)** (Acesso não autorizado ao sistema informático e ao portador de informação) do Código Penal:

  Quem tiver acesso a um sistema informático ou meio de armazenamento e

  (a) Faz uso não autorizado de dados armazenados num sistema informático ou num suporte de armazenamento,
  (b) elimina ou destrói, danifica, modifica, suprime ou corrompe a qualidade dos dados armazenados num sistema informático ou em suportes informáticos, ou inutiliza-os sem autorização....

  Decorre desta disposição que um agressor que cometa um ataque DoS ou DDoS deve obter acesso não autorizado a um sistema informático e depois suprimir os dados nele contidos para ser considerado criminalmente responsável.[69]
- **Possíveis sanções penais em Portugal**

  Tais actos são indubitavelmente abrangidos pelo âmbito da sabotagem informática [Interferência Ilegal] (Artigo 5(1) da Lei sobre a Cibercriminalidade), possivelmente como uma infracção agravada em caso de danos graves ou perturbações de infra-estruturas críticas ou outros serviços essenciais (Artigo 5(5)).

Divulgação de conteúdos não desejados

- Actualmente, podem ser descritos dois tipos básicos de divulgação de conteúdos indesejáveis. A divulgação de tipos de pornografia proibidos e a divulgação de conteúdos de ódio e extremismo.
- **Possíveis sanções penais na Polónia**

  Na Polónia, aplica-se o seguinte artigo do Código Penal:
  Artigo 200b. Promoção pública de conteúdos pedófilos
  Artigo 202º Apresentação e difusão de pornografia
- **Possíveis sanções penais na República Checa**

  No caso da criação, posse ou distribuição de material abrangido pelo termo pornografia infantil, é possível punir o utilizador ao abrigo da **secção 192** (Produção e outro tratamento de pornografia infantil), secção **193** (Utilização de uma criança na produção de pornografia) do Código Penal. É também um crime participar num espectáculo pornográfico ou outro espectáculo semelhante envolvendo uma criança (**artigo 193a do Código Penal**). É também um crime ter acesso a pornografia infantil através das tecnologias da informação ou comunicação (artigo **192 (2) do Código Penal**).

[69]Supressão significa a acção enumerada no artigo 4º da Convenção sobre o Cibercrime.

- **Possíveis sanções penais em Portugal**
  Tais actos, dependendo do caso, são criminalizados de forma diferente. Por um lado, podem ser considerados como delitos de pornografia infantil (Arts. 176 CC). Por outro lado, constituem uma violação agravada da privacidade (Artes. 191(1)(b) e 197(b) do Código Penal) ou como Vingança pornográfica relacionada com a violência doméstica (art. 152(2)(b) do Código Penal (art. 193() do Código Penal).

Ataques cibernéticos a plataformas de redes sociais

- Dentro das redes sociais, é possível cometer a maior parte dos ataques cibernéticos descritos anteriormente (por exemplo, malware, phishing, spam, etc.). A razão pela qual os ciberataques a plataformas de redes sociais foram descritos separadamente é que ocorrem principalmente (mas não exclusivamente) no ambiente das redes sociais.
- O cyberbullying move então 'bullying clássico' para o mundo virtual e permite ao agressor utilizar ferramentas e recursos que podem ter um impacto muito maior na vítima do que seria o caso no mundo real. O cyberbullying, através da utilização das TIC e da persistência de dados no ciberespaço, permite ataques repetidos à vítima, mesmo que a vítima se tenha afastado geograficamente no mundo real de onde originalmente foi assediada.
- **As manifestações mais comuns de cyberbullying:**
  Fofocar, intimidar, insultar, ridicularizar ou envergonhar (redes sociais, e-mail, SMS, chat, ICQ, Skype, jogos, etc.).

  Adquirir gravações de som, vídeos ou fotografias, processá-las graficamente ou não, e depois publicá-las para prejudicar (ridicularizar) uma pessoa seleccionada.

  Fazer vídeos nos quais a vítima é fisicamente atacada ou de outra forma abusada psicologicamente e ridicularizada. Estes vídeos são então publicados na Internet (isto é conhecido como Happy Slapping).

  Criar websites, contas nos meios de comunicação social (modificando os originais ou criando novos perfis), sites de discussão, etc. que insultam, denigrem ou humilham uma pessoa específica.

  Abuso da conta de outra pessoa - roubo de identidade (e-mail, discussão, etc.).

  Provocar e atacar os utilizadores em fóruns de discussão (salas de chat, etc.).

  Descobrindo os segredos de outras pessoas.

  Chantagem utilizando um telemóvel ou a Internet.

  Assédio e perseguição através de chamadas, escrevendo mensagens.

- **Possíveis sanções penais na Polónia**
  Na Polónia, isto é regulamentado por:
  Art. 212 CC - Difamação e Art. 190 § 1
- **Possíveis sanções penais na República Checa**
  O cyberbullying (como o bullying clássico) não é em si mesmo um crime ou uma ofensa. Depende sempre das acções do assediador. Se tal acção fosse uma forma de, por exemplo, dano físico à vítima, chantagem ou intimidação, então poderia ser considerada a aplicação, por exemplo, do artigo 146 (BodilyHarm) ou do artigo 145 (GrievousBodilyHarm), artigo 175 (Extorsão) do Código Penal. No caso de assédio e acusação de uma pessoa, poderia ser aplicado o artigo 354º do Código Penal (acusação perigosa).
- **Possíveis sanções penais em Portugal**

Como tal, o cyberbullying não é um delito criminal. Contudo, pode ser considerado uma forma de perseguição (art. 154-A do Código Penal), mas também assédio sexual, insulto, difamação, invasão grave da privacidade, e até discriminação e incitação ao ódio e à violência (Artes. 170, 181, 180, 192 e 197 (b) e 240, todos do Código Penal).

Cybergrooming

- O ciberespaço é um acto de manipulação psicológica de uma pessoa (geralmente utilizando engenharia social), realizado através da Internet ou das tecnologias de informação e comunicação (por exemplo, telemóveis, etc.). O objectivo do ciberespaço é criar uma falsa confiança na vítima e assim induzir um encontro pessoal. O resultado de um tal encontro pode ser qualquer ataque físico, sexual ou outro ataque à vítima. Tanto as crianças como os adultos podem ser vítimas de ciberconferência. De acordo com as estatísticas, as vítimas mais comuns são raparigas com idades compreendidas entre os 13 e os 17 anos.
- **Possíveis sanções penais na Polónia**
  Em Junho de 2010, entrou em vigor uma alteração ao Código Penal. Um tipo de infracção completamente novo apareceu no Código Penal, regulado no Artigo 200 a KK, o chamado grooming, ou seja, a sedução através da Internet. Trata-se de pessoas que, através de um sistema TIC ou de uma rede de telecomunicações, estabelecem contacto com um menor de 15 anos com o objectivo de o enganar, tirando partido do seu erro ou incapacidade de apreender a situação de forma adequada ou ameaçando ilegalmente uma reunião. Esta infracção é punível com uma pena de prisão até três anos.

- **Possíveis sanções penais na República Checa**
  Uma pessoa que comete um ciberespaço pode, pelos seus actos, cumprir os elementos objectivos de certas infracções previstas no Código Penal. Como regra geral, dependendo da natureza do comportamento do agressor, estes serão considerados delitos ao abrigo das disposições do § 168 (Tráfico de seres humanos), § 171 (Privação ilegal da liberdade), § 175 (Extorsão), § 185 (Violação), § 187 (Abuso sexual), § 201 (Ameaça à custódia de menores), § 209 (Fraude), § 353 (Ameaça perigosa), § 354 (Acusação perigosa) do Código Penal.
- **Possíveis sanções penais em Portugal**
  A solicitação de crianças para fins sexuais através das tecnologias da informação e comunicação é um crime (Artigo 176-A do Código Penal).

Sexting

- Uma forma de comportamento perigoso, especialmente no ambiente das redes sociais, é o chamado sexting. O termo sexting foi cunhado a partir de uma combinação das palavras sexo e texturização. É a disseminação electrónica de mensagens de texto, fotografias ou vídeos com conteúdo sexual.

- **Possíveis sanções penais na Polónia**

  De acordo com a lei polaca, é proibido o seguinte:

  - produção para divulgação;

- gravação;
- divulgação;
- apresentação;
- posse e armazenamento;
- Importações

material pornográfico com a participação de um menor - uma pessoa com menos de 18 anos (Artigo 202 CC).

- **Possíveis sanções penais na República Checa**
  Se as fotografias de outra pessoa forem publicadas sem o seu consentimento, é possível para ela fazer valer os seus direitos em processos civis
- **Possíveis sanções penais em Portugal**
  O envio de tal conteúdo a outro adulto pode ser processado como assédio sexual (Art. 170 CC). Contudo, se alguém enviar tal conteúdo a um terceiro, será considerado difamação, invasão opressiva da privacidade, violência doméstica opressiva ou mesmo discriminação e incitação ao ódio e violência (artigos 180, 152, 192 e 197 (b) e 240, todos do Código Penal).

Cyberstalking

- Cyberstalking é o acto de contactar repetidamente a vítima, por exemplo, através de mensagens de texto, e-mails, chamadas telefónicas, VoIP, mensagens instantâneas, etc. As acções do agressor normalmente aumentam e normalmente suscitam preocupações sobre a privacidade, saúde ou vida da vítima.
- *Os ciberstalkers* caracterizam-se pela sua persistência e *natureza* sistemática, e não é raro um ciberstalker criar múltiplas identidades falsas, que utilizam para contactar a vítima.
- O ciberstalker também pode demonstrar o seu poder e força, por exemplo publicando informação sobre a vida da vítima, que pode obter de várias fontes online.
- **Possíveis sanções penais na Polónia**
  De acordo com o Código Penal polaco, a perseguição pode ser cometida de duas formas. Através do assédio persistente de uma pessoa punida (Artigo 190a § 1 do Código Penal) ou através da imitação (Artigo 190a § 2 do Código Penal). A qualificação de um comportamento específico como perseguição depende do facto de o perpetrador preencher várias condições.
- **Possíveis sanções penais na República Checa**
  A perseguição ou ciberperseguição pode ser abrangida pela **secção 354** (Perseguição perigosa) do Código Penal sob certas condições. As condições básicas incluem que o perseguidor deve contactar a vítima "*persistentemente por meios electrónicos, escritos ou outros*" durante um longo período de tempo e tal acção é capaz de causar um medo razoável pela vida ou saúde da vítima ou pela vida e saúde dos familiares da vítima. Uma circunstância agravante nos termos do **artigo 354 § 2 (a) do** Código Penal é se o referido acto tiver sido cometido em detrimento de uma criança
- **Possíveis sanções penais em Portugal**
  Recentemente, a perseguição, incluindo a perseguição cibernética, tornou-se uma infracção penal como perseguição (Artigo 154-A do Código Penal).

Roubo de identidade

- O roubo de identidade é um ataque em que uma identidade virtual é roubada[70] , ou é a tomada de controlo (permanente ou temporária) dessa identidade. O motivo do atacante pode ser um ganho financeiro, mas também outros benefícios relacionados com o facto de o atacante estar a agir em nome de outra pessoa, por exemplo, acesso a informações sobre outras pessoas, acesso a dados da empresa, etc.
- **Possíveis sanções penais na Polónia**
  Nos termos do Artigo.190 a § 2 do Código Penal, quem, fazendo-se passar por outra pessoa, utilizar a sua imagem ou outros dados pessoais para causar danos materiais ou pessoais a essa pessoa, será passível de pena de prisão até três anos.
- **Possíveis sanções penais na República Checa**
  Se a segurança for derrotada e for obtido acesso não autorizado à identidade da vítima, a infracção ao abrigo do **artigo 230 (1)** (Acesso não autorizado aos sistemas informáticos e meios de informação) do Código Penal será cumprida. Ao utilizar software malicioso para o mesmo fim, o agressor comete uma infracção ao abrigo do artigo 230 (2) do Código Penal. Se o objectivo do roubo de identidade for obter uma vantagem injustificada para si próprio ou para outra pessoa, as disposições do artigo **230 (3) do Código** Penal podem também ser aplicáveis. Se o agressor roubar uma identidade com o objectivo de enganar outra pessoa, ou seja, enganar alguém para se enriquecer a si próprio, tal conduta pode também ser avaliada ao abrigo do **artigo 209** (Fraude) do Código Penal.
- **Possíveis sanções penais em Portugal**
  Fingir ser outra pessoa já não é punível. No entanto, a criação de dados não autênticos para fins legalmente relevantes seria considerada falsificação informática (artigo 3º da Lei sobre o Cibercrime). Além disso, se o objectivo de tal falsificação for a intenção fraudulenta ou desonesta de obter ilegalmente um benefício pecuniário para si próprio ou para outra pessoa a expensas da vítima, isto também seria considerado fraude informática (Artigo 221(1) do Código Penal).

APT

- APT representa uma ameaça avançada e persistente. É um ciberataque sistemático sustentado centrado no sistema informático alvo ou nas TIC da organização visada. Diferentes técnicas e recursos relativamente grandes são utilizados para tal ataque, e normalmente alvos secundários (por exemplo, sistemas informáticos, tais como ataques repetidos de DoS ou outros) podem ser atacados para distrair a atenção do alvo principal (infiltração da empresa por malware), que é depois atacado.
- Durante um ataque APT, os atacantes podem utilizar outros tipos diferentes de ataques ao alvo escolhido, dependendo dos dados e informações adquiridas.
- **Possíveis sanções penais na Polónia**
  Ao analisar o ataque APT do ponto de vista das violações da lei em vigor na Polónia, deve reconhecer-se que se o ataque tivesse sido levado a cabo em todas as suas fases, teriam sido cometidas pelo menos várias infracções penais. De acordo com a lei aplicável, um ataque APT pode ser considerado como tal:
  - hacking ao abrigo do artigo 267 § 1 do Código Penal.
  - a infracção de fazer ou fornecer dispositivos ou programas informáticos, palavras-passe e códigos nos termos do artigo 269b do Código Penal

[70] Identidade virtual significa qualquer identidade ou avatar utilizado por uma pessoa para interagir no ciberespaço (por exemplo, e-mail, conta de rede social, jogo, vários mercados online, sistema informático, etc.) Não importa se a identidade virtual é real ou falsa, ou seja, se representa uma pessoa real ou se é uma identidade completamente criada artificialmente e sem base real.

- fraude informática nos termos do artigo 287º do Código Penal

- **Possíveis sanções penais na República Checa**
  A possível sanção penal do(s) atacante(s) que efectua(m) o ataque APT depende então inteiramente das suas acções, que podem tomar a forma, por exemplo, de distribuição de malware, um dos ataques de phishing, Roubo de Identidade, etc.
- **Possíveis sanções penais em Portugal**
  Um ataque APT não é especificamente criminalizado, mesmo como uma infracção agravada.

Terrorismo

- O terrorismo pode ser dividido por forma em *formas letais* e *não letais,* em que o primeiro grupo se caracteriza pela utilização de meios de violência comummente disponíveis (*convencionais* - ataques cometidos com armas comummente disponíveis, tais como armas de fogo, e não convencionais - o uso indevido de armas de destruição maciça). Em contraste, as formas não letais **de terrorismo**[71] ou ataques que utilizam instrumentos mais modernos em combinação com meios letais são mais comuns em linha.
- A forma convencional de terrorismo não letal inclui os seguintes subgrupos:

  - *Terrorismo desarmado*.

  - Ciber-terrorismo - uma das maiores ameaças do século XXI. O princípio é principalmente a má utilização das TIC (incluindo a Internet) como meio e ambiente para levar a cabo um ataque. Tal como um ataque terrorista clássico convencional, é uma actividade planeada, geralmente motivada política ou religiosamente e levada a cabo por pequenas estruturas organizadas em vez de militarmente.

Terrorismo mediático, no qual há uma má utilização planeada dos media e de outras armas psicológicas para influenciar as opiniões da população em geral ou dos grupos alvo

- **Possíveis sanções penais na Polónia**
  Na Polónia, os artigos 265 a 269 e 287 do Código Penal aplicam-se à implementação de um ataque ciberterrorista, e dependendo do efeito do ataque ciberterrorista, alguns outros artigos do Código Penal podem também aplicar-se, como por exemplo:
  Artigo 163 Causar uma catástrofe
  Artigo 164º Provocar o perigo de catástrofe
  Artigo 165º Causar perigo público
  Artigo 173 Causar um acidente de viação
  Artigo 174 Causar o perigo iminente de uma catástrofe de trânsito

[71] No entanto, uma combinação destes ataques pode ser imaginada. Mais detalhes podem ser encontrados, por exemplo, em:
Exclusivo: O vírus informático atinge a frota de zangões dos EUA. [online]. [citado 10.7.2016]. Disponível a partir de: https://www.wired.com/2011/10/virus-hits-drone-fleet/.

- **Possíveis sanções penais na República Checa**
  Do ponto de vista do direito penal, os actos acima mencionados podem cumprir os elementos objectivos das infracções ao abrigo do artigo 311(2) (ataque terrorista), artigo 355 (difamação de uma nação, raça, grupo étnico ou outro grupo de pessoas), artigo 356 (incitamento ao ódio contra um grupo de pessoas ou supressão dos seus direitos e liberdades), Secção 364 (incitamento a uma infracção), Secção 403 (criação, apoio e promoção de movimentos destinados a suprimir os direitos humanos e as liberdades) e Secção 404 (expressão de simpatia por movimentos destinados a suprimir os direitos humanos e as liberdades) do Código Penal.
- **Possíveis sanções penais em Portugal**
  De acordo com a Lei Antiterrorista N.º 52/2003, se as infracções estiverem relacionadas com fins terroristas, as penas para infracções tais como fraude informática ou falsificação informática serão aumentadas em um terço (Artigo 4(2)). Além disso, as penas para infracções relacionadas com a comunicação electrónica (artigo 4(3)(4), recrutamento (artigo 4(5)(6)) ou promoção de grupos ou actividades terroristas são aumentadas se cometidas através da Internet (artigo 4(8)(9)).

3. Durante as aulas

<u>Algumas ideias para actividades:</u>

WORKSHOPS

1. Análise de ataques cibernéticos individuais e da sua subsunção ao abrigo das disposições da Convenção sobre o Cibercrime (TJCE nº 185) e da legislação nacional (República Checa, Polónia, Portugal).
2. Análise de ataques individuais - modus operandi
3. Teste de segurança contra ataques seleccionados.
4. Definição de opções para prevenir determinados tipos de ataque
5. Concepção de uma solução personalizada para proteger contra ataques cibernéticos individuais.
6. Testes de segurança de certos sistemas, aplicações e dados. Os estudantes tentarão conceber as suas próprias soluções para aumentar a segurança destes sistemas, aplicações ou dados.
7. Familiarização com ferramentas e recursos para armazenamento seguro de dados e estabelecimento de comunicação segura em linha (por exemplo, administração e configuração de VPN, PGP, gestor de senhas, etc.).

PERGUNTAS DE REVISÃO

1.

- O que é a cibercriminalidade?
- O que não é um crime cibernético?
- O que é um ataque cibernético?
- Qual é a diferença entre a cibercriminalidade e o ciberataque?
- Qual é a diferença entre dados e informação?
- O que é a tríade da CIA?

2.

- O que é característico da engenharia social?
- O que é uma botnet e como funciona?
- Quais são as típicas topologias botnet?
- Pode ser considerado crime ser proprietário de uma botnet?
- O que é malware?
- Quais são os exemplos mais comuns de malware?
- Quais são os vectores de infecção por malware mais comuns?
- O que é um resgate e quais são as suas manifestações?
- O que é o phishing e como é que este ataque é mais comummente realizado?
- Qual é a diferença entre phishing e pharming?
- O que é hacking?
- O que é característico da fissuração?
- Qual é a diferença entre hacking e cracking?
- O que é um ataque DoS e como é que funciona?
- Qual é a diferença entre DoS e DDoS?
- O que pode ser incluído na distribuição de conteúdo defeituoso?
- O que é APT?

Trabalhar em pares/grupos

- **Pares - mini-projecto**
  Em pares, os estudantes escolhem um dos tópicos discutidos. Eles escrevem as suas conclusões e apresentam-nas aos outros. Após a apresentação, os outros estudantes preparam perguntas adicionais para o grupo de apresentação.

- **Mapa de pensamentos**
  Os estudantes em pares escolhem um dos tópicos abordados e criam um mapa mental, que depois descrevem aos outros estudantes numa breve apresentação.

- **Palavras-chave**
  Os alunos em pares seleccionam individualmente palavras-chave a partir do glossário.

  Eles escrevem as definições destas palavras em tiras de papel. Viram as tiras de papel com o lado em branco para cima. Um aluno escolhe uma tira, lê a definição e o outro aluno procura uma palavra-chave correspondente.
  ou
  Os alunos escrevem algumas palavras-chave do glossário num pedaço de papel. Eles viram os cartões com o lado em branco para cima. Um estudante pega no primeiro cartão e diz o que a palavra significa. O segundo aluno adivinha a palavra-chave.

- 10 palavras-chave
  Os estudantes escolhem 10 palavras-chave relacionadas com o tema escolhido. Estas 10 palavras-chave são dadas a outros pares. Os pares escrevem um texto que deve conter todas as palavras-

chave. Uma frase só pode conter uma palavra-chave. Assim, o texto consiste em pelo menos 10 frases-chave.

- Painel de discussão

  Os alunos escolhem 3 oradores. Cada orador escolhe um tópico para discutir. Os outros estudantes fazem perguntas sobre os tópicos. Cada orador pode usar um tipo de resposta -TRUE X FALSE. O estudante recebe um ponto para cada resposta verdadeira, por exemplo, GDPR significa REGULAMENTO GERAL DE PROTECÇÃO DE DADOS? - VERDADEIRO X FALSO.

4. Recursos da Internet

Ver bibliografia abaixo

5. Perguntas/testões adicionais

SELECCIONAR A RESPOSTA CORRECTA:
(A resposta correcta foi destacada)

1. _____ pode ser definido como um comportamento dirigido contra um computador ou, em alguns casos, uma rede informática, ou como um comportamento em que um computador é utilizado como uma ferramenta para cometer um crime.

   a) Cyber hacking
   b) Efeito cibernético
   (c) Ataque cibernético
   d) Cibercriminalidade

2. _____ pode ser definido como qualquer comportamento ilegal de um agressor no ciberespaço que seja dirigido contra os interesses de outra pessoa.

   a) Incidente cibernético
   (b) Ataque cibernético
   d) Acidente cibernético
   (c) Cybernapad

3. Computador _____ significa "qualquer expressão de factos, informações ou conceitos de uma forma adequada ao processamento num sistema informático, incluindo um programa capaz de levar um sistema informático a executar uma função".

   (a) conceitos
   (b) orientação
   (c) Limites temporais
   (d) Dados

4. _____ é "uma violação da segurança da informação nos sistemas de informação, ou uma violação da segurança da prestação de serviços, ou uma violação da segurança e integridade das redes de comunicações electrónicas como resultado de um evento cibernético".

(a) Crime de segurança cibernética
b) Alcançar a segurança cibernética
c) Enfraquecimento da segurança cibernética
(d) Incidente de ciber-segurança

5. _____ é "um evento que tem o potencial de comprometer a segurança da informação nos sistemas de informação ou de comprometer a segurança dos serviços ou a segurança e integridade das redes de comunicações electrónicas".

(a) Incidente de ciber-segurança
b) Escândalo de ciber-segurança
c) Negligência da ciber-segurança
d) A questão da segurança cibernética

6. _____ não pode ser considerado directamente aplicável de forma transversal a um ataque cibernético, mas é uma condição para o sucesso de muitos ataques cibernéticos.

(a) Engenharia civil
(b) engenharia social
(c) engenharia cibernética
(d) engenharia criminal

7. _____ pode muito simplesmente ser definido como uma rede de bots ligados por software que executam alguma acção baseada num comando do 'proprietário' (ou administrador) dessa rede.

(a) Bennet
(b) Máscara
(c) Botnet
(d) Bootnet

8. _____ são geralmente os programas informáticos que contêm funções ocultas que o utilizador não consente ou não tem conhecimento, e que são potencialmente perigosos para a continuação do funcionamento do sistema.

a) Roubo de dados
(b) Farming
c) Rootkits
(d) Cavalos de Tróia

9. O termo _____ é mais comummente utilizado para descrever comportamentos fraudulentos ou enganosos destinados a obter informações do utilizador tais como nomes de utilizador, palavras-passe, números de cartões de crédito, PINs, etc.

(a) Pescaria clandestina
(b) spyware
(c) Porta traseira
(d) vermes

10. O que é que significa BEC?

a) Certificado de Economia Empresarial
(b) Violação da segurança do correio electrónico
c) Contribuição para o esforço empresarial
d) Efeito comercial cibernético

11. O termo _____ é agora visto pejorativamente pelo público como qualquer acção por uma pessoa para obter acesso ilegal ao sistema ou computador pessoal de outra pessoa.

(a) malware
(b) adware
(c) hacking
(d) fraude

12. O termo _____ é um termo geral que cobre crimes que infringem os direitos de propriedade intelectual (muito frequentemente limitado aos direitos de autor).

(a) Pirata da Internet
(b) Percepções da Internet
(c) Piranha na Internet
(d) Pirataria na Internet

13. O que significa DDoS?

(a) Negação de Serviço Perturbada
(b) Negação de serviço distribuída
c) Dia de Serviço Dividido
(d) Bloqueio Desastrutivo do Serviço

14. O que significa APT?

a) Perigos persistentes avançados
b) Ameaça criminosa avançada
c) Percepção avançada da ameaça
(d) Ameaça trivial avançada

Bibliografia

1. *Os 10 grupos de hacking mais notórios.* [em linha]. [citado 15.7.2016]. Disponível em: https://www.hackread.com/10-most-notorious-hacking-groups/.
2. *7 tipos de motivação de hacker.* [em linha]. [citado 16.8.2015]. Disponível a partir de: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/.
3. *7 tipos de hackers que deve conhecer.* [em linha]. [citado 16.8.2015]. Disponível em: https://www.cybrary.it/0p3n/types-of-hackers/.
4. *Ameaça Persistente Avançada - ciclo de vida* [online]. [citado 20. 8. 2016]. Disponível em: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg.
5. *Ameaça Persistente Avançada (APT).* [online]. [citado 20. 8. 2016]. Disponível em: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.
6. *Ameaça Persistente Avançada.* [online]. [citado.20.8.2016]. Disponível em: https://www.isouvislosti.cz/advanced-persistent-threat.
7. *Ameaças persistentes avançadas: Como eles trabalham.* [em linha]. [citado 10.7.2016]. Disponível em: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1
8. *Adware.* [online]. [citado 10.8.2016]. Disponível a partir de: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking.
9. *O Android Ransomware agora também tem como alvo a sua Smart TV, Too!* [online]. [citado 14.8.2016]. Disponível a partir de: https://thehackernews.com/2016/06/smart-tv-ransomware.html
10. *Distribuição da quota de mercado das versões Android entre os proprietários de smartphones a partir de Maio de 2016.* [online]. [citado 14.8.2016]. Disponível a partir de: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/
11. BALIGA, Arati, Liviu IFTODE e Xiaoxin CHEN. Contenção Automatizada de Ataques de Rootkits. *Computers& Security*, 2008, vol. 27, no. 7-8, pp. 323-334.
12. *Cuidado com o Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [citado 14.8.2016]. Disponível a partir de: https://www.hackread.com/fake-android-prisma-app-phishing-malware/
13. *Botnet - uma lista histórica de botnets.* [em linha]. [citado 15.8.2016]. Disponível a partir de: http://www.liquisearch.com/botnet/historical_list_of_botnets
14. *Botnet.* [citado 8.7.2016]. Disponível a partir de: http://research.omicsgroup.org/index.php/Botnet.
15. *Botnet.* [online]. [citado 15.7.2016]. Disponível a partir de: https://en.wikipedia.org/wiki/Botnet.
16. *Botnets.* [online]. [citado 15.7.2016]. Disponível em: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6.
17. *Bots e botnets - uma ameaça crescente.* [em linha]. [citado 11.8.2016]. Disponível em: https://us.norton.com/botnet/
18. *Buffalo Spammerjde na 7 let za mřížekvůlirozesílánínevyžádanépošty.*[online]. [citado 14.8.2016]. Disponível em: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality.
19. CARL, Glenn, Richard BROOKS e Rai SURESH. Detecção de Negação de Serviço com Base em Ondas. *Computers& Security*, 2006, vol. 25, no. 8, pp. 600-615
20. CHOO, Kim-Kwang Raymond. *Aliciamento de crianças em linha: uma revisão bibliográfica sobre a má utilização de sítios de redes sociais para aliciamento de crianças para delitos sexuais* [em linha]. Canberra: Instituto Australiano de Criminologia, c2009, [citado em 19.3.2014]. ISBN 978-1-921532-

33-7. Available from: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

21. *Combate ao cibercrime na era digital.* [em linha]. [citado 7.5.2016]. Disponível a partir de: https://www.europol.europa.eu/ec3.
22. *A 'Queridinha' gerada por computador captura predadores em linha.* [em linha]. [citado 19.8.2016]. Disponível em: http://www.bbc.com/news/uk-24818769
23. Condenado spammer desafia a lei Va. [citado 14.8.2016]. Disponível em: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm
24. *Ciberterrorismo: quão perigosa é a ameaça do ciber-califado ISIS?* [em linha]. [citado 20.8.2016]. Disponível em: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html
25. *Cibercriminalidade*. [online]. [citado 1.2.2015]. Disponível em: http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; et al.
26. *Digital Doom's Digi World*, 2008. ISSN 1802-047X. [online]. [citado 14.8.2016]. Disponível a partir de: http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html.
27. *O perturbador vídeo ISIS mostra militantes a decapitar quatro reclusos e um pistoleiro a encurralar compradores num mercado.* [online]. [citado 20.8.2016]. Disponível a partir de: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017
28. Protocolo adicional. Protocolo Adicional à Convenção sobre Cibercriminalidade, relativo à criminalização de actos de natureza racista e xenófoba cometidos através de sistemas informáticos https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189
29. DODGE, Ronald. C., Curtis CARVE E AARON J. FERGUSON. Phishing para a sensibilização dos utilizadores para a segurança. *Computers& Security*, 2007, vol. 26, no. 1, pp. 73-80.
30. *A Estónia recupera de um poderoso ataque DDoS.* [online]. [citado 4. 3.2010] Disponível a partir de: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack.
31. *Exclusivo: O vírus informático atinge a frota de zangões dos EUA.* [online]. [citado 10.7.2016]. Disponível a partir de: https://www.wired.com/2011/10/virus-hits-drone-fleet/.
32. *Combate ao cibercrime: patrulhas cibernéticas e equipas de investigação cibernética como um reforço da estratégia da UE.* [em linha]. [citado.10.7.2016]. Disponível a partir de: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827
33. *Os clones de aves Flappy Bird ajudam as taxas de malwares móveis a subir* [online]. [citado 14.8.2016]. Disponível a partir de: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx
34. *FLocker Mobile Ransomware cruza para Smart TV.*[online]. [citado 14.8.2016]. Disponível a partir de: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/
35. *A França deixa cair a controversa "lei Hadopi" depois de gastar milhões*[online]. [citado 15.7.2016]. Disponível em:https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy etc.
36. *Frigorífico apanhado a enviar spam em ataque de botnet.* [online]. [citado 17.5.2016]. Disponível em: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/.
37. GONZÁLES-TALAVÁN, Guillermo. Um simples filtro de spam SMTP configurável: Greilistas. *Computers&Security*, 2006, vol. 25, No. 3, pp. 229-236.

38. BOM BOM MARKETO, Marc. Uma *visão do crime no futuro* [online]. [citado.13.11.2014]. Disponível a partir de: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071
39. *O Google diz que os melhores esquemas de phishing têm uma taxa de sucesso de 45 por cento.* [em linha]. [citado 14.8.2016]. Disponível em: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/
40. GREENBERG, Andy. *Hackers matam jipe remotamente na auto-estrada - comigo lá dentro.* [online]. [citado 4.5.2016]. Disponível a partir de: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
41. GRIFFITHS, Mark. Criminalidade Informática e Hacking: uma questão séria para a Polícia? *The Police Journal,* 2000, vol. 73, No. 1, pp. 18-24.
42. GŘIVNA, Tomáš e Radim POLČÁK. *Kyberkriminalita a právo*. Praga: Auditório, 2008.
43.
44. HILL, Caxemira. *Estes dois jogadores de Diablo III roubaram armadura virtual e ouro - e foram processados pela IRL*. [online]. [citado 10.8.2015]. Disponível a partir de: http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/
45. *Uma lista histórica de botnets.* [em linha]. [citado 15.8.2016]. Disponível em: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html.
46. *Mapas históricos de redes informáticas*. [Online]. [citado 10.7.2016]. Disponível em: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html.
47. *Como funcionam os APTs? O Ciclo de Vida das Ameaças Persistentes Avançadas (Infográfico)* [online]. [citado 10. 7. 2016]. Disponível em: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/
48. *Como utilizar a Wireshark para capturar, filtrar e inspeccionar os pacotes.* [online]. [citado 15.7.2016]. Disponível a partir de: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/
49. *Divisão de hacking do Estado Islâmico.* [em linha]. [citado.20.8.2016]. Disponível em: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355.
50. *Jessica Logan - 'The Rest of the Story'.*[citado 8.8.2016]. Disponível em: http://nobullying.com/jessica-logan/.
51. *Juiz, 69 anos, que descarregou pornografia infantil ameaça 'humilhação catastrófica'.* [em linha]. [citado 1.9.2009]. Disponível a partir de: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo
52. *Caso Kevin Mitnick: 1999* [online]. [citado 2.11.2011]. Disponível a partir de: http://www.encyclopedia.com/doc/1G2-3498200381.html
53. KOLOUCH, Jan, Pavel BAŠTA et al. *Cibersegurança*. Praga: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
54. KOLOUCH, Janeiro. Evolução das Campanhas dePhishing e Compromisso de Email de Negócios na República Checa. Em: *Academic and Applied Research in Military and Public Management Science*. Budapeste: Universidade Nacional de Serviço Público, 2018, pp. 83-100. ISSN 2498-5392.
55. KOLOUCH, Janeiro. *Cibercriminalidade.* Praga: CZ.NIC, 2016. ISBN 978-80-88168-15-7.
56. KOLOUCH, Jan iAndrera KROPÁČOVÁ. Ransomware. Em: ZHUANG, Xiaodong. *Recent Advances in Computer Science: Proceedings of the 19th International Conference on Computers*. B.m.: B.n., 2015, pp. 304-307. Recent Advances in Computer Engineering Series, [No. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109.

57. NÍVEL, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly Media, pp. 32-41. ISBN 978-1449388393.
58. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modelação e análise da propagação de vermes activos com base em sistemas P2P. *Computers& Security*, 2007, vol. 26, no. 3, pp. 213-218.
59. *Malware, mayhem, e o takedown McColo* [online]. [citado 14.8.2016]. Disponível a partir de: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/
60. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO e Pedro GARCÍA-TEODORO. Avaliação de um ataque de baixa taxa de DoS contra Servidores de Aplicação. *Computers& Security*, 2008, vol. 27, no. 7-8, pp. 335-354.
61. MELOY, Reid J. *STALKING (SEGUIMENTO OBSESSIONAL): UMA REVISÃO DE ALGUNS ESTUDOS PRELIMINARES.* [online]. [citado 3.10.2015]. Disponível em: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf.
62. MITNICK, Kevin D. e William L., SIMON. *Ghost in the Wires: as minhas aventuras como o hacker mais procurado do mundo*. Nova Iorque: Little, Brown & Co, 2012. ISBN 9780316037723.
63. MITNICK, Kevin D. *A arte da intrusão: as histórias reais por detrás das explorações de hackers, intrusos e enganadores*. Indianapolis: Wiley, 2006. ISBN 0-471-78266-1.
64. MUELLER, Robert. [Online]. [citado 3.4.2013]. Disponível a partir de: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.
65. *O novo Ransomware encripta ficheiros de jogo.* [online]. [citado 14.8.2016]. Disponível em: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/
66. NIGAM, Ruchna. Uma *linha temporal de botnets móveis.* [online]. [citado 12.7.2016]. Disponível a partir de: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf.
67. *OWASP, XSS* [online]. [citado 15.7.2016]. Disponível em: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
68. *Senha Sniffer Spy.* [online]. [citado 18.8.2016]. Disponível a partir de: http://securityxploded.com/password-sniffer-spy.php.
69. *Relatório de actividade de PhishingTresnds.* [online]. [citado 14.8.2016]. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf
70. *Phishing by the Numbers: Must-Know Phishing Statistics 2016.*[online]. [citado 14.8.2016]. Disponível em: https://blog.barkly.com/phishing-statistics-2016
71. PLETZER, Valentin. Desmascaramento de spyware. *CHIP*, 2007, no. 10, pp. 116-120.
72. PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. *Botnets: Detecção, Medição, Desinfecção &Defesa.* ENISA, 2011 [online]. [citado.17.5.2015], p. 14. Disponível a partir de: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence
73. PROSISE, Chris e Kevin MANDIVA. *Resposta a Incidentes & Forense Informática, 2ª ed.* Emeryville: McGraw-Hill, 2003.
74. RAK, Roman e Radek KUMMER. Informačníhrozby v letech 2007-2017. *revista de segurança*, 2007, vol. 14, no. 1, p. 4.
75. *Ransomware.* [online]. [citado 14.8.2016]. Disponível em: https://www.trendmicro.com/vinfo/us/security/definition/ransomware.
76. SCHNEIER, Bruce. *Crime: A Próxima Grande Coisa da Internet* [online]. [citado 6.11.2007]. Disponível em: https://www.schneier.com/crypto-gram/archives/2002/1215.html.

77. SCHNEIER, Bruce. *A Internet das Coisas Transformará os Hacks de Grande Escala em Catástrofes do Mundo Real* [online]. *[*citado 10.8.2016]. Disponível em: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster
78. SCHNEIER, Bruce. *Sete tipos de hackers.* [online]. [citado 16.8.2015]. Disponível em: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html.
79. SCHRYEN, Guido. O impacto que a colocação de endereços de e-mail na Internet tem na recepção de spam: Uma Análise Empírica. *Computers& Security*, 2007, vol. 26, No. 5, pp. 361-372.
80. Selfmite - O *verme SMS do Android Selfmite está de volta, mais agressivo do que nunca.* [online]. [citado 14.8.2016]. Disponível em: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html
81. *Estatísticas e factos Spam.* [em linha]. [citado 14.8.2016]. Disponível em: http://www.spamlaws.com/spam-stats.html
82. *Estatísticas de Spam*. [online]. [citado 14.8.2016]. Disponível em: https://www.spamcop.net/spamstats.shtml.
83. *Stuxnet.* [online]. [citado.23.7.2016]. Disponível em: https://cs.wikipedia.org/wiki/Stuxnet.
84. *Diário de ataques cibernéticos direccionados.* [online]. [citado 10.7. 2016]. Disponível em: https://apt.securelist.com/#secondPage
85. TAYLOR, Harriet. *Como a 'internet das coisas' pode ser desastrosa.* [em linha]. [citado 17.6.2016]. Disponível em: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html.
86. *Aperto de mão TCP passo a passo.* [online]. [citado 18.8.2016]. Disponível em: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000.
87. *Avaliação da ameaça da criminalidade organizada em linha (iOCTA) 2014.* [em linha]. [citado 10.8.2015]. Disponível em: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
88. *O Museu Malware @ Internet Archive*. [em linha]. [citado 17.5.2016]. Disponível a partir de: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/.
89. *Testemunho de um antigo hacker.* [em linha]. [citado 26.9.2008]. Disponível em: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html
90. *O primeiro malware móvel: como Kaspersky Lab descobriu Cabir*. [online]. [citado 29.6.2015]. Disponível a partir de: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
91. Tinba: *W32. Tinba (Tinybanker).* [Online]. [citado 15.8.2016]. Disponível em: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf.
92. *Julho 2016 Dica do Mês - Evite ser viciado em Phishing*. [online]. [citado 14.8.2016]. Disponível em: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/
93. *Top Spammer Sentenciado a Quase Quatro Anos* [online]. [citado 14.8.2016]. Disponível a partir de: http://www.pcworld.com/article/148780/spam.html
94. Convenção sobre o Cibercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
95. *Manual das Nações Unidas sobre a prevenção e controlo da criminalidade informática.* [em linha]. [citado 20.8.2016]. Disponível em: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf
96. *Advertência! Mais de 900 milhões de telefones Android Vulneráveis ao Novo Ataque 'QuadRooter'.* [online]. [citado 10.8.2016]. Disponível a partir de: https://thehackernews.com/2016/08/hack-android-phone.html

97. *ATENÇÃO: ISIS Downs Prisioneiros Vivos & Sopram Reféns com RPG & Mata Outros com Explosivos - vídeo gráfico.* [online]. [citado 20.8.2016]. Disponível a partir de: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382
98. WILSON Tracy,V.*How Phishing Works*[online]. [citado.14.8.2016]. Disponível a partir de: http://computer.howstuffworks.com/phishing.htm.
99. Xshqi - *Um verme andróide para o Dia dos Namorados chinês.* [online]. [citado 14.8.2016]. Disponível a partir de: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/
100. YAR, Majid. Computer Hacking: Apenas mais um caso de Delinquência Juvenil? *The Howard Journal*, 2005, vol. 44, no. 4, pp. 387-399.
101. ZETTER, Kim. *Os passageiros podem hackear companhias aéreas comerciais?* [online]. [citado 5.5.2016]. Disponível em: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

Módulo 4

CSIRT e CERT

1. Introdução

1.1 Resumo do curso

O curso concentra-se na segurança cibernética e introduz o aluno aos princípios de estabelecer a segurança cibernética. A fim de compreender toda a questão, é também necessário conhecer os direitos e responsabilidades das equipas de segurança e as suas tarefas, papéis e processos. Uma parte significativa do curso abrange CERTs e CSIRTs (estrutura, hierarquia) e a ancoragem legal das CERTs e CSIRTs (direitos e responsabilidades). Além disso, o tema do tratamento de incidentes (IH) não deve ser negligenciado. A análise de código aberto dentro do IH, as capacidades de transferência de dados e informação são também tópicos chave que constituem uma parte essencial desta parte do curso.

1.2 Objectivos do curso

Os incidentes de segurança, ciberataques e crimes relacionados com as TIC no mundo real e virtual estão a tornar-se mais graves e as suas consequências e efeitos estão a piorar. Há uma necessidade crescente de melhorar a defesa contra estes ataques e, em particular, de melhorar o ambiente e os meios de localizar o perpetrador, de uniformizar e formalizar os procedimentos e de educar os utilizadores sobre como identificar, lidar e, idealmente, prevenir ameaças e situações de risco. Para tal, está a ser construída uma infra-estrutura de equipas de segurança como as CERTs e CSIRTs. O objectivo do curso é familiarizar os alunos com estas equipas de segurança, o seu funcionamento, hierarquia, processo de acreditação, capacidades de partilha de dados e informações, etc. Além disso, os alunos irão explorar o Sistema de Gestão da Segurança da Informação. Finalmente, irão descobrir a importância da protecção de dados no ciberespaço.

1.3 Conteúdo do curso

Palestras individuais introduzem os estudantes ao tema da segurança cibernética. Além disso, os alunos são introduzidos aos princípios da criação de uma equipa de segurança cibernética (tarefas, papéis, processos, etc.) Um dos tópicos-chave é CERTs e CSIRTs (estrutura, hierarquia) e a ancoragem legal das CERTs e CSIRTs (direitos e responsabilidades). Além disso, os estudantes estudam os direitos e responsabilidades das equipas de segurança. O tratamento de incidentes (IH), a análise de código aberto dentro do IH e as capacidades de transferência de dados e informações são também extremamente importantes, pelo que a última parte das aulas lhes é dedicada.

1.4 Objectivos de aprendizagem

1) Introdução aos princípios de criação de segurança cibernética
2) Definição de riscos, bens, vulnerabilidades
3) Compreender as ameaças cibernéticas e outros termos-chave
4) Conhecer as CERTs e CSIRTs
5) Definição do quadro legal dos CERT/CSIRTs

1.5 Equipamento e materiais necessários

CSIRTs e CERTs - disponíveis online
Directiva (UE) 2016/1148 (Directiva NIS)

1.6 Programa de estudos

Resultado da aprendizagem	O aluno que completar o módulo com sucesso saberá/ será competente no seguinte.
NOVIDADES	
W1	O estudante obterá informações sobre o desenvolvimento histórico das equipas de segurança que operam no ambiente da Internet. O estudante conhecerá os papéis das diferentes equipas de segurança e a base legal para o seu funcionamento.
HABILIDADES	
U1	Compreende o funcionamento de equipas de segurança como as CERTs e CSIRTs, aprende sobre a sua estrutura e as ligações entre as equipas.
U2	Compreender a questão do tratamento de incidentes.
COMPETÊNCIAS	
K1	Ele poderá actuar como membro da equipa de segurança.

Conteúdo do módulo (programa de palestras e outras actividades)	**Referência aos resultados da aprendizagem**
LECTURAS 1. Cibersegurança 2. Princípios para o estabelecimento da segurança cibernética 3. Equipa de segurança (tarefas, papéis, processos, etc.) 4. CERTs e CSIRTs (estrutura, hierarquia) 5. Poderes legais das CERTs e CSIRTs (direitos e obrigações) 6. Direitos e responsabilidades das equipas de segurança 7. Tratamento de incidentes (IH) 8. Análise de código aberto IH 9. Capacidades de transferência de dados e informações WORKSHOPS 1. Construção de uma equipa de segurança	W1, U1, U2, K1

Métodos de verificação dos resultados da aprendizagem

Resultado da aprendizagem	**Formas de classes de crédito**								
	Exame oral	Exame escrito	Trabalho escrito parcial	Trabalho final escrito (ensaio, etc.)	Teste	Desenho/apresentação	Relatório	Actividades de sala de aula	Outros ...
NOVIDADES									
W1		x			x			x	
HABILIDADES									
U1						x		x	
U2						x		x	
COMPETÊNCIAS									
K1						x		x	

Saldo de crédito ECTS		
Forma de carga de trabalho dos estudantes		Número de horas
Número de horas com participação directa do professor académico		
1.1	Participação em conferências	10
1.2	Participação em seminários	
1.3	Participação em workshops	8
1.4	Participação em actividades laboratoriais	
1.5	Participação em projectos	
1.6	Participação em consultas (2-3 vezes por semestre)	
1.7	Participação na consulta do projecto	
1.8	Participação em exames/teste	2
1.9	Outros ...	
1.10	**Número de horas passadas com assistência directa de pessoal académico (soma 1.1 - 1.9)**	20
1.11	**Número de créditos ECTS obtidos pelo aluno em aulas que requerem a participação directa de um professor académico)**	1
Trabalho individual do estudante		
2.1	Estudos individuais (incluindo palestras de e-learning)	25
2.2	Preparação individual para workshops	10
2.3	Preparação do teste individual	
2.4	Preparação individual para aulas de laboratório	
2.5	Elaboração de relatórios	
2.6	Implementação de tarefas auto-realizadas (projectos, documentação)	
2.7	Preparação para o exame/teste final do seminário	5
2.8	Preparação para exame/teste final de conferências	5
2.9	Outros	
2.10	**Número de horas de trabalho individual (soma de 2,1 - 2,9)**	45
2.11	**Número de créditos ECTS obtidos pelo estudante em trabalhos individuais de ensino**	1,5
Carga de trabalho total (h)		**65**
Créditos ECTS para o módulo		**2,5**

Critérios para avaliar a competência dos estudantes
Os requisitos mínimos para os três grupos de resultados de aprendizagem que o Estudante deve atingir a fim de passar na disciplina são apresentados abaixo de forma sintética. Para que um Estudante passe num módulo, todos os resultados de aprendizagem descritos no programa devem ser verificados positivamente pela(s) pessoa(s) que ensina(m) o módulo.

W - CONHECIMENTO
Avaliação:
Satisfatório - O aluno lembra-se e reproduz os conhecimentos a dominar dentro do módulo.
Bom - O estudante interpreta adicionalmente fenómenos/problemas e é capaz de resolver um problema típico
Muito bom - O estudante é capaz de resolver problemas mesmo complexos num determinado campo, é capaz de sintetizar, realizar uma avaliação abrangente, criar um trabalho que é original e inspirador para outros.

U - HABILIDADES
Avaliação:
Satisfatório - O aluno conhece a natureza das actividades e é capaz, sob a orientação do professor académico, de realizar as actividades / resolver os problemas relacionados com o conteúdo do módulo

Bom - O estudante é capaz de realizar actividades / tarefas / resolver problemas típicos relacionados com o conteúdo do módulo
Muito bom - O aluno dominou totalmente a capacidade / habilidade para realizar as actividades / tarefas / problemas previstos no conteúdo do módulo, também em casos mais complexos.

K - COMPETÊNCIA SOCIAL
Avaliação:
Satisfatório - O aluno assimila passivamente o conteúdo do módulo, demonstrando capacidade de concentração e escuta
Bom - O estudante participa activamente nas aulas, faz juízos de valor de acordo com os critérios aceites no domínio em questão, pode cooperar activamente num grupo
Muito bom - O estudante integra a atitude de acordo com o modelo proposto, desenvolve o seu próprio sistema de valores profissionais e sociais, é capaz de assumir a responsabilidade pelas acções do grupo, incluindo a liderança.

2. Material básico para o professor

Definições (glossário)

Segurança - um Estado em que as ameaças a uma instalação (na maioria das vezes um Estado-nação ou mesmo uma organização internacional) e os seus interesses são reduzidos ao mínimo possível, e a instalação está efectivamente equipada e disposta a cooperar para eliminar as ameaças existentes e potenciais".[72]
Segurança - uma característica de um objecto ou entidade que determina o grau em que está protegido de potenciais danos e ameaças".[73]
Segurança - A propriedade de um item (por exemplo, um sistema de informação) que é protegido a algum nível contra perda, ou o estado de ser protegido (a algum nível) contra perda. A segurança informática inclui a protecção da confidencialidade, integridade e disponibilidade no processamento, armazenamento, distribuição e apresentação da informação. [74]
Segurança cibernética - é o conjunto de medidas que são tomadas para proteger um sistema informático contra acessos ou ataques não autorizados. [75]
A cibersegurança é o **estado em que estamos protegidos contra a utilização criminosa ou não autorizada de dados electrónicos.** A segurança cibernética abrange então as medidas que têm de ser tomadas para alcançar este estado.[76]
Cibersegurança - é "**um conjunto de medidas** legais, organizacionais, técnicas e educativas concebidas para **assegurar a protecção do ciberespaço.** "[77]
Segurança cibernética - representa **um conjunto de medidas e instrumentos** organizacionais, políticos,

[72] ZEMAN, Petr et al. *Terminologia de segurança checa: interpretação de conceitos básicos* [online]. [citado 2018-07-10]. Disponível a partir de: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13
[73] *PO`ÁR, Josef. Segurança da informação*. Pilsen: AlešČeněk, 2005, p. 37.
[74] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 23 [online]. [citado 2018-07-10]. Disponível em: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.
[75] *Ciber-segurança.* [em linha]. [citado 2018-07-06]. Disponível a partir de: https://www.merriam-webster.com/dictionary/cybersecurity Tradução do autor.
[76] *Ciber-segurança.* [em linha]. [citado 2018-07-06]. Disponível em: https://en.oxforddictionaries.com/definition/cybersecurity Tradução do autor.
[77] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 69 [online]. [citado 2018-07-10]. Disponível em: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.

jurídicos, técnicos e educacionais **destinados a garantir um ciberespaço seguro, protegido e resiliente na República Checa,** tanto para entidades do sector público e privado como para o público checo em geral". [78]
Segurança cibernética - refere-se à segurança do ciberespaço, referindo-se o próprio ciberespaço ao conjunto de ligações e relações entre objectos acessíveis através da rede geral de telecomunicações, e o próprio conjunto de objectos cujas interfaces permitem o seu controlo remoto, o acesso remoto a dados ou a realização de actividades de controlo no ciberespaço
A definição de cibersegurança de acordo com a lei polaca é - a resistência dos sistemas de informação a acções que violem a confidencialidade, integridade, disponibilidade e autenticidade dos dados processados ou serviços relacionados oferecidos por estes sistemas
Ciber-segurança - pode ser definida como: a totalidade das medidas legais, organizacionais, técnicas e educativas para assegurar a protecção dos sistemas informáticos e outros elementos das TIC, aplicações, dados e utilizadores,
A cibersegurança - pode ser definida como: a capacidade dos sistemas e serviços informáticos utilizados para responder a ameaças ou ataques cibernéticos e aos seus efeitos, e para planear a recuperação da funcionalidade dos sistemas informáticos e serviços relacionados.
CIA - significa C - **Confidencialidade**; **I** - **Integridade**; **A - Acessibilidade**
Dados informáticos - significa "**qualquer expressão de factos, informações ou conceitos numa forma adequada ao processamento por um sistema informático,** incluindo um programa capaz de levar um sistema informático a executar **uma** função".
Informação "são dados que foram processados num formulário que é útil para o destinatário. Portanto, qualquer informação é um dado, mas qualquer dado armazenado não se torna necessariamente informação".[79]
Informação - é vista como algo mais 'qualificado' do que dados. Os dados são factos que se tornam informação quando são percebidos ou expressos em contexto e transportam um significado que as pessoas podem compreender.[80]
Top secret - o tratamento não autorizado de informações pode causar danos extremamente graves aos interesses do Estado.
Segredo - o tratamento não autorizado da informação pode causar sérios danos aos interesses do Estado.
Confidencial - a utilização não autorizada da informação pode causar danos comuns aos interesses do Estado.
Restrição - a utilização não autorizada da informação pode ser prejudicial para os interesses do Estado.
Protegido - O tratamento não autorizado da informação pode causar sérios danos ou destruição à organização (por exemplo, fuga de informação estratégica, código fonte, esquemas de segurança, palavras-passe, etc.).
Interno - o tratamento não autorizado de informações pode causar danos à organização (por exemplo, fuga de dados pessoais, contratos, etc.).
Sensível - o tratamento não autorizado de informações pode ter consequências negativas para a empresa (por exemplo, informações não publicadas sobre projectos, eventos planeados, etc.).
Público - a utilização não autorizada de informação não deve prejudicar ninguém e não deve afectar o público (por exemplo, contactos publicamente disponíveis, apresentações de projectos, etc.).[81]
TLP significa **Protocolo de Semáforo**
Acessibilidade - é definida como "a propriedade de estar disponível e utilizável a pedido de uma entidade autorizada".
IDS - abreviatura de IntrusionDetectionSystém (sistema de detecção de intrusão)
IPS - abreviatura de IntrusionPreventionSystém (sistema de prevenção de intrusão)

[78] *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [citado 2018-07-01]. Disponível em: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf p. 5
[79] PO`ÁR, Josef. *Segurança da informação.* Pilsen: AlešČeněk, 2005, p. 25
[80] SÁMAL, Pavel et al. *Kodekskarny II. §§ 140-421. comentário.* 2ª ed. Praga: C. H. Beck, 2012, p. 2308
[81] Cf. mais adiante: SécULC, Vladimír. *Cybersecurity.* Plzeň: AlešČeněk, 2018. p. 20 e seguintes.

Risco - é "(1) Perigo, a possibilidade de dano, perda, falha. (2) O impacto da incerteza na realização dos objectivos. (3) A possibilidade de uma ameaça explorar a vulnerabilidade de um activo ou grupo de activos e causar danos à organização".[82]
Risco - também pode ser definido como o potencial de uma ameaça para se materializar e explorar a vulnerabilidade de um bem.
O risco é definido como "**qualquer circunstância ou evento razoavelmente identificável que possa afectar negativamente a segurança das redes e dos sistemas de informação". '**
Bens - qualquer coisa de valor para uma pessoa, organização ou país**.**
Bens - de uma perspectiva de direito civil, **um bem** pode ser **uma coisa tangível** (edifício, sistema informático, rede, energia, mercadoria, etc.) **ou uma coisa intangível** (informação, conhecimento, dados, programas, etc.).
Bens - pode também ser uma **propriedade** (por exemplo, disponibilidade e funcionalidade do sistema e dos dados, etc.) ou **reputação,** etc. **As pessoas** (utilizadores, administradores, etc.) e os seus conhecimentos e experiência são também uma mais-valia do ponto de vista da segurança cibernética.
Bens de apoio - são os recursos técnicos, empregados e contratantes envolvidos na operação, desenvolvimento, gestão ou segurança de um sistema TIC
O principal activo é a informação ou serviço processado ou fornecido pelo sistema de TIC.
Vulnerabilidade - refere-se a uma fraqueza num bem, software ou segurança que é explorado por uma ou mais ameaças.
Ameaça - pode muito simplesmente ser definida como algo capaz de perturbar o estado normal ou ordeiro e interferir com os direitos dos outros. É uma acção negativa que pode ou não ser levada a cabo
Uma ameaça é considerada como "qualquer fenómeno que tenha o potencial de causar danos aos interesses e valores protegidos pelo Estado". O grau de ameaça é determinado pela magnitude do dano potencial e pela distância temporal (geralmente expressa em termos de probabilidade ou risco) da possível aplicação dessa ameaça".[83]
Perigo - é definido como "a causa potencial de um evento não intencional que possa causar danos a um sistema ou organização". [84]
Ameaça à Segurança da **Informação**[85] - é definida como "a causa potencial de um evento adverso que possa resultar em danos ao sistema e aos seus bens, tais como destruição, acesso não desejado (compromisso), modificação de dados ou indisponibilidade de serviços". [86]
Ameaça cibernética - é a possibilidade de uma tentativa maliciosa de danificar ou perturbar uma rede ou sistema informático.[87]
Uma ameaça cibernética também **pode** ser definida como uma acção destinada a alterar a informação[88] , aplicações ou o próprio sistema.
A fuga de informação é quando a informação protegida é revelada a uma parte não autorizada.
Uma violação da integridade é a corrupção, alteração ou apagamento de dados.
A supressão de serviços significa impedir deliberadamente o acesso à informação, a uma aplicação ou a um

[82] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 99. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[83] *Jeopardy.* [online]. [citado 2018-07-28]. Disponível em: http://www.mvcr.cz/clanek/hrozba.aspx.

[84] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 52. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[85]Neste caso, podemos notar um problema com a tradução de alguns termos do inglês e vice-versa. Se quisermos traduzir consistentemente o termo Ameaça à segurança da informação, o equivalente checo correcto é, por exemplo, ameaça à segurança da informação; ameaça à segurança da informação, etc.

[86] Ibid p. 25

[87] *Ameaça cibernética.* [online]. [citado 2018-07-06]. Disponível a partir de: https://en.oxforddictionaries.com/definition/cyberthreat.

[88] Alterar também significa roubar informação, destruí-la ou impedir a sua utilização.

sistema.[89]
A utilização ilegal é a utilização de informação por uma parte não autorizada ou de uma forma não autorizada.[90]
"Incidente de segurança informática" (que pode ser entendido como um ataque informático ou crime informático) - uma acção ilegal, não autorizada e inaceitável envolvendo um sistema ou rede informática.
Um incidente de segurança - é "**um evento que pode causar ou conduzir a uma violação dos** sistemas e tecnologias de informação e das regras definidas para os proteger (política de segurança)".[91]
Evento de segurança - é um sistema, serviço ou **condição de** rede **identificável que indica uma possível violação da política de segurança ou falha das medidas de segurança**
Um incidente de cibersegurança - é **um evento que pode causar uma violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas.**
Incidente de segurança da informação - um ou mais eventos de segurança não intencionais ou inesperados que têm uma elevada probabilidade de comprometer as operações de uma organização e de comprometer a segurança da informação
Incidente de segurança informática - é uma violação ou ameaça iminente de violação de políticas de segurança, políticas de utilização aceitável (sistema, serviço) ou práticas de segurança padrão".[92]
Incidente de cibersegurança - é uma **violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas como resultado de um incidente cibernético.**
Ataque cibernético - "um ataque à infra-estrutura informática para causar danos e obter informação sensível ou estrategicamente importante. É mais frequentemente utilizado no contexto de ataques de motivação política ou militar".[93]
Ataque cibernético[94] - pode ser definido como **qualquer acção deliberada de um atacante no ciberespaço que seja dirigida contra os interesses de outra pessoa.**
Cibercrime - pode ser definido **como uma acção dirigida contra um sistema informático, rede informática, dados ou utilizadores, ou como uma acção em que um sistema informático é utilizado como uma ferramenta para cometer um crime.**
CERT - representa a Equipa de Resposta a Emergências Informáticas
CSIRT - abreviatura para Equipa de Resposta a Incidentes de Segurança Informática
CERT/CSIRT - pode ser **entendido como o mesmo tipo de equipa - uma equipa responsável pelo tratamento de incidentes de segurança e ameaças (cibernéticas) na sua área de operação claramente definida, do ponto de vista dos utilizadores ou outras equipas, um local a que se pode recorrer com um incidente de segurança detectado, solicitando cooperação, troca de informações, assistência, etc.**
Âmbito da equipa - define o que é da responsabilidade da equipa e qual é o seu papel. Isto, claro, depende do tipo de equipa que é.
Equipa interna - opera e é responsável por uma rede específica (por exemplo, uma gama específica de endereços IP, domínios), e é normalmente nomeada pelo operador de rede.

[89] Estes incluem ataques tais como **DoS - Denial of Service**, **DDoS - Distributed Denial of Service**, etc. Mais detalhes podem ser encontrados no livro KOLOUCH, Jan. *Cibercriminalidade.* Praga: CZ.NIC, 2016, pp. 295 ff.

[90] Por exemplo, um sistema baseado em taxas é comprometido e os seus serviços são utilizados sem pagamento por serviços.

[91] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 28. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[92] *Guia de tratamento de incidentes de segurança informática* **[online]. [citado 2018-02-17]**, p. 6**. Disponível em:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[93] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 71. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[94] É necessário distinguir o conceito de incidente de segurança do conceito de ataque informático, que constitui uma violação da segurança SI/TI e das regras definidas para a sua protecção (política de segurança).

Equipa de coordenação - uma equipa cuja principal tarefa é coordenar a resolução de incidentes de segurança, e não resolvê-los.
Equipa de vendedores - a equipa que lida com incidentes de segurança que envolvem um produto específico (SW).
Equipa nacional/governamental - casos especiais baseados nos princípios das duas primeiras equipas mencionadas (equipa interna e equipa de coordenação), o seu âmbito e papel dependem do fundador e muitas vezes da legislação do país específico.
Back-office - uma ferramenta para a gestão eficaz dos relatórios de incidentes de segurança que irá rastrear todo o ciclo de vida do relatório, ou seja, quando o relatório foi enviado, por quem, quem lidou com o incidente em que fases, porquê, como foi tratado, quem pediu a quem cooperar, qual a gravidade do incidente e que procedimentos de escalonamento foram aplicados ao mesmo, etc.
A base organizacional é a referida "prontidão" para resolver o problema, ou seja, definir as regras básicas da equipa, para que cada membro da equipa conheça o seu papel, deveres e responsabilidades, política de tratamento de incidentes de segurança, regras de comunicação, partilha e intercâmbio de informação, cooperação, etc. A base nesta área é geralmente bem gerida, a chamada **gestão de incidentes.**
FIRST significa Fórum de Resposta a Incidentes e Equipas de Segurança
TF-CSIRT (Task Force for CSIRT) - é um grupo de trabalho que permite às equipas colaborar através de reuniões regulares de dois dias realizadas 3 vezes por ano (o anfitrião desta reunião é geralmente a equipa CERT/CSIRT).
Formação CSIRT - é utilizada para formar novos membros da equipa CSIRT/CERT ou aqueles que estão prestes a criar uma equipa CERT/CSIRT. É geralmente realizada duas vezes por ano e os formadores são membros experientes de equipas CERT/CSIRT de renome e de outros peritos de segurança de topo.
TrustedIntroducer[95] - um escritório cujo papel principal é criar confiança entre as equipas CERT/CSIRT e ajudar a estabelecer novas equipas.
A equipa com o estatuto **listado** forneceu informações básicas sobre si própria, declarou a sua vontade de agir como uma equipa CSIRT e foi aceite pela comunidade
Uma equipa com estatuto **acreditado** declara o nível de prática desejado pela comunidade e compromete-se com os princípios comuns da TI.
A equipa **certificada** demonstrou então o seu "nível de maturidade" através de um processo de certificação.
ENISA - significa a Agência Europeia para a Segurança das Redes e da Informação.
RIR - abreviatura para Registos Regionais da Internet
Tratamento de incidentes - o processo de notificação e resolução de incidentes de segurança.
BotnetFeed- esta ferramenta é utilizada para processar dados de servidores C&C descarregados sobre estações finais ligadas a botnets. A fim de identificar um sistema informático potencialmente infectado, o endereço IP e a informação sobre a botnet à qual está ligada são passados ao gestor da gama IP.
IHAP - abreviatura de Projecto de Automatização da Gestão de Incidentes
MDM - abreviatura de Malicious Domain Manager (Gestor de Domínio Malicioso)
Indicadores de compromisso - abreviatura de IoC
Shadowserver- o projecto centra-se na procura contínua de informação relevante sobre vulnerabilidades cibernéticas e a ocorrência destas vulnerabilidades em endereços IP específicos.

Citações chave de material em linha:

- A palavra **ciberespaço** significa interdependência com elementos das tecnologias de informação e comunicação e o ciberespaço enquanto tal.

[95] Mais tempo também **TI**.

- Marés define segurança como "*um Estado em que as ameaças a um objecto (geralmente um Estado-nação ou mesmo uma organização internacional) e os seus interesses são reduzidos ao mínimo possível, e o objecto está efectivamente equipado e disposto a cooperar para eliminar as ameaças existentes e potenciais*".[96]
- *A propriedade de um item (por exemplo, um sistema de informação) que é protegido a algum nível contra perda, ou o estado de ser protegido (a algum nível) contra perda. A segurança informática inclui a protecção da confidencialidade, integridade e disponibilidade no processamento, armazenamento, distribuição e apresentação da informação.* [97]
- Este alargamento do círculo de segurança requer, entre outros, a abordagem das seguintes questões: **Cuja segurança está em jogo** (organização internacional, estado, organização, indivíduo, etc.).

  Que valores são protegidos (organizações, pessoas, dados, etc.)**?**

  Quais são (devem ser) estes valores protegidos contra (ataques físicos, cibernéticos, ataques combinados, etc.)**?**

  Que recursos são necessários para proteger estes valores? [98]
- Ao definir a própria segurança cibernética, é útil confiar em definições estabelecidas. Vou enumerar algumas dessas definições estabelecidas:
  - **A cibersegurança** é um **conjunto de medidas que são tomadas para proteger um sistema informático contra o acesso ou ataque não autorizado.** [99]
  - O Dicionário Oxford afirma que **a ciber-segurança** é **um estado de protecção contra a utilização criminosa ou não autorizada de dados electrónicos.** A ciber-segurança abrange então as medidas a serem tomadas para alcançar este estado.[100]
  - Segundo Jirásek et al. a **cibersegurança** é *"**um conjunto de medidas** legais, organizacionais, técnicas e educativas destinadas a **assegurar a protecção do ciberespaço.** "*[101]
  - A Estratégia Nacional de Segurança Cibernética 2015-2020 da República Checa define a segurança cibernética de uma forma relativamente semelhante, afirmando que *"A segurança cibernética é um **conjunto de medidas e instrumentos** organizacionais, políticos, legais, técnicos e educacionais **destinados a assegurar um ciberespaço seguro, protegido e***

---

[96] ZEMAN, Petr et al. *Terminologia de segurança checa: interpretação de conceitos básicos* [online]. [citado 2018-07-10]. Disponível a partir de: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

[97] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 23 [online]. [citado 2018-07-10]. Disponível em: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.

[98] Mais detalhes podem ser encontrados, por exemplo, em MAREŠ, Miroslav. *Segurança.* [Online]. [citado 2018-07-10]. Disponível em: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511.
WAISOVÁ, sárka. *Segurança: desenvolvimento e mudanças conceptuais.* Pilsen: AlešČeněk, s.r.o., 2005. ISBN 80-86898-21-0
FRANCISCO, Libor. *Estudos de segurança.* [Online]. [citado 2018-07-10]. Disponível em: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf.

[99] *Ciber-segurança.* [em linha]. [citado 2018-07-06]. Disponível a partir de: https://www.merriam-webster.com/dictionary/cybersecurity Tradução do autor.

[100] *Ciber-segurança.* [em linha]. [citado 2018-07-06]. Disponível em: https://en.oxforddictionaries.com/definition/cybersecurity Tradução do autor.

[101] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 69 [online]. [citado 2018-07-10]. Disponível em: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.

***resiliente na República Checa**, tanto para entidades do sector público e privado como para o público checo em geral".* [102]

- **Os seguintes princípios, também conhecidos como a tríade cibernética, são implementados na aplicação da segurança cibernética.**[103]
  Para os fins desta monografia, serão definidas as três tríades seguintes:

  CIA [**C** - **Confidencialidade**; **I** - **Integridade**; **A - Acessibilidade**].

  Elementos de segurança cibernética (Pessoas, Tecnologia, Processos).

  Ciclo de Vida Ciber-segurança (Prevenção, Detecção, Resposta).

- A tríade de cibersegurança mais conhecida e amplamente utilizada é a tríade da **CIA**, mas a aplicação desta tríade básica de princípios de cibersegurança por si só, sem a implementação de outros princípios, é actualmente insuficiente para manter um nível adequado de cibersegurança
- Por exemplo, a literatura aponta para a utilização de **Parker'shexad**[104] , uma tríade de facto da CIA complementada por três outros elementos: **P/C - Possessão/Controlo**, **A - Autenticidade** e **U - Utilidade**.
- Muito frequentemente, a tríade da CIA está principalmente associada à informação.
  Este conceito restrito deve-se principalmente à própria definição de segurança da **informação**, que se centra na protecção da informação. No contexto desta protecção, não é relevante em que meio (papel, meio electrónico, etc.) ou em que sistema a informação é processada. A segurança da informação refere-se então à informação ao longo de todo o seu ciclo de vida.
- A segurança da informação é também definida por uma série de normas ISO 27000. As normas básicas de segurança da informação incluem:
  ISO/IEC 27001:2014 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos
  ISO/IEC 27002:2014 Tecnologia da informação - Técnicas de segurança - Conjunto de práticas para medidas de segurança da informação
- De acordo com a Convenção sobre o Cibercrime[105] **, dados informáticos** significam *"**qualquer expressão de factos, informações ou conceitos numa forma adequada ao processamento por um sistema informático,** incluindo um programa capaz de levar um sistema informático a executar **uma** função".*
- **Informação** *"são dados que foram processados num formulário que é útil para o destinatário. Portanto, qualquer informação é um dado, mas qualquer dado armazenado não se torna necessariamente informação".*[106]

---

[102] *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [citado 2018-07-01]. Disponível em: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf p. 5

[103] Ver, por exemplo, HSU, D. Frank e D. MARINUCCI (eds.). *Avanços na segurança cibernética: tecnologia, operações, e experiências*. Nova Iorque: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. p 41. KADLECOVÁ, Lucie. *Aspectos conceptuais e teóricos da segurança cibernética.* [em linha]. [citado 2018-07-21]. Disponível em: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf.

[104] Mais detalhes podem ser encontrados, por exemplo, em *ParkerianHexad.* [Online]. [citado 2016 Ago. 20]. Disponível a partir de: https://vputhuseeri.wordpress.com/2009/08/16/149/.

[105] Artigo 1(b) da Convenção sobre o Cibercrime. *Convenção sobre a Criminalidade Cibernética.* [em linha]. [citado 20 de Agosto de 2016]. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0.

[106] PO`ÁR, Josef. *Segurança da informação.* Pilsen: AlešČeněk, 2005, p. 25

- **Por conseguinte, a informação é vista como algo mais 'qualificado' do que os dados.** Os dados são factos que se tornam informação quando são percebidos ou expressos em contexto e transportam um significado que as pessoas podem compreender.[107]
- O conceito de confidencialidade define o facto de apenas as pessoas autorizadas a ter acesso à informação, aos dados ou às tecnologias de informação e comunicação poderem ter acesso à mesma
- As normas de segurança ISO/IEC 27000 especificam isso:
  "A informação deve ser classificada tendo em conta o seu valor, requisitos legais, sensibilidade e criticidade".
  "Devem ser desenvolvidos e implementados procedimentos para rotular e tratar a informação que seja coerente com o esquema de classificação adoptado pela organização".
  "A fim de impedir o acesso não autorizado ou a utilização indevida da informação, devem ser estabelecidas regras para o seu tratamento e armazenamento".
- Exemplos de alguns esquemas de classificação:

1. **Classificação das informações de acordo com a Lei Checa 412/2005 Coll., relativa à protecção das informações classificadas e à habilitação de segurança**[108] :

- **Top secret** - o tratamento não autorizado de informações pode causar danos extremamente graves aos interesses do Estado.
- **Segredo** - o tratamento não autorizado da informação pode causar sérios danos aos interesses do Estado.
- **Confidencial** - o tratamento não autorizado da informação pode causar danos comuns aos interesses do Estado.
- **Restrição - a** utilização não autorizada da informação pode ser prejudicial para os interesses do Estado.

2. **Classificação das informações utilizadas na esfera comercial**:

- **Protegido - O** tratamento não autorizado da informação pode causar sérios danos ou destruição à organização (por exemplo, fuga de informação estratégica, código fonte, esquemas de segurança, palavras-passe, etc.).
- **Interno - o** tratamento não autorizado de informações pode causar danos à organização (por exemplo, fuga de dados pessoais, contratos, etc.).
- **Sensível - o** tratamento não autorizado de informações pode ter consequências negativas para a empresa (por exemplo, informações não publicadas sobre projectos, eventos planeados, etc.).
- **Público - a** utilização não autorizada de informação não deve prejudicar ninguém e não deve afectar o público (por exemplo, contactos publicamente disponíveis, apresentações de projectos, etc.).[109]

3. **Protocolo de semáforos**

- Dentro da comunidade de cibersegurança, tem havido historicamente uma necessidade de partilhar informações e dados (geralmente relacionados com ciberataques) que são de natureza sensível. Por esta razão, o Centro Nacional de Coordenação de Segurança de Infra-estruturas[110] criou o **TrafficLightProtocol**(**TLP**)[111] no início dos anos 2000.

---

[107] SÁMAL, Pavel et al. *Código Penal II. §§ 140-421. comentário.* 2ª ed., Pavel et al. Praga: C. H. Beck, 2012, p. 2308

[108] Para mais detalhes, ver https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/.

[109] Cf. mais adiante: SécULC, Vladimír. *Cybersecurity.* Plzeň: AlešČeněk, 2018. p. 20 e seguintes.

[110] Actualmente o Centro para a Protecção das Infra-estruturas Nacionais - CPNI

[111] Para mais detalhes, ver, por exemplo, Definições e Utilização do Protocolo TrafficLightProtocol (TLP). [Online]. [citado 2018 Jan 13]. Disponível a partir de: https://www.us-cert.gov/tlp.

4. **Avaliação da confidencialidade em conformidade com o Decreto Checo n.º 82/2018 Coll., sobre medidas de segurança, incidentes de cibersegurança, medidas reactivas, requisitos de notificação de cibersegurança e disposição de dados** (Decreto de Segurança Cibernética)[112]

- De acordo com o Interpretive Cyber Security Dictionary[113] , a **integridade é** definida como "*a propriedade da precisão e integridade". A* **integridade dos dados** é ainda definida no mesmo dicionário como *"a confiança de que os dados não foram alterados". Figurativamente, refere-se também à validade, consistência e exactidão dos dados, tais como bases de dados ou sistemas de ficheiros. É fornecido por checksums, funções de hash, códigos auto-correctores, redundância, registo, etc. Na criptografia e segurança da informação em geral, a integridade refere-se à validade dos dados". A integridade* **do sistema**, portanto, é *"a propriedade de que um sistema desempenha a sua função pretendida de forma ininterrupta, sem manipulação intencional ou acidental, não automatizada do sistema".*
- **A integridade significa, portanto, que a informação, os dados, os sistemas informáticos, as suas configurações,** etc. **não podem ser adulterados por outras pessoas que não as autorizadas para o efeito.**
- De acordo com o Interpretive Cyber Security Dictionary[114] , a **disponibilidade é** definida como "*a propriedade de estar disponível e utilizável a pedido de uma entidade autorizada".*
- A disponibilidade pode portanto ser definida como a garantia de poder aceder a informação, dados ou a um sistema informático quando necessário. Um sistema autónomo que garanta a integridade e permita o acesso ao sistema, aos dados ou à própria informação é inútil se não proporcionar um acesso fiável quando necessário.[115]
- *"A destruição de certas informações é referida na segurança da informação como a perturbação da sua disponibilidade".*
- Os três elementos seguintes ou a sua interacção permitem, em certa medida, criar ou estabelecer a segurança cibernética. Estes elementos são:
    - Pessoas,
    - Tecnologias
    - Processos.
- As pessoas que interagem com a segurança cibernética podem ser vistas como:

  o(s) **criador**(es) **dessa segurança** (ou seja, tipicamente a(s) pessoa(s) que tenta(m) impor e implementar os vários elementos da segurança cibernética, quer para si próprios quer para a organização),

  Os beneficiários da legislação de segurança cibernética (ou seja, aqueles que escolheram ou são obrigados a implementar a legislação de segurança cibernética existente), entidades que precisam de ser protegidas contra ataques cibernéticos,

  Entidades a serem informadas e formadas sobre regulamentos e princípios de segurança cibernética,

---

[112] A seguir referido como Regulamento de Segurança Cibernética ou **VoKB.**

[113] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 58 [online]. [citado 2018-07-10]. Disponível em: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.

[114] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 43 [online]. [citado 2018-07-10]. Disponível em: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf.

[115] Ver, por exemplo, EVANS, DONALD, PHILIP, BOND e ARDEN BEMET. *Normas para Categorização de Segurança de Sistemas Federais de Informação e Informação.* Instituto Nacional de Normas e Tecnologia, Centro de Recursos de Segurança Informática. [online]. [citado 2017 Dez 10]. Disponível em: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.

- **Risco ou ameaça no contexto da criação e manutenção da segurança cibernética**.
- Na nossa opinião, é importante para as pessoas que utilizam as TIC e optam por interagir no ciberespaço:

  conhecer pelo menos **os princípios e regras básicas aplicáveis à segurança cibernética**,

  compreender pelo menos **as funções básicas dos sistemas informáticos** (por exemplo, computador, portátil, telemóvel, televisão inteligente, etc.) que **utilizam** para esta interacção,

  analisar as aplicações que utilizam para esta interacção, e se não se sentirem confiantes na utilização destas aplicações ou na compreensão dos seus termos, devem deixar de as utilizar,

  foram educados em segurança cibernética.
- A tecnologia é normalmente um meio de ligação dos utilizadores à Internet, redes sociais e outras aplicações. É uma ferramenta que utiliza vários pacotes de escritório para criar documentos, enviar e-mails, ver vídeos, etc. Como regra, o utilizador comum percebe e interage com as tecnologias finais (PC, tablet, telemóvel, etc.) que utiliza pessoalmente, enquanto que normalmente não está interessado nas outras camadas tecnológicas que são essenciais para a sua actividade no ciberespaço.
- Em termos de tecnologia, uma parte integrante das TIC de uma organização deve ser o seguinte, dependendo das especificidades dessa organização:
    - sistemas de detecção - Sistema de Detecção de Intrusão (**IDS**)/ Sistema de Prevenção de Intrusão (**IPS**),
    - gestão central de utilizadores e funções,
    - gestão centralizada da classificação da informação,
    - protecção contra código malicioso (firewall de aplicação, anti-vírus, anti-spam e outras soluções),
    - tecnologia para registar as actividades de componentes individuais de TIC, administradores e utilizadores (**sistema de registo)**,
    - sistemas de backup activos e offline; backups de servidores, aplicações e bases de dados importantes (**sistema de recuperação de dados)**,
    - gestão da segurança da rede (VLAN, DMZ, firewall, etc.).
- Os processos são as acções que precisam de ser tomadas para que a tecnologia e os serviços relacionados possam ser utilizados pelas pessoas.
- Em termos da passagem do tempo, os seguintes processos podem ser seguidos:
    - gestão de activos e riscos,
    - definição e categorização dos bens,
    - análise e categorização do risco,
    - implementação de tecnologias e aplicações de informação e comunicação,
    - gestão de utilizadores e funções,
    - autorização e autenticação,
    - manutenção (actualizações) de sistemas e serviços,
    - testes de segurança de sistemas e serviços informáticos individuais,
    - análise da acção correctiva,
    - implementação de medidas correctivas,
    - auditoria de segurança cibernética,

- detecção de anomalias ou ataques cibernéticos,
- responder a ataques informáticos ou outros incidentes,
- processos para assegurar a continuidade,
- treino e exercícios, etc.

- Em retrospectiva, a implementação da segurança cibernética requer a aplicação ou modificação tanto da tríade CIA como dos sub-elementos de segurança cibernética ao longo do seu ciclo de vida. Em particular, a prevenção, detecção e resposta a ataques. [116]
- O Data BreachInvestigations Report[117] , que analisa as violações de segurança que levam ao compromisso de dados, para 2017, mostra o seguinte:
- o atacante foi
  - **pessoa não organizativa - 73 %.**
  - pessoa na organização - 28 %.
  - **grupo de crime organizado - 50%**
- o atacante foi utilizado para os ataques:
  - **hacking - 48 por cento.**
  - **malware - 30%**
    - **49% do malware** foi distribuído e depois instalado pelo atacante **via e-mail**
  - **engenharia social - 43**
  - assalto físico - 8%[118]
- As vítimas são organizações que operam em:
  - cuidados de saúde - 24 %.
  - sector público (tipicamente governo estatal e local, etc.) - 14%
- o motivo do ataque:
  - **enriquecimento - 76%**
  - aquisição de dados e informações (espionagem) - 13%
- **68% dos ataques foram detectados após vários meses ou mais**
- **De acordo com um relatório da NationalCyber and Information Security Authority**, *"**é de esperar um maior crescimento das ameaças cibernéticas em 2018, especialmente** mais ataques de phishing da próxima geração, ataques a mercados, carteiras e trocas de moeda criptográfica, variantes de resgate sem ficheiros, utilização de inteligência artificial para ataques cibernéticos, ataques a dados em soluções de Cloud, ataques a IoT, sistemas industriais, etc. **Espera-se que o número de entidades estatais ou patrocinadas pelo Estado em ataques cibernéticos aumente e que as fugas maciças de dados pessoais, palavras-passe e dados de acesso continuem.** Por conseguinte, é essencial construir segurança cibernética para sistemas TIC críticos para o funcionamento do Estado e das suas infra-estruturas críticas".*[119]

---

[116] Para mais detalhes, ver SVOBODA, Ivan. *Soluções de segurança cibernética.* Palestra na Academia CRIF. (23. 9. 2014)
[117] *Relatório de Investigação de Violação de Dados de 2018. 11th Edição.* [Online]. [citado 2018-07-28]. Disponível em: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.
[118] Os ataques isolados envolvem geralmente uma combinação de técnicas e ferramentas.
[119] *2017 Relatório do Estado da Ciber-segurança* [online]. [citado 2018 Jun 29]. Disponível em: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

- "A ciber-segurança também ajuda a identificar, avaliar e combater as ameaças cibernéticas, mitigar os riscos cibernéticos e eliminar os efeitos de ataques cibernéticos, crimes de informação, terrorismo cibernético e espionagem cibernética no reforço da confidencialidade, integridade e disponibilidade de dados, sistemas e outros elementos da infra-estrutura das TIC".
- **O principal objectivo da segurança cibernética é proteger o ambiente para a realização dos direitos humanos à informação**". [120]
- O Cybersecurity Interpretive Dictionary define risco como: *"(1) Perigo, a possibilidade de dano, perda, falha. (2) O impacto da incerteza na realização dos objectivos. (3) A possibilidade de uma ameaça explorar uma vulnerabilidade de um recurso ou grupo de activos e causar danos a uma organização".*[121]
- **O risco** também **pode** ser definido como o **potencial de uma ameaça para se materializar e explorar uma vulnerabilidade de um bem**. De acordo com o artigo 4(9) do SRI, **risco é definido** como ***"qualquer circunstância ou evento razoavelmente identificável que possa afectar negativamente a segurança das redes e sistemas de informação.*** No ciberespaço, os riscos são expostos aos utilizadores, aos sistemas e aplicações informáticas que os utilizam, e a outros elementos das TIC.
- O termo **risco expressa a probabilidade de um evento indesejável**. O grau de probabilidade com que este evento irá ocorrer é expresso através de uma análise de risco. Os valores-padrão mínimos para os métodos de identificação, análise, avaliação e investigação do risco são especificados na norma EN 31010.
- Valášek et al.[122] relatam que a avaliação de risco é geralmente baseada em três questões básicas:
  Que coisas más (indesejáveis) podem acontecer? O que pode correr mal?

  Qual é a possibilidade/probabilidade de isto acontecer?

  Quão graves (intensidade, magnitude, etc.) podem ser os efeitos (impactos, consequências)?
- É calculado um nível de materialidade de risco para cada risco, que pode ser expresso da seguinte forma:
  Importância do risco = **Impacto do risco** * **Probabilidade de** ocorrência do risco

- **Um bem é qualquer coisa de valor para uma pessoa, organização ou país.**
- Um bem pode ser uma **coisa tangível** (edifício, sistema informático, rede, energia, bens, etc.) **ou uma coisa intangível** (informação, conhecimento, dados, programas, etc.) de uma perspectiva de direito civil.
- No entanto, um bem pode também ser uma **propriedade** (por exemplo, disponibilidade e funcionalidade do sistema e dos dados, etc.) ou **reputação,** etc. **As pessoas** (utilizadores, administradores, etc.) e os seus conhecimentos e experiência são também uma mais-valia do ponto de vista da segurança cibernética.
- De acordo com a Secção 2(f) e (g) da VoKB, os **activos são** divididos em **activos auxiliares** e **essenciais.**

---

[120] *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [citado 2018-07-01]. Disponível em: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[121] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 99. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[122] VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Gestão de crises em situações de emergência não-militares*. Praga: MinistryInterior Affairs - General Directorate of the Fire and Rescue CorpsRepublic of the Czech Republic, 2008 [online]. [citado 1 de Julho de 2018]. Disponível a partir de: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx.
ISBN 978-80-86640-93-8 pp. 73

- **Os meios de apoio** são recursos técnicos, empregados e empreiteiros envolvidos na operação, desenvolvimento, gestão ou segurança de um sistema TIC.
- **O principal activo** é a informação ou serviço processado ou fornecido pelo sistema TIC.
- Vulnerabilidade significa uma fraqueza num bem, software ou segurança que é explorado por uma ou mais ameaças
- A vulnerabilidade, tal como o perigo, pode ser causada por uma variedade de factores, que consistem em acção humana, falha técnica ou possivelmente força maior.
- No domínio da segurança cibernética, as vulnerabilidades dividem-se em:
- **buracos de segurança conhecidos** (publicados)
    - **corrigido** (**fixo**) - um caso típico são as vulnerabilidades de software para as quais o fabricante já emitiu uma actualização
    - **não corrigida** - a entidade afectada (fabricante, administrador, etc.) conhece a vulnerabilidade, mas não teve o cuidado de a corrigir
- **vulnerabilidades desconhecidas**
    - escondido
    - não descoberto
- O Decreto de Segurança Cibernética no Anexo 3 lista algumas vulnerabilidades a título de exemplo. **De acordo com** este **decreto, as vulnerabilidades são:**
    - manutenção inadequada do sistema de informação e comunicação,
    - a obsolescência do sistema das TIC,
    - protecção insuficiente dos circuitos externos,
    - falta de consciência de segurança entre utilizadores e administradores,
    - configurações incorrectas dos direitos de acesso,
    - procedimentos inadequados para a identificação e detecção de eventos de segurança adversos, incidentes de segurança cibernética e incidentes de segurança cibernética,
    - monitorização inadequada dos utilizadores e administradores e falha na detecção de comportamentos inadequados ou problemáticos,
    - definição insuficiente das regras de segurança, definição imprecisa ou ambígua dos direitos e responsabilidades dos utilizadores, administradores e funções de segurança,
    - protecção insuficiente dos bens,
    - arquitectura de segurança inadequada,
    - controlo independente insuficiente,
    - não detecção atempada da má conduta do empregado.
- Uma ameaça pode muito simplesmente ser definida como algo capaz de perturbar o estado normal ou ordeiro e interferir com os direitos dos outros. É uma acção negativa que pode ou não ser realizada. Para uma definição adequada, é suficiente que a possibilidade de um estado de coisas negativo seja iminente e real.
- De acordo com a dicção do Ministério do Interior da República Checa, uma ameaça é considerada "*qualquer fenómeno que tenha a capacidade potencial de prejudicar os interesses e valores protegidos pelo Estado". O grau de ameaça é determinado pela magnitude do dano potencial e pela*

distância temporal (geralmente expressa em termos de probabilidade ou risco) da possível aplicação desta ameaça".[123]

- O termo real ameaça **é** definido como "a *causa potencial de um evento não intencional que possa causar danos a um sistema ou organização".* [124]
- Directamente relacionado com este conceito básico está o termo risco de segurança da **informação**[125] , que é definido como "*a causa potencial de um evento adverso que possa resultar em danos a um sistema e aos seus activos, tais como destruição, acesso não desejado (compromisso), modificação de dados ou indisponibilidade de serviços*". [126]
- Para além dos dois termos acima, os autores definem os termos **ameaça activa, ameaça passiva e ameaça avançada e persistente** no glossário. [127]

- O Dicionário Oxford afirma que uma **ameaça cibernética é a possibilidade de uma tentativa maliciosa de danificar ou perturbar uma rede ou sistema informático.**[128] Um sistema, neste contexto, é um sistema informático.
- **Uma ameaça** cibernética também **pode** ser definida como uma acção destinada a alterar a informação[129] , aplicações ou o próprio sistema.
- Jirovský define quatro grupos de ameaças básicas e caracteriza as suas relações:[130]
    - **A fuga de informação** é quando a informação protegida é revelada a uma parte não autorizada.
    - **Uma violação da integridade** é a corrupção, alteração ou apagamento de dados.
    - **A supressão de serviços** significa impedir deliberadamente o acesso à informação, a uma aplicação ou a um sistema.[131]
    - **A utilização ilegal** é a utilização de informação por uma parte não autorizada ou de uma forma não autorizada.[132]
- Existem muitas classificações de ameaças cibernéticas, sendo a mais comum:

1. Fontes de perigo

a) **Perigos causados pelo homem.** Se o perigo for provocado pelo homem, o foco deve ser também a forma de culpabilidade que levou ao início do perigo. Nesta perspectiva, os perigos podem ser distinguidos :

- **causouecelowo,**

As ameaças cibernéticas deliberadamente causadas incluem, por exemplo:

- eliminação deliberada de dados, configurações do sistema, etc,

[123] *Jeopardy.* [online]. [citado 2018-07-28]. Disponível em: http://www.mvcr.cz/clanek/hrozba.aspx.
[124] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 52. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.
[125]Neste caso, podemos notar um problema com a tradução de alguns termos do inglês e vice-versa. Se quisermos traduzir consistentemente o termo Ameaça à segurança da informação, o equivalente checo correcto é, por exemplo, ameaça à segurança da informação; ameaça à segurança da informação, etc.
[126] Ibid p. 25
[127] Ibid, pp. 16, 81 e 87
[128] *Ameaça cibernética.* [online]. [citado 2018-07-06]. Disponível a partir de: https://en.oxforddictionaries.com/definition/cyberthreat.
[129] Alterar também significa roubar informação, destruí-la ou impedir a sua utilização.
[130] Cf. JIROVSKÝ, Václav. A *cibercriminalidade não é apenas sobre hacking, cracking, vírus e trojans sem segredos.* Praga: Grada Publishing, a. s., 2007. p. 21 ff.
[131] Estes incluem ataques tais como **DoS - Denial of Service**, DDoS- **Distributed Denial of Service**, etc. Mais detalhes podem ser encontrados no livro KOLOUCH, Jan. *Cibercriminalidade.* Praga: CZ.NIC, 2016, p. 295 ff.
[132] Por exemplo, um sistema baseado em taxas é comprometido e os seus serviços são utilizados sem pagamento por serviços.

- danos físicos a um sistema informático ou outro componente das TIC,
- roubo de dados e informações,
- ataques informáticos (malware, DoS, DDoS, phishing, espionagem não autorizada, etc.).[133]

- **causado por negligência.**

Os riscos cibernéticos causados por negligência / descuido incluem:

- dados apagados acidentalmente,
- danos físicos a um sistema informático ou outro item de comunicação de dados
- danos em dados, sistemas ou outros elementos devido a falta de conhecimento de actos internos (legais ou técnicos),
- outros erros do utilizador.

b) **Erros técnicos** (por exemplo, erro de software ou hardware).

c) **Vis maior (poder superior)**.

As ameaças cibernéticas causadas por motivos de força maior incluem, por exemplo:

- falha de energia inesperada (a menos que seja um perigo causado por negligência humana),
- acontecimentos naturais (relâmpagos, tempestades, etc.) ou catástrofes (inundações, terramotos, etc.),
- fogo (a menos que se trate de um perigo causado pelo homem).

2. Fontes de acção

a) **Ameaças internas** (a fonte da ameaça está dentro da organização)

b) **ameaças externas** (a fonte da ameaça está fora da organização)[134]

3. Objectivos da ameaça

a) Ataque da tríade da CIA.

- **Confidencialidade** - por exemplo, roubo de dados, dados de acesso e chaves, equipamento informático, etc.
- **Integridade** - erros nas bases de dados, definições de permissões, etc.
- **Disponibilidade** - por exemplo, ataques DoS e DDoS; ataques físicos a servidores e cablagem estruturada; falhas de energia, etc.

b) Ataque ao elemento de segurança cibernética.

- **Pessoas -** ataques de engenharia social (no mundo real, mas também no ciberespaço), phishing, malware, roubo, etc.
- **Tecnologia -** todos os perigos enumerados na Secção 1 desta classificação**.** Tipicamente, os perigos podem actuar:

[133] Sobre ataques cibernéticos individuais ver, por exemplo, KOLOUCH, Jan. O *cibercrime.* Praga: CZ.NIC, 2016, pp. 181 ff.

[134] Mais detalhes podem ser encontrados, por exemplo, em PO`ÁR, Josef. *Ameaças seleccionadas à segurança da informação nas organizações.* [em linha]. [citado 6 de Julho de 2018]. Disponível em: https://www.cybersecurity.cz/data/pozar2.pdf.

- hardware (sistemas de computadores endpoint, servidores, controladores de rede, IoT, etc.).
- bases de dados,
- redes e infra-estruturas de rede,
- software (sistema operativo ou outras aplicações),
- informação e dados armazenados em sistemas informáticos.

- **Processos -** testes não autorizados de segurança ou funcionalidade de processos estabelecidos na organização, etc.

4. Motivação

Se a ameaça for causada por uma acção intencional de uma pessoa, a motivação da ameaça deve ser abordada. Ao analisar a motivação de tais acções, podem ser desenvolvidas acções correctivas como parte do processo de resposta à ameaça, para evitar que esta motivação seja estimulada no futuro.
Consoante a motivação, pode-se observar:

- ameaças aos benefícios financeiros,
- ameaças, a fim de ganhar uma vantagem competitiva,
- ameaças, a fim de provar as suas capacidades,
- ameaças em retaliação,
- perigos de incumprimento.[135]

5. Tipo de perigo

- engenharia social,
- botnet,
- malware,
- resgate,
- spam/fraude,
- ofertas fraudulentas,
- phishing, pharming, spear phishing, vishing, smishing,
- hacking,
- farejar,
- DoS, DDoS, DRDoS ataca,
- divulgação de conteúdos nocivos,
- roubo de identidade,
- APT (Advanced PersistentThreat),
- o ciberterrorismo,
- extorsão cibernética.

O Decreto de Segurança Cibernética no Anexo 3 enumera algumas das ameaças a título de exemplo. **De acordo com** este **decreto, uma ameaça é:**

- violação da política de segurança, actividades não autorizadas, abuso de privilégios por parte de utilizadores e administradores,
- falha ou avaria do equipamento técnico e/ou software,

[135] Contra o que se deve proteger? - Ameaças à segurança, eventos, incidentes. [Online]. [citado 2018-07-06]. Disponível a partir de: https://www.kybez.cz/bezpecnost/pred-cim-chranit

- uso indevido da identidade,
- utilização do software em violação das condições da licença,
- código malicioso (por exemplo, vírus, spyware, cavalos de Tróia),
- violações de segurança física,
- interrupção dos serviços de comunicações electrónicas ou do fornecimento de electricidade,
- utilização indevida ou modificação não autorizada de dados,
- perda, roubo ou dano de um bem,
- o não cumprimento de uma obrigação contratual por parte do fornecedor,
- má conduta por parte dos empregados,
- utilização indevida de recursos internos, sabotagem,
- interrupção prolongada dos serviços de comunicação electrónica, fornecimento de electricidade ou outros serviços essenciais,
- falta de pessoal com os conhecimentos necessários,
- ataque cibernético direccionado utilizando engenharia social, utilização de técnicas de espionagem,
- utilização indevida de meios técnicos de armazenamento intercambiáveis,
- intrusão nas comunicações electrónicas (intercepção, modificação).

- Prosise e Mandiva caracterizam um **"incidente de segurança informática"** (que pode ser entendido como um ataque informático ou crime informático) como uma acção ilegal, não autorizada e inaceitável relativa a um sistema ou rede informática. Esta acção pode visar, por exemplo, o roubo de dados pessoais, spam ou outro tipo de assédio, desvio de fundos, distribuição ou posse de pornografia infantil, etc.[136]
- Jirásek et al. definem um ***incidente de*** segurança como *"**um evento que pode causar ou conduzir a uma violação dos** sistemas e tecnologias de informação e das regras definidas para os proteger (política de segurança)".*[137]
- A definição de um evento de segurança também pode ser encontrada na cláusula 3.5 da ISO/IEC 27001, que afirma que tal evento é: *"um **estado identificável de um** sistema, serviço ou rede **que indique uma possível violação da política de segurança ou falha das medidas de segurança"**. Pode também ser qualquer outra situação que não tenha ocorrido anteriormente que possa ser relevante para a segurança da informação".*
- Uma definição semelhante pode ser encontrada no documento NIST, Guia de Tratamento de Incidentes de Segurança Informática 800-61, que afirma que um incidente de segurança é "um *evento com consequências negativas, tais como falha do sistema, inundação de pacotes, utilização não autorizada de privilégios do sistema, acesso não autorizado a dados sensíveis, ou execução de código malicioso que destrói dados*". [138]

---

[136] PROSISE, Chris e Kevin MANDIVA. *Resposta a incidentes e forenses informáticos, 2ª ed.* Emeryville: McGraw-Hill, 2003, p. 13
Cf. mais CASEY, Eoghan. *Evidência Digital e Crime Informático: Ciência Forense, Computadores, e Internet, Segunda Edição.* Londres: Academic Press, 2004, p. 9 inast.

[137] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 28. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[138] *Guia de tratamento de incidentes de segurança informática* **[online]. [citado 2018 Ago 13], p. 6. Disponível em:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

- **Um evento de cibersegurança** é também definido no Artigo 7(1) da Lei de Cibersegurança como *"**um evento que possa causar uma violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas**".*
- De facto, **é um acontecimento sem consequências negativas reais** para o sistema de comunicação ou TI, na realidade é apenas uma ameaça, mas deve ser real.

- A norma ISO/IEC 27001 **fornece** uma definição apropriada de **incidente de segurança da informação**. No artigo 3.6 desta norma, um incidente de segurança da informação é definido como *"um ou mais eventos de segurança não intencionais ou inesperados que tenham uma elevada probabilidade de comprometer as operações de uma organização e de pôr em risco a segurança da informação".*
- Uma definição muito semelhante de **incidente de segurança informática** pode também ser encontrada no documento NIST, Guia de Tratamento de Incidentes de Segurança Informática 800-61, que afirma que é *"uma violação ou ameaça iminente de violação de uma política de segurança, política de utilização aceitável (sistema, serviço) ou práticas de segurança padrão".*[139]
- **Um incidente de cibersegurança** é também definido na secção 7(2) da Cyber Security Act como *"uma **violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas como resultado de um incidente cibernético".*** "
- A dicção da lei deixa claro que um incidente pode ser causado tanto por acção humana intencional como por negligência, mas também por força maior. O que importa é que existe uma **violação da segurança da informação ou dos serviços e dos sistemas de TIC a eles associados.**
- Jirásek et al. definem um ataque cibernético como "Um ataque *às infra-estruturas informáticas para causar danos e obter informação sensível ou estrategicamente importante". É mais frequentemente utilizado no contexto de ataques de motivação política ou militar".*[140]
- **O ciberataque**[141] pode ser definido como **qualquer acção deliberada de um agressor no ciberespaço que seja dirigida contra os interesses de outra pessoa.**
- Ao definir o conteúdo do termo **cibercrime, é importante notar** que à medida que a possibilidade de utilizar as TIC aumenta, aumenta também a possibilidade de as utilizar (abusar) para cometer crimes. Por conseguinte, em princípio, não existe uma definição universal, universalmente aceite, que capte totalmente o alcance e a profundidade deste conceito.
- Nos termos mais gerais, o cibercrime pode ser definido **como uma actividade dirigida contra um sistema informático, rede informática, dados ou utilizadores, ou como uma actividade em que um sistema informático é utilizado como um instrumento para cometer um crime. O facto de** uma rede informática ou ciberespaço ser o ambiente em que esta actividade tem lugar é essencial para a definição de cibercriminalidade a aplicar

- **CERT** (Computer Emergency Response Team) **eCSIRT** (Computer Security Incident Response Team). Embora cada uma destas abreviaturas tenha um significado ligeiramente diferente e, mais importante, uma génese histórica ligeiramente diferente, de facto, hoje em dia ambas as abreviaturas podem ser entendidas como o mesmo tipo de equipa - **uma equipa responsável por lidar com incidentes de segurança e ameaças (cibernéticas) na sua área de operação claramente definida, na**

[139] *Guia de tratamento de incidentes de segurança informática* **[online]. [citado 2018-02-17]**, p. 6**. Disponível em:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
[140] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 71. Disponível em: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.
[141] É necessário distinguir o conceito de incidente de segurança do conceito de ataque informático, que constitui uma violação da segurança SI/TI e das regras definidas para a sua protecção (política de segurança).

perspectiva dos utilizadores ou de outras equipas, um local a que se podem dirigir com um incidente de segurança detectado, solicitando cooperação, partilha de informação, assistência, etc.

- As equipas CERT/CSIRT são constituídas a nível de organizações individuais, tanto organizações que medeiam o funcionamento da Internet (ISP) como organizações que utilizam a Internet para o seu negócio principal (por exemplo, empresas de TI, fornecedores de conteúdos, bancos).
- **A principal responsabilidade de qualquer equipa CSIRT é responder a uma ameaça ("resposta") e cooperar na resposta a incidentes.** Uma equipa CSIRT lida geralmente com um problema que ocorre na sua área de responsabilidade (por exemplo, a sua própria infra-estrutura de rede), ou seja, onde tem uma oportunidade real de intervir.
- Isto não é nada de revolucionário e é praticamente inexistente; cada grande organização, ISP ou fornecedor de serviços tem uma equipa de segurança. **A principal diferença entre uma equipa de segurança regular e uma CERT/CSIRT é o compromisso com uma infra-estrutura de segurança global**, a **partilha de informação dentro** dessa infra-estrutura **e a aderência aos procedimentos formais estabelecidos.**
- Em cada país, **as equipas de cimeiras nacionais** e **governamentais** globais **têm** um **papel** importante e **específico a desempenhar**, ao qual será dedicada uma subsecção separada.
- **Um requisito básico da** comunidade **é que o CERT/CSIRT anuncie publicamente os seus dados de contacto e regras de funcionamento:**
    - que é o seu operador,
    - que são os seus membros,
    - Como e quando a equipa pode ser contactada,
    - os **serviços que** oferece.

  O âmbito (número AS[142] , rede, domínios, serviços) em que a equipa está autorizada a actuar e como, ou seja, a definição da sua autoridade e responsabilidade. Com base no âmbito, a equipa é então contactada (por exemplo, pelos atacados) e resolve as questões relevantes (incidentes).
- O termo **resolução de incidentes de segurança** pode variar em especificidade dependendo da configuração da equipa e das suas políticas internas - pode ser a simples eliminação do ataque (desactivando a fonte do problema, por exemplo, desligando o sistema informático comprometido da rede), rastreando o atacante, restaurando rapidamente o funcionamento do serviço/rede atacado, etc.
- Para que uma equipa se chame oficialmente CERT/CSIRT, deve antes de mais oferecer o serviço de resolver ou coordenar a resolução de incidentes de segurança dentro do seu âmbito definido, concretizando assim a ideia de 'resposta' tal como utilizada nas siglas CERT/CSIRT, ou seja, deve ser capaz de *responder a um* incidente de segurança.
- De uma perspectiva 'externa', uma equipa torna-se uma CERT/CSIRT quando é aceite como tal por outras equipas CERT/CSIRT existentes no mundo. O caminho para se tornar uma equipa CERT/CSIRT não é complicado, no início da viagem é suficiente para declarar em termos claros o seguinte:

1. **Informações básicas de contacto** - nome da equipa, nome da organização que dirige a equipa, -endereço(s) de correio electrónico da equipa onde os incidentes de segurança podem ser comunicados ou a equipa pode ser contactada, número(s) de telefone da equipa, endereço do escritório, nomes dos membros da equipa, horas em que a equipa pode ser contactada, etc.

[142] **AS** - Sistema Autónomo. Um sistema autónomo é um conjunto de redes e encaminhadores IP sob uma gestão técnica comum que representa uma política comum de encaminhamento para a Internet.

2. **Âmbito da equipa** - define o que é da responsabilidade da equipa e qual é o seu papel. Isto, claro, depende do tipo de equipa que é. É possível criar equipas de aproximadamente os seguintes tipos:
   - ***Interno*** - funciona e é responsável por uma rede específica (por exemplo, uma gama específica de endereços IP, domínios), e é normalmente configurado pelo operador de rede,
   - ***Coordenação*** **-** uma equipa cuja principal tarefa é coordenar a resolução de incidentes de segurança, e não resolvê-los,
   - ***fornecedor -*** a equipa que lida com incidentes de segurança que envolvem um produto específico (SW),
   - ***nacional, governamental*** - casos especiais baseados nos princípios das duas primeiras equipas mencionadas (interna e coordenação), o seu âmbito e papel dependem do fundador e muitas vezes da legislação do país específico.
3. **Serviços oferecidos - No mínimo, o** CERT/CSIRT deve gerir um serviço de resposta a incidentes de segurança.

- **A base organizacional** é a referida "prontidão" para resolver o problema, ou seja, definir as regras básicas da equipa, para que cada membro da equipa conheça o seu papel, deveres e responsabilidades, política de tratamento de incidentes de segurança, regras de comunicação, partilha e troca de informações, cooperação, etc. A base nesta área é geralmente bem gerida, a chamada ***gestão de incidentes.***
- As CERTs/CSIRTs são criadas numa base voluntária e têm interesse em comunicar eficazmente umas com as outras, partilhar informação e conhecimentos relevantes, e cooperar. É por esta razão que as equipas se reúnem em organizações internacionais. Actualmente, as organizações mais conhecidas e activas que lidam com esta questão e criam o ambiente apropriado para alcançar os objectivos acima mencionados são a organização internacional **GÉANT**[143] e **FIRST** (Forum for IncidentResponse and Security Teams)[144] .
- GÉANT, uma organização europeia, tem várias actividades nas quais CERTs/CSIRTs globais podem participar se estiverem interessados:

  TF-CSIRT (Task Force for CSIRT) é um grupo de trabalho que permite às equipas colaborar através de reuniões regulares de dois dias realizadas 3 vezes por ano (o anfitrião desta reunião é geralmente a equipa CERT/CSIRT). Mais informações podem ser encontradas em: https://tf-csirt.org/.

  Formação CSIRT - é utilizada para formar novos membros da equipa CSIRT/CERT ou aqueles que estão prestes a criar uma equipa CERT/CSIRT. É geralmente realizada duas vezes por ano e os formadores são membros experientes de equipas CERT/CSIRT de renome e de outros peritos de segurança de topo. Mais informações podem ser encontradas em: https://tf-csirt.org/transits/.

  TrustedIntroducer[145] - um escritório cujo papel principal é criar confiança entre as equipas CERT/CSIRT e ajudar a estabelecer novas equipas. Mais informação pode ser encontrada em: https://www.trusted-introducer.org/.
- Entre as equipas existentes, deve haver também pelo menos duas equipas (chamadas patrocinadores) que irão apoiar a nova equipa, e nenhuma das equipas existentes pode opor-se à admissão da nova equipa. Se tudo correr bem, a informação da nova equipa é mantida numa lista mantida pelo escritório de TI (e parte dela é tornada pública), a equipa ganha o estatuto de equipa ***listada,*** e a comunidade dá as boas-vindas ao novo membro.
- No caso do FIRST, o procedimento de entrada é muito semelhante, mas termina com a ***adesão e*** não com o estatuto de ***membro.***

[143] A associação foi formada a partir da fusão da TERENA (Trans-EuropeanResearch and Education Networking Association) e da DANTE.
[144] Mais informações sobre o FIRST podem ser encontradas em https://www.first.org
[145] Mais tempo também **TI**.

- Com o TrustedIntroducer, é possível alcançar outros estatutos, mais importantes, nomeadamente ***acreditados*** e ***certificados.*** As diferenças são as seguintes:

  Uma equipa com um estatuto listado ***forneceu*** informações básicas sobre si própria, declarou a sua vontade de se comportar como uma equipa CSIRT e foi aceite pela comunidade.

  Uma equipa com estatuto ***acreditado*** declara o nível de prática desejado pela comunidade e compromete-se com os princípios comuns da TI.

  A equipa ***certificada*** demonstrou então o seu "nível de maturidade" através de um processo de certificação
- Ser uma equipa ***acreditada*** ou ***certificada*** requer um esforço contínuo para manter o estatuto de equipa. Parte deste esforço é a obrigação de manter a informação da equipa actualizada na lista de TI. Não o fazer durante um período de tempo prolongado pode resultar na perda do estatuto da equipa e, no pior dos casos, na expulsão da comunidade.

- Outra organização activa na área da segurança é a **ENISA** (Agência Europeia para a Segurança das Redes e da Informação, http://www.enisa.europa.eu/). Trabalha em estreita colaboração com os Estados-Membros da UE e o sector privado e engloba uma série de actividades, incluindo exercícios pan-europeus de cibersegurança, o desenvolvimento de estratégias nacionais de cibersegurança, cooperação e capacitação entre CERT/CSIRTs, tratando de questões de protecção de dados pessoais e trabalhando no desenvolvimento e implementação de legislação sobre questões de segurança da informação em rede (SRI).
- **As equipas CERT/CSIRT não têm uma hierarquia oficial** que faça com que uma equipa seja superior a outra. **Todas as equipas são iguais em** termos de funcionamento, comunicação, cooperação e partilha de informação e não estão limitadas nestas áreas.
- No mundo das equipas CERT/CSIRT, a **vontade de partilhar informações importantes sobre** incidentes e ameaças é fundamental. Para tal, é essencial que as equipas confiem umas nas outras e que os utilizadores confiem nas suas equipas.

- **Um CERT/CSIRT nacional** actua como **último *recurso* - uma última instância para a qual a assistência e a intervenção podem ser** solicitadas. O seu objectivo (dentro do país ou região onde opera) é actuar como intermediário entre a parte atacada e o iniciador do problema e facilitar uma resolução bem sucedida.

- As equipas dos países não controlam (normalmente) as infra-estruturas físicas, pelo que não têm (ao contrário das equipas internas/institucionais) a possibilidade de intervir directamente. O seu papel é mediar contactos ou coordenar (daí o tipo de equipa de **coordenação**) as actividades de diferentes actores quando o problema é maior e requer a cooperação de vários actores.

- Um CERT/CSIRT nacional tem geralmente a **educação e a cooperação como** parte das suas responsabilidades. Isto inclui tanto a educação do público como o trabalho dentro da infra-estrutura da Internet. O objectivo é apoiar a criação de outras CERT/CSIRT no país, lançá-las internacionalmente e apoiar a implementação de práticas e procedimentos padrão. Tudo isto aumenta consideravelmente a transparência do ambiente e dá àqueles que são atacados uma oportunidade de reparação eficaz.
- **As CERTs/CSIRTs governamentais** centram-se normalmente nas autoridades estatais e locais e em lidar com incidentes que ameaçam a segurança do Estado e dos seus serviços. Uma CERT/CSIRT governamental pode tomar a forma de uma equipa interna com a capacidade de intervir directamente em caso de problema. A sua existência é geralmente apoiada por legislação.

- **O processo de notificação e resolução de incidentes de segurança** (ou realmente "quem devo contactar para notificar ou resolver um incidente de segurança") **pode ser considerado de duas perspectivas.** Do ponto de vista dos **técnicos** (administradores de rede e serviços, membros da equipa de segurança) e do ponto de vista dos **utilizadores**

- Para os **técnicos** (administradores de redes e serviços, membros de equipas de segurança), a resposta à pergunta "quem devo realmente contactar para agir" é bastante óbvia, mas isto vem da experiência e, sobretudo, de um conhecimento muito bom do ambiente da Internet e dos seus princípios básicos, bem como de saber onde encontrar informações de contacto para as várias redes, serviços, domínios, etc. existentes.
- Os Registos Regionais da Internet (**RIR)** armazenam e partilham informações sobre quem foi atribuído um bloco de endereços IP. O mundo está dividido em regiões e cada RIR (actualmente RIPE, ARIN, APNIC, LACNIC, AFRINIC) atribui endereços IP para a sua região. A região da Europa, Médio Oriente e partes da Ásia é gerida pela RIPE NCC (https://www.ripe.net/).

- O processo de notificação e resolução de incidentes de segurança (***tratamento*** técnico ***de*** incidentes) não é um processo rigoroso, pelo contrário, e muito depende da experiência e por vezes até da criatividade da pessoa que executa o processo. A troca de informação entre equipas é geralmente rápida e eficiente, embora mesmo isto muitas vezes não garanta uma resolução rápida, uma vez que a infra-estrutura global ainda é bastante "esparsa" para tal, e infelizmente há que dizer que o nível das equipas varia.
- **O estado óptimo da infra-estrutura seria se cada endereço IP estivesse ao alcance de um CSIRT oficial.** Nesta situação, porém, a infra-estrutura das equipas CERT/CSIRT está muito longe de estar ao alcance.
- **Da perspectiva de um utilizador comum,** a situação é muito pouco clara e essencialmente confusa. Então, o que deve um utilizador fazer no caso de um incidente de segurança e quem deve contactar? É difícil exigir ao utilizador que conheça as CERTs/CSIRTs, encontre a correcta, estude a sua política de comunicação de incidentes de segurança e tome medidas.
- Em primeira instância, os utilizadores devem **contactar o administrador da sua rede ou serviço** (se o tiverem) ou devem contactar o seu fornecedor de ligação, ou seja, o **helpdesk do ISP ou o seu apoio ao utilizador.** Deve haver um ponto de contacto claramente descrito do lado do ISP, ao qual os utilizadores podem e devem recorrer se forem visados, descobrir um incidente de segurança ou sentir que algo está errado.
- **Existe uma cooperação muito estreita** e troca de informações e dados relevantes **entre a equipa do país e a equipa governamental,** transmitindo assim um problema relatado a ser resolvido por uma equipa à outra ou trabalhando directamente para uma solução.
- **Em geral, contudo, seria desejável que os administradores de redes e serviços e os membros das equipas de segurança dominassem e aplicassem os princípios do processo de tratamento de incidentes e maximizassem a comunicação directamente** (não através de equipas de nível superior). Isto torna o processo de tratamento de incidentes rápido e eficiente; etapas intermédias adicionais podem introduzir atrasos e, infelizmente, perturbações. Mas, como mencionado, isto depende da gravidade da situação e do problema a ser resolvido

- **As CERTs/CSIRTs e as suas infra-estruturas não são geralmente abrangentes e não representam segurança "em poucas palavras".**

- Em 6 de Julho de 2016, a Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas para um elevado nível comum de segurança das redes e sistemas de informação na União (Directiva NIS) foi adoptada pelo Parlamento Europeu.

- Com base na Lei de **Ciber-Segurança** na **República Checa, duas equipas** CERT/CSIRT **são obrigatoriamente estabelecidas: uma nacional e uma governamental.** Cada uma destas equipas tem direitos e responsabilidades legais estritamente definidos (§ 17 et seq. da Lei CERT).
- A Directiva SRI prevê medidas legais para aumentar o nível global de segurança cibernética na UE, garantindo:
    - O grau de preparação dos Estados-Membros, exigindo-lhes que estejam adequadamente equipados. Por exemplo, numa Equipa de Resposta a Incidentes de Segurança Informática (CSIRT) e numa autoridade nacional competente em matéria de NIS,
    - cooperação entre todos os Estados-Membros através da criação de um grupo de cooperação para promover e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros.
    - cultura de segurança em sectores que são fundamentais para a nossa economia e sociedade e dependem fortemente das TIC, tais como energia, transportes, água, banca, infra-estruturas dos mercados financeiros, cuidados de saúde e infra-estruturas digitais.
- Os Estados-Membros adoptaram abordagens diferentes na implementação dos NEI.

3. Durante as aulas

<u>Algumas ideias para actividades:</u>

WORKSHOPS

1. Analisar a necessidade de uma equipa de segurança dentro da organização.
2. Definição de activos individuais e análise SWOT em relação a eles.
3. Criação e integração da equipa de segurança na organização - adopção de regras e políticas.
4. Simulação de um incidente ou evento cibernético dirigido contra uma organização.
5. Gestão de incidentes.
6. Análise das medidas tomadas.
7. Partilha de informação com outros.

PERGUNTAS DE REVISÃO

1.

- O que é a tríade da CIA?
- Como pode ser definida a segurança cibernética?
- Quais são os elementos da segurança cibernética?
- O que se entende por bens?
- Como pode ser definida uma vulnerabilidade?

2.

- O que é uma equipa CSIRT/CERT?
- Como é formada e estabelecida uma equipa CSIRT/CERT?
- Qual é o foco da equipa nacional do CSIRT?
- Qual é o foco da equipa do CSIRT do governo?
- Quais são os requisitos básicos da comunidade para uma equipa CSIRT/CERT?

3.

- Existe uma hierarquia entre as equipas CSIRT/CERT?
- Como é definido o âmbito da equipa CSIRT/CERT?
- Quem é a equipa do CSIRT/CERT do governo?
- Quem é a equipa nacional CSIRT/CERT?
- Quais são as funções e responsabilidades de outras equipas CSIRT/CERT?
- Como são constituídas as equipas CSIRT/CERT no seu país?

Trabalhar em pares/grupos

- **Pares - mini-projecto**
  Em pares, os estudantes escolhem um dos tópicos discutidos. Eles escrevem as suas conclusões e apresentam-nas aos outros. Após a apresentação, os outros estudantes preparam perguntas adicionais para o grupo de apresentação.

- **Mapa de pensamentos**
  Os estudantes em pares escolhem um dos tópicos abordados e criam um mapa mental, que depois descrevem aos outros estudantes numa breve apresentação.

- **Palavras-chave**
  Os alunos em pares seleccionam individualmente palavras-chave a partir do glossário.

Eles escrevem as definições destas palavras em tiras de papel. Viram as tiras de papel com o lado em branco para cima. Um aluno escolhe uma tira, lê a definição e o outro aluno procura uma palavra-chave correspondente.
ou
Os alunos escrevem algumas palavras-chave do glossário num pedaço de papel. Eles viram os cartões com o lado em branco para cima. Um estudante pega no primeiro cartão e diz o que a palavra significa. O segundo aluno adivinha a palavra-chave.

- 10 palavras-chave

  Os estudantes escolhem 10 palavras-chave relacionadas com o tema escolhido. Estas 10 palavras-chave são dadas a outros pares. Os pares escrevem um texto que deve conter todas as palavras-chave. Uma frase só pode conter uma palavra-chave. Assim, o texto consiste em pelo menos 10 frases-chave.

- Painel de discussão

  Os alunos escolhem 3 oradores. Cada orador escolhe um tópico para discutir. Os outros estudantes fazem perguntas sobre os tópicos. Cada orador pode usar um tipo de resposta - TRUE X FALSE. O estudante recebe um ponto para cada resposta verdadeira, por exemplo, GDPR significa Regulamento Geral de Protecção de Dados? - VERDADEIRO X FALSO.

4. Recursos da Internet

Ver bibliografia abaixo

5. Perguntas/testões adicionais

SELECCIONAR A RESPOSTA CORRECTA:
(A resposta correcta foi destacada)

1. _____ é um conjunto de medidas tomadas para proteger um sistema informático contra acesso ou ataque não autorizado.

   a) Cybersafe
   (b) Segurança no ciberespaço
   c) Cibersegurança
   d) Ciber-segurança

2. Os elementos de segurança cibernética incluem: _____

   (a) Pessoas, tecnologia, processos

   (b) realidade, software, hardware

   (c) fornecedores, virtualidade, procedimentos

   (d) Utilizadores, tecnologia, questões

3. _____ refere-se a uma situação em que apenas aqueles que estão autorizados a fazê-lo têm acesso a informação, dados ou TIC.

   (a) Credibilidade
   b) Realidade
   (c) Autenticidade
   (d) Confidencialidade

4. É calculado um grau de materialidade de risco para cada risco, que pode ser expresso da seguinte forma:
   a) Significado do risco = Impacto do risco * Probabilidade de ocorrência do risco
   (b) Significado do risco = Gama de risco * Probabilidade de risco.
   c) Significado do risco = Impacto do risco * Possibilidade de ocorrência do risco
   d) Significado do risco = Questões de risco * Probabilidade de ocorrência de risco

5. _____ são recursos técnicos, empregados e fornecedores envolvidos no funcionamento, desenvolvimento, administração ou segurança do sistema de TIC.

   (a) Património subjacente
   (b) Bens ordinários
   (c) Recibos
   (d) Activos auxiliares

6. _____ refere-se a um ponto fraco de um recurso, software, segurança que é explorado por uma ou mais ameaças.

   a) Fragilidade
   (b) Vulnerabilidade

c) Fraqueza
(d) Dúvidas

7. _____ é a possibilidade de uma tentativa maliciosa de danificar ou perturbar uma rede ou sistema informático.

a) Ameaça cibernética
(b) Cibercultura
c) Poder cibernético
d) Cibercriminalidade

8. **O que é que** significa **CSIRT**?

(a) Equipa de resposta a emergências informáticas
(b) Resposta da equipa a incidentes de segurança informática
(c) Equipa de Resposta a Emergências Informáticas
(d) Equipa de Resposta a Incidentes de Segurança Informática

9. As equipas CERT/CSIRT não têm uma hierarquia oficial que faça com que uma equipa seja superior a outra. Todas as equipas são _____ em termos de funcionamento, comunicação, cooperação e partilha de informação e não estão limitadas nestas áreas.

(a) diferente
(b) estável
(c) Igual
(d) Não especificado

10. Os Estados-Membros adoptaram _____ abordagens à implementação dos SRI.

(a) o mesmo
(b) idênticos
(c) Junção
(d) Diversos

11. O que representa o CIS?

a) Cuidados, influência, acessibilidade
(b) Confidencialidade, integridade, disponibilidade
c) Cooperação, Integridade, Acessibilidade
d) Impacto, credibilidade, acessibilidade

12. A diferença entre uma equipa de segurança normal e uma CERT/CSIRT é principalmente o envolvimento na infra-estrutura _____**,** o intercâmbio de informação dentro desta infra-estrutura e a aderência aos procedimentos formais estabelecidos.

(a) Segurança nacional

(b) agitação global

(c) A ameaça global

(d) Segurança global

13. O que é que a ENISA representa?

(a) A Agência Europeia para a Segurança das Redes e da Informação
(b) A Agência Europeia para a Segurança dos Netsurfers e da Informação
(c) a Agência Europeia de Negociações e Segurança da Informação
(d) Agência Europeia para a Segurança Nacional e a Informação

14. _____ - uma equipa dedicada à resolução de incidentes de segurança que afectam um produto específico.

a) Interno
b) Governo
(c) Vendedor
(d) Coordenação

Bibliografia

1. *Relatório de Investigação de Violação de Dados de 2018. 11th Edição.* [Online]. [citado 2018-07-28]. Disponível em: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.
2. *Análise de risco [*online]. [citado 2018-07-01]. Disponível em: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/.
3. ANDRESS, Jason. *Fundamentos da segurança da informação*. 2ª Edição. Singressos. 9780128007440
4. CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Segunda Edição.* Londres: Academic Press, 2004, pp. 9 e seguintes.
5. *Metodologias da CIA.* [em linha]. [citado 2018-07-10]. Disponível em: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png.
6. *Guia de tratamento de incidentes de segurança informática* **[online]. [citado 2018 Ago 13]**, p. 6**. Disponível em:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
7. *Ciber-segurança.* [em linha]. [citado 2018-07-06]. Disponível em: https://en.oxforddictionaries.com/definition/cybersecurity Tradução do autor.
8. *Ciber-segurança.* [em linha]. [citado 2018-07-06]. Disponível a partir de: https://www.merriam-webster.com/dictionary/cybersecurity Tradução do autor.
9. *Ameaça cibernética.* [online]. [citado 2018-07-06]. Disponível a partir de: https://en.oxforddictionaries.com/definition/cyberthreat.
10. *Definição de segurança cibernética - lacunas e sobreposições na normalização*. [em linha]. [citado 2017 Dez 10]. Disponível em: https://www.enisa.europa.eu/publications/definition-of-cybersecurity p. 30
11. *ENISA CSIRT modelo de avaliação da maturidade* [online], 2019. VERSÃO 2.0. Atenas, Grécia: Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) [citado 2021-03-16]. ISBN 978-92-9204-292-9. Disponível em: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, p. 6.
12. EVANS, DONALD, PHILIP, BOND e ARDEN BEMET. *Normas para categorizar a segurança da informação federal e dos sistemas de informação.* NationalInstitute of Standards and Technology, Computer Security Resource Center. [online]. [citado 2017 Dez 10]. Disponível em: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.
13. FRANCISCO, Libor. *Estudos de segurança.* [Online]. [citado 2018-07-10]. Disponível em: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf.
14. FRUHLINGER, Josh. *O que é o Stuxnet, quem o criou e como é que funciona?* [online]. [citado 2018-07-01]. Disponível a partir de: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
15. HENDERSON, Anthony. *A Tríade da CIA: Confidencialidade, Integridade, Disponibilidade.* [Online]. [citado 2018]. Disponível em: http://panmore.com/the-cia-triad-confidentiality-integrity-availability.
16. *Jeopardy.* [online]. [citado 2018-07-28]. Disponível em: http://www.mvcr.cz/clanek/hrozba.aspx.
17. HSU, D. Frank e D. MARINUCCI (eds.). *Avanços na segurança cibernética: tecnologia, operações, e experiências*. Nova Iorque: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. p 41.
18. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Dicionário interpretativo de segurança cibernética.* [em linha]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 23 [online]. [citado 2018-07-10]. Disponível em: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.

19. JIROVSKÝ, Václav. A *cibercriminalidade não é apenas sobre hacking, cracking, vírus e trojans sem segredos.* Praga: Grada Publishing, a. s., 2007. p. 21 ff.
20. KADLECOVÁ, Lucie. *Aspectos conceptuais e teóricos da segurança cibernética.* [em linha]. [citado 2018-07-21]. Disponível em: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf.
21. KOLOUCH, Janeiro. *Cibercriminalidade.* Praga: CZ.NIC, 2016.
22. *Segurança cibernética: o que fazer a esse respeito?* [em linha]. [citado 2018 Jun 29]. Disponível em: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html
23. *O pessoal eleitoral de Macron foi atacado por hackers, diz a empresa japonesa anti-vírus.* [online]. [citado 2017 Jun 29]. Disponível:http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san
24. MAREÍSIA, Miroslav. *Segurança.* [Online]. [citado 2018-07-10]. Disponível em: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511.
25. MATUROVÁ, Jana e Miroslav VALTA. *Prevenção de riscos - inspecções do estado do equipamento técnico.* [Online]. [citado 1 de Julho de 2018]. Disponível em: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni.
26. *National Cyber Security Strategy of the Czech Republic 2015-2020 [*online]. [citado 2018-07-01]. Disponível em: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf p. 5
27. *Parkerian Hexad*. [Online]. [citado 2016 Ago. 20]. Disponível a partir de: https://vputhuseeri.wordpress.com/2009/08/16/149/.
28. *PO`ÁR, Josef. Segurança da informação*. Pilsen: AlešČeněk, 2005, p. 37.
29. PO`ÁR, Jozef. *Ameaças seleccionadas para a segurança da informação das organizações.* [Em linha]. [citado em 2018, 6 de Julho]. Disponível em: https://www.cybersecurity.cz/data/pozar2.pdf.
30. PROSISE, Chris e Kevin MANDIVA. *Resposta a incidentes e forenses informáticos, 2ª ed.* Emeryville: McGraw-Hill, 2003, p. 13
31. Contra o que se deve proteger? - Ameaças à segurança, eventos, incidentes. *[Online]. [citado 2018-07-06]. Disponível a partir de: https://www.kybez.cz/bezpecnost/pred-cim-chranit*
32. *A vinda dos hackers: a história de Stuxnet.* [Em linha]. [citado 2018-07-01]. Disponível em: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/.
33. RAK, Roman. Homo sapiens e segurança. ICT Forum/PERSONALIS 2006 [apresentado a 27 de Setembro de 2006]. Praga (apresentação da conferência).
34. SCHNEIER, Bruce. [Online]. [citado 2018-07-18]. Disponível em: https://www.azquotes.com/quote/570039.
35. SCHNEIER, Bruce. [Online]. [citado 2018-07-18]. Disponível a partir de: https://www.azquotes.com/quote/570035.
36. SCHNEIER, Bruce. [Online]. [citado 2018-07-18]. Disponível a partir de: https://www.azquotes.com/quote/570047.
37. SCHNEIER, Bruce. [Online]. [citado 2018-07-18]. Disponível em: https://www.azquotes.com/quote/570040.
38. *Directrizes do SRI.* [em linha]. [citado 1 de Julho de 2018]. Disponível em: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN.
39. SVOBODA, Ivan. *Soluções de segurança cibernética.* Palestra na Academia CRIF. (23. 9. 2014)
40. SÁMAL, Pavel et al. *Código Penal II. §§ 140-421. comentário.* 2ª ed., Pavel et al. Praga: C. H. Beck, 2012, p. 2308

41. Século, Vladimír. *Cibersegurança.* Pilsen: AleščČeněk, 2018. p. 20 e seguintes.
42. *Inteligência: a campanha para influenciar as eleições presidenciais americanas foi ordenada por Putin.* [em linha]. [citado 2017 Jun 29]. Disponível em: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin
43. *A gama completa de serviços de CGI Cyber Security.* [online]. [citado 2018-07-10]. Disponível a partir de: https://mss.cgi.com/service-portfolio
44. *Definições e Aplicações do TrafficLightProtocol (TLP).* [online]. [citado 2018 Jan 13]. Disponível a partir de: https://www.us-cert.gov/tlp.
45. VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Gestão de crises em situações de emergência não-militares*. Praga: Ministério do Interior - Direcção Geral do Corpo de Bombeiros e Salvamento da República Checa, 2008 [online]. [citado 1 de Julho de 2018]. Disponível a partir de: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx.
46. WAISOVÁ, sárka. *Segurança: desenvolvimento e mudanças conceptuais.* Pilsen: AleščČeněk, s.r.o., 2005. ISBN 80-86898-21-0
47. *WannaCry nunca deveria ter-se espalhado em primeiro lugar. Tudo o que precisava de fazer era utilizar o serviço Windows Update.* [online]. [citado 2017 Jun 27]. Disponível em: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx
48. WIENER, Norbert. *Cibernética: ou controlo e comunicação em organismos vivos e máquinas.* Praga: Editora Estatal de Literatura Técnica, 1960. 148 p.
49. *Conceitos básicos.* [online]. [citado 2018-07-10]. Disponível em: https://www.kybez.cz/bezpecnost/pojmoslovi.
50. ZEMAN, Petr et al. *Terminologia de segurança checa: interpretação de conceitos básicos* [online]. [citado 2018-07-10]. Disponível a partir de: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

Módulo 5

Fundamentos da perícia informática

1. Introdução

O módulo cinco é um módulo 'físico' largamente baseado em workshops, que deve ser feito na sala de aula. Os alunos serão apresentados a uma variedade de situações em que tenha ocorrido uma intrusão ou outra ameaça cibernética e terão de chegar ao fundo da questão.

1.1 Resumo do curso

O módulo Fundamentos Forenses Digitais fornece a aplicação teórica e prática destes conhecimentos na recolha, análise e preservação de provas, resultando na sua constituição como prova em tribunal. O conteúdo presente no programa deste módulo, permite consolidar este objectivo.

1.2 Objectivos do curso

Os objectivos deste módulo são fornecer uma compreensão teórica dos conceitos de informática forense e aplicar este conhecimento à recolha, análise e preservação de provas, resultando na sua constituição como prova em tribunal. O conteúdo presente no programa deste módulo, permite consolidar este objectivo do módulo.

1.3 Conteúdo do curso

Devido à sua natureza prática, o curso terá lugar principalmente em aulas físicas sob a orientação de um instrutor. No seminário, os alunos serão desafiados a assegurar uma cena de crime e a obter o maior número possível de pistas claras sobre o curso do incidente, as perdas sofridas e possíveis pistas.

1.4 Objectivos de aprendizagem

- definições básicas
- assegurar provas físicas
- assegurar provas digitais
- utilização de provas em tribunal

1.5 Equipamento e materiais necessários

Sala de computadores com acesso à Internet
1 Disco de caneta (cartão de memória) < 8GB
1 Pen Disk (cartão de memória) > 8GB

1.6 Syllabus

Resultado da aprendizagem	O aluno que completar o módulo com sucesso saberá/ será competente no seguinte.
NOVIDADES	
W1	O estudante conhece modelos de análise forense digital
W2	O estudante conhece a relação entre pistas, provas e crime
HABILIDADES	
U1	O estudante faz relatórios forenses
U2	O estudante no local identifica, recolhe, adquire e assegura provas digitais utilizando uma variedade de técnicas, protegendo a integridade das provas
U3	O estudante aplica as melhores práticas e procedimentos na aquisição e processamento de provas digitais
U4	O estudante está familiarizado com várias técnicas informáticas forenses para a recolha e análise de diferentes tipos de provas digitais, utilizando técnicas e ferramentas específicas
COMPETÊNCIAS	
K1	Poderá servir como membro ou líder da equipa de investigação

Conteúdo do módulo (programa de palestras e outras actividades)	**Referência aos resultados da aprendizagem**
LECTURAS 1. conceitos, definições e modelos WORKSHOPS 1. Assegurar e recolher provas digitais nos locais de crime 2. Procedimentos para a obtenção de provas digitais a. Procedimentos de esterilização b. Técnicas de aquisição 3. Recolha e análise de informação 4. Identificação e análise da informação armazenada nos sistemas operacionais 5. Utilização de ferramentas analíticas OpenSource 6. Estudos de caso em medicina legal digital a. Estudo de caso: Hacking usando ferramentas SO do Windows	W1, W2 U1-4 K1

Métodos de verificação dos resultados da aprendizagem									
Resultado da aprendizagem	**Formas de classes de crédito**								
	Exame oral	Exame escrito	Trabalho escrito parcial	Trabalho final escrito (ensaio, etc.)	Teste	Desenho/apresentação	Relatório	Actividades de sala de aula	Outros ...
NOVIDADES									
W1					x			x	
					x			x	

HABILIDADES									
U1						x		x	
U2						x		x	
U3						x		x	
U4						x		x	
COMPETÊNCIAS									
K1						x		x	

Saldo de crédito ECTS		
Forma de carga de trabalho dos estudantes		Número de horas
Número de horas com participação directa do professor académico		
1.1	Participação em conferências	4
1.2	Participação em seminários	
1.3	Participação em workshops	30
1.4	Participação em actividades laboratoriais	
1.5	Participação em projectos	
1.6	Participação em consultas (2-3 vezes por semestre)	
1.7	Participação na consulta do projecto	
1.8	Participação em exames/teste	2
1.9	Outros ...	
1.10	**Número de horas passadas com assistência directa de pessoal académico (soma 1.1 - 1.9)**	26
1.11	**Número de créditos ECTS obtidos pelo aluno em aulas que requerem a participação directa de um professor académico)**	1
Trabalho individual do estudante		
2.1	Estudos individuais (incluindo palestras de e-learning)	20
2.2	Preparação individual para workshops	10
2.3	Preparação do teste individual	
2.4	Preparação individual para aulas de laboratório	
2.5	Elaboração de relatórios	
2.6	Implementação de tarefas auto-realizadas (projectos, documentação)	
2.7	Preparação para o exame/teste final do seminário	5
2.8	Preparação para exame/teste final de conferências	5
2.9	Outros	
2.10	**Número de horas de trabalho individual (soma de 2,1 - 2,9)**	40
2.11	**Número de créditos ECTS obtidos pelo estudante em trabalhos individuais de ensino**	1,5
Carga de trabalho total (h)		**66**
Créditos ECTS para o módulo		**2,5**

Critérios para avaliar a competência dos estudantes
Os requisitos mínimos para os três grupos de resultados de aprendizagem que o Estudante deve atingir a fim de passar na disciplina são apresentados abaixo de forma sintética. Para que um Estudante passe num módulo, todos os resultados de aprendizagem descritos no programa devem ser verificados positivamente pela(s) pessoa(s) que ensina(m) o módulo.

W - CONHECIMENTO
Avaliação:
Satisfatório - O aluno lembra-se e reproduz os conhecimentos a dominar dentro do módulo.
Bom - O estudante interpreta adicionalmente fenómenos/problemas e é capaz de resolver um problema

típico
Muito bom - O estudante é capaz de resolver problemas mesmo complexos num determinado campo, é capaz de sintetizar, realizar uma avaliação abrangente, criar um trabalho que é original e inspirador para outros.

U - HABILIDADES
Avaliação:
Satisfatório - O aluno conhece a natureza das actividades e é capaz, sob a orientação do professor académico, de realizar actividades / resolver problemas relacionados com o conteúdo do módulo
Bom - O estudante é capaz de realizar actividades / tarefas / resolver problemas típicos relacionados com o conteúdo do módulo
Muito bom - O aluno dominou totalmente a capacidade / habilidade para realizar as actividades / tarefas / problemas previstos no conteúdo do módulo, também em casos mais complexos.

K - COMPETÊNCIA SOCIAL
Avaliação:
Satisfatório - O aluno assimila passivamente o conteúdo do módulo, demonstrando capacidade de concentração e escuta
Bom - O estudante participa activamente nas aulas, faz juízos de valor de acordo com os critérios aceites no domínio em questão, pode cooperar activamente num grupo
Muito bom - O estudante integra a atitude de acordo com o modelo proposto, desenvolve o seu próprio sistema de valores profissionais e sociais, é capaz de assumir a responsabilidade pelas acções do grupo, incluindo a liderança.

2. Material básico para o professor

- Todas as Definições e notas-chave estão incluídas nas apresentações.

3. Actividades

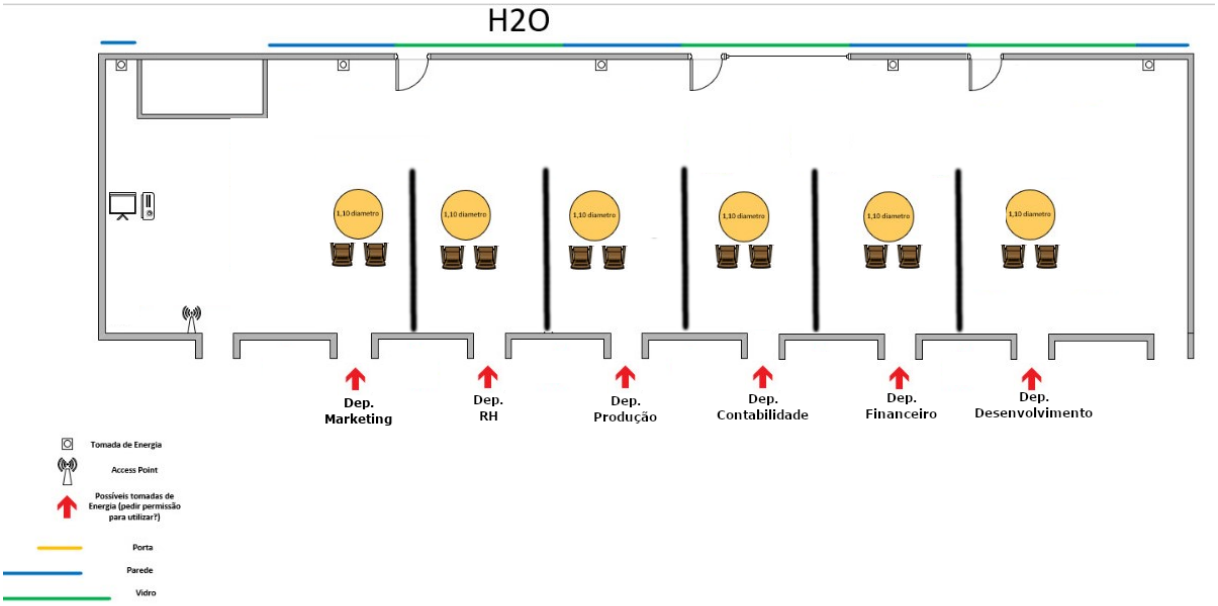
- **Discussão** (entrega de perguntas) - Este tipo de interrogatório é utilizado para levar os alunos a pensar sobre os procedimentos e a importância da perícia digital. Os participantes devem chegar a uma resposta por si próprios ou através de actividades de grupo, tais como brainstorming.

    1- Quando encontramos um documento importante numa pasta de trabalho suspeita, como podemos compreender como esse documento foi guardado nessa pasta? Que artefactos devem ser analisados?
    2- Quando todas as pistas apontam para a utilização da nuvem para armazenar provas importantes, conhecendo as credenciais de um utilizador, será que precisamos de entrar nessa nuvem e analisar os dados aí contidos?
    3- A autópsia com The Sleuth Kit será suficiente para analisar um disco rígido Microsoft Windows? Em que contexto devemos utilizar outras ferramentas?

- **Criação e análise de artefactos** - Este poderia ser um exercício para trabalhar em pares/grupos. O principal objectivo é ter uma equipa a criar apenas um tipo de artefacto digital, partilhando com a outra equipa a actividade que lhe estava associada. A outra equipa, fazendo a análise, recolherá provas forenses desta actividade. Quando obtêm os resultados forenses esperados, invertem os papéis.

- **Criação de páginas para análise de artefactos** - Os sistemas operativos estão sempre a criar novos artefactos que precisavam de ser submetidos a análise forense. Esta análise pode ser informação importante para os investigadores forenses nos seus procedimentos.

- Exercício sobre a cena do crime - O objectivo deste exercício é desenvolver o conteúdo prático relacionado com o funcionamento no local do crime/incidente, bem como o funcionamento em frente a um computador potente (dados forenses em directo). É necessário preparar os seguintes passos:
    1. **Criação do cenário** - Isto começa com o convite / nomeação de estudantes para estarem no local com as ferramentas necessárias para fazerem parte da equipa de recolha de provas forenses. Será necessário preparar o tipo de crime sob investigação, o local de recolha, o equipamento envolvido, etc.
    2. **Preparação dos computadores** - Esta é a etapa mais importante, preparando os computadores com os artefactos necessários que serão recolhidos pelos estudantes. Será necessário criar todos os artefactos e, uma vez preparado o primeiro computador, duplicamos ou clonamos o disco rígido para o número de computadores necessários, de acordo com o cenário.
    3. **Preparar o espaço** - No que diz respeito ao espaço de procedimentos, será imperativo ter o cenário mais realista possível, como qual secção do espaço com o Network Router e a Internet, com as pessoas como cabeças de figura, e assim por diante. Isto ajuda a desenhar o espaço como no exemplo abaixo:



    As instalações podem ser apenas uma sala, mas neste caso a opção era ter 6 equipas a trabalhar ao mesmo tempo, passando menos tempo, mas envolvendo mais pessoas a agir como figurantes e a observar cada equipa.
    4. Avaliação - Cada equipa irá recolher todos os dados e informações necessárias antes de desligar o cabo de alimentação, com confiança na análise forense bem sucedida da caixa morta. O equipamento ficará ao cuidado de cada equipa até que a equipa tenha entregue todo o equipamento e o relatório da análise forense. A avaliação incidirá sobre este relatório.

4. **Recursos da Internet**

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition (ojp.gov) - https://www.ojp.gov/pdffiles1/nij/219941.pdf

NIST SP 800-86 Guia de integração de técnicas forenses na **resposta** a incidentes https://doi.org/10.6028/NIST.SP.800-86

Subcomité sobre Provas Digitais | NIST - https://www.nist.gov/organization-scientific-area-committees-forensic-science/digital-evidence-subcommittee

Grupo de Trabalho Científico sobre Provas Digitais, Digitais e Multimédia (Digital Forensics) como disciplina de Ciência Forense

DFIRScience - YouTube - https://www.youtube.com/c/DFIRScience

Forensics - start.me - https://start.me/p/q6mw4Q/forensics

Formação DFIR - https://dfir.training/

FSIDIIN | Forensic Science International: Digital Investigation | Journal | ScienceDirect.com by Elsevier - https://www.sciencedirect.com/journal/forensic-science-international-digital-investigation

5. **Eventos cíclicos interessantes**
    - **SANS CyberThreatIntelligenceSummit& Training [OnLine].**
    - **IFIP WorkingGroup 11.9 International Conference on Digital Forensics [Arlington, USA].**
    - **General Police EquipmentExhibition& Conference (GPEC Digital) [Frankfurt, Alemanha].**
    - **Techno Security & Digital Forensics [Pasadena, EUA].**
    - **Forensics Asia Expo [Jacarta, Indonésia].**
    - **Forensics Europe Expo [Londres, Reino Unido].**
    - **Cimeira Virtual de Ímanes [OnLine].**
    - **Cimeira de utilizadores de ímanes [Nashville].**
    - **Conferência Nacional sobre o Cibercrime [OnLine].**
    - **Conferência Internacional sobre o Sistema de Justiça e Forense Digital [OnLine].**
    - **International Association of ForensicSciences (IAFS) [Sydney, Austrália].**
    - **CongresoInformatica y Ciberseguridad 2023 [Madrid, Espanha].**
    - **CHICYBERCON [Chicago, EUA].**
    - **DFRWS - Digital ForensicResearch Workshop [Bonn, Alemanha].**
    - **International Association of ComputerInvestigativeSpecialists (IACIS) [Orlando, Florida].**
    - **Conferência ADFSL sobre forense digital, segurança e direito**

6. Perguntas/testões adicionais

https://quizlet.com/ca/750977127/computer-and-digital-forensics-flash-cards/

7. Bibliografia

[1] BUNTING, Steve, The OfficialEnCE: EnCaseCertifiedExaminerStudy Guide, 2012.
[2] GRUNDY, Barry J., The Law Enforcement and ForensicExaminer'sIntroduction to Linux (http://www.linuxleo.com/Docs/linuxintro-LEFE-4.31.pdf), 2017.
[3] CASEY, Eoghan, Digital Evidence and ComputerCrime, Academicpress, 2011.
[4] BROWN, Christopher L. T., Computer evidence: Collection and Preservation, 2nd Edition, 2009.
[5] CARVEY, Harlan, Investigating Windows Systems, 1ª Edição, 2018.
[6] HALE LIGH, Michael, The Art of Memory Forensics: DetectingMalware and Threats in Windows, Linux, e Mac Memory 1st Edition, 2014.
[7] ENISA, Identification and handling of electronic evidence Toolset, Setembro de 2013.
[8] ENISA, Identification and handling of electronic evidence Handbook, Setembro de 2013.
[9] NIST, Computer Security Incident Handling Guide, Publicação Especial 800-61r2.

Módulo 6

Segurança abrangente da rede

1. Introdução

O módulo Comprehensive Network Security centra-se nos métodos de hardware e software de prevenção e detecção de intrusões e ataques. Os métodos apresentados devem ser amplamente utilizados em todas as instituições e o conhecimento dos mesmos é essencial para qualquer pessoa que queira estar envolvida na segurança cibernética.

1.1 Objectivos do curso

Os objectivos deste módulo são apresentar aos estudantes as formas básicas de protecção da rede local em qualquer instituição. Estes métodos estão amplamente disponíveis, não exigem conhecimentos muito especializados e permitem, no entanto, aumentar significativamente a segurança de qualquer rede.

1.2 Conteúdo do curso

A parte da palestra do curso decorrerá principalmente em linha, embora o instrutor possa expandir os tópicos durante as sessões em sala de aula.

1. firewalls
1.1 Introdução às firewalls
1.2 A necessidade de uma firewall
1.3 Tipos e características das firewalls
1.4 Topologias e arquitecturas de parede de fogo
1.5 Exemplos de firewalls

2. sistemas de detecção de intrusão
2.1 Introdução aos sistemas de detecção de intrusão
2.2 Tipos e características dos sistemas de detecção de intrusão
2.3 Arquitecturas de implementação de sistemas de detecção de intrusão
2.4 Sistemas de detecção de intrusão soluções e exemplos comuns

3. sistemas de prevenção de intrusão
3.1 Introdução aos sistemas de prevenção de intrusão
3.2 Tipos e características dos sistemas de prevenção de intrusão

3.3 Arquitecturas de implementação de sistemas de prevenção de intrusão
4 Antivírus
4.1 Introdução ao malware
4.2 Como ocorre uma infeção por malware
4.3 Os tipos mais comuns de malware
4.4 Como detectar, remover e prevenir infeções por malware
4.5 O caso especial do programa antivírus
4.6 Como funciona o programa antivírus
4.7 Escolher o software antivírus certo

1.3 Objectivos de aprendizagem

1. Compreender o papel da Firewall nas tecnologias de cibersegurança, os seus tipos e características, topologias e arquitecturas, e soluções comuns;
2. Compreender o papel dos sistemas de detecção de intrusão nas tecnologias de segurança cibernética, os seus tipos e características, arquitecturas de implementação e soluções comummente utilizadas;
3. Compreender o papel dos sistemas de prevenção de intrusão nas tecnologias de segurança cibernética, os seus tipos e características, arquitecturas de implementação e soluções comummente utilizadas;
4. Compreender o papel do Anti-Malware nas tecnologias de Cyber Security, como o malware se espalha, os diferentes tipos de malware, como detectar, remover e prevenir contra infecções malware, como funciona o caso específico do Anti-Malware - antivírus - e as suas soluções comuns.

1.4 Equipamento e materiais necessários

Sala de computadores com acesso à Internet
Software anti-vírus

1.5 Syllabus

Resultado da aprendizagem	O aluno que completar o módulo com sucesso saberá/ será competente no seguinte.
NOVIDADES	
W1	O aluno conhece o princípio de funcionamento dos sistemas de firewall, IPS, IDS e programas anti-vírus.
W2	O estudante compreende a importância de utilizar salvaguardas apropriadas na sua instituição
HABILIDADES	
U1	Os estudantes poderão aplicar métodos comummente disponíveis para detectar e prevenir intrusões e ataques.
U2	O estudante é capaz de encontrar elos fracos na segurança cibernética de uma instituição
COMPETÊNCIAS	
K1	O estudante é capaz de transferir conhecimentos e competências relativamente à segurança básica para os funcionários da sua instituição.

Conteúdo do módulo (programa de palestras e outras actividades)	**Referência aos resultados da aprendizagem**
LECTURAS 1. firewalls 2. sistemas de detecção de intrusão 3. sistemas de prevenção de intrusão 4 Programas anti-vírus WORKSHOPS 1. configuração da firewall 2. configuração dos sistemas IDS e IPS 3. familiarização com e instalação de software anti-vírus 4. observar as estatísticas de ataque e tirar conclusões	W1, W2 U1, U2 K1

Métodos de verificação dos resultados da aprendizagem									
Resultado da aprendizagem	**Formas de classes de crédito**								
	Exame oral	Exame escrito	Trabalho escrito parcial	Trabalho final escrito (ensaio,	Teste	Desenho/apresentação	Relatório	Actividades de sala de aula	Outros ...
NOVIDADES									
W1					x			x	
W2					x			x	
HABILIDADES									
U1						x		x	
U2						x		x	
COMPETÊNCIAS									
K1						x		x	

Saldo de crédito ECTS		
Forma de carga de trabalho dos estudantes		Número de horas
Número de horas com participação directa do professor académico		
1.1	Participação em conferências	4
1.2	Participação em seminários	
1.3	Participação em workshops	12
1.4	Participação em actividades laboratoriais	
1.5	Participação em projectos	
1.6	Participação em consultas (2-3 vezes por semestre)	
1.7	Participação na consulta do projecto	
1.8	Participação em exames/teste	2
1.9	Outros ...	
1.10	**Número de horas passadas com assistência directa de pessoal académico (soma 1.1 - 1.9)**	18
1.11	**Número de créditos ECTS obtidos pelo aluno em aulas que requerem a participação directa de um professor académico)**	0,5
Trabalho individual do estudante		
2.1	Estudos individuais (incluindo palestras de e-learning)	30
2.2	Preparação individual para workshops	10
2.3	Preparação do teste individual	
2.4	Preparação individual para aulas de laboratório	
2.5	Elaboração de relatórios	
2.6	Implementação de tarefas auto-realizadas (projectos, documentação)	
2.7	Preparação para o exame/teste final do seminário	10
2.8	Preparação para exame/teste final de conferências	5
2.9	Outros	
2.10	**Número de horas de trabalho individual (soma de 2,1 - 2,9)**	55
2.11	**Número de créditos ECTS obtidos pelo estudante em trabalhos individuais de ensino**	2
Carga de trabalho total (h)		**73**

Créditos ECTS para o módulo	2,5

Critérios para avaliar a competência dos estudantes
Os requisitos mínimos para os três grupos de resultados de aprendizagem que o Estudante deve atingir a fim de passar na disciplina são apresentados abaixo de forma sintética. Para que um Estudante passe num módulo, todos os resultados de aprendizagem descritos no programa devem ser verificados positivamente pela(s) pessoa(s) que ensina(m) o módulo.

W - CONHECIMENTO
Avaliação:
Satisfatório - O aluno lembra-se e reproduz os conhecimentos a dominar dentro do módulo.
Bom - O estudante interpreta adicionalmente fenómenos/problemas e é capaz de resolver um problema típico
Muito bom - O estudante é capaz de resolver problemas mesmo complexos num determinado campo, é capaz de sintetizar, realizar uma avaliação abrangente, criar um trabalho que é original e inspirador para outros.

U - HABILIDADES
Avaliação:
Satisfatório - O aluno conhece a natureza das actividades e é capaz, sob a orientação do professor académico, de realizar actividades / resolver problemas relacionados com o conteúdo do módulo
Bom - O estudante é capaz de realizar actividades / tarefas / resolver problemas típicos relacionados com o conteúdo do módulo
Muito bom - O aluno dominou totalmente a capacidade / habilidade para realizar as actividades / tarefas / problemas previstos no conteúdo do módulo, também em casos mais complexos.

K - COMPETÊNCIA SOCIAL
Avaliação:
Satisfatório - O aluno assimila passivamente o conteúdo do módulo, demonstrando capacidade de concentração e escuta
Bom - O estudante participa activamente nas aulas, faz juízos de valor de acordo com os critérios aceites no domínio em questão, pode cooperar activamente num grupo
Muito bom - O estudante integra a atitude de acordo com o modelo proposto, desenvolve o seu próprio sistema de valores profissionais e sociais, é capaz de assumir a responsabilidade pelas acções do grupo, incluindo a liderança.

2. Materiais básicos para o professor

- Todas as definições e notas-chave estão incluídas nas apresentações.

3. Actividades

- Workshop sobre "hacking" de websites com demonstração de como funcionam os sistemas de segurança

- Apresentação de ataques ao vivo e estatísticas sobre quantos destes ataques poderiam ter sido bloqueados por métodos de segurança comummente disponíveis

4. Recursos da Internet

- https://www.parallels.com/blogs/ras/types-of-firewalls/
- https://phoenixnap.com/blog/types-of-firewalls

- https://www.idc-online.com/technical_references/pdfs/data_communications/Firewall_Architectures.pdf
- https://phoenixnap.com/blog/intrusion-detection-system
- https://wisdomplexus.com/blogs/different-types-of-intrusion-detection-systems-ids/
- https://www.educba.com/types-of-intrusion-prevention-system/
- https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- https://www.snort.org/
- https://www.techtarget.com/searchsecurity/definition/malware
- https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

5. Eventos cíclicos interessantes

- Conferência Europeia de Ciber-Segurança (https://eucybersecurity.com/)
- A Cimeira Oficial de Ciber-Segurança (https://cybersecuritysummit.com/)
- Experiência anual do CPX Checkpoint
- Cisco Live ALL IN (https://www.ciscolive.com/emea.html?zid=pp)
- Conferência Internacional sobre Comunicação e Segurança de Redes (http://www.iccns.org/)

6. Perguntas/testões adicionais

- https://quizlet.com/199055325/firewall-flash-cards/
- https://www.proprofs.com/quiz-school/topic/firewall
- https://quizlet.com/180954294/chapter-8-using-intrusion-detection-systems-flash-cards/
- https://quizlet.com/534059481/chapter-7-intrusion-detection-and-prevention-systems-flash-cards/
- https://quizlet.com/222087233/what-is-malware-flash-cards/
- https://quizlet.com/27987027/malware-flash-cards/
- https://www.gns3.com/
- https://www.brianlinkletter.com/open-source-network-simulators/

7. Bibliografia

1. Carter, E., & Hogue, J. (2006). *Fundamentos da prevenção de intrusões*. Cisco Systems.
2. Chapman, D. B., & Zwicky, E. D. (1995). *Construir firewalls para a Internet*. Oreilly & Associates.
3. Grubb, S. (2021). *Como funciona realmente a ciber-segurança: Um guia prático para o total de principiantes*. National Geographic Books.
4. Gupta, B., & Srinivasagopalan, S. (2020). *Manual de investigação sobre sistemas de detecção de intrusão*.
5. Guyer, J. P. (2017). *Uma introdução aos sistemas de detecção de intrusão*. Plataforma de publicação independente Createspace.
6. Komar, B., Beekelaar, R., & Wettern, J. (2003). *Firewalls para manequins*. Para chupetas.
7. Mendoza, H. (2018). *Remover malware, Spyware e vírus do seu PC: Guia para aumentar a segurança e velocidade do seu computador através da remoção de vírus maliciosos, malware, e Spyware*. Cria Espaço Plataforma de Publicação Independente.
8. Noonan, W., Noonan, W. J., & Dubrawsky, I. (2006). *Fundamentos de Firewall*. Cisco Press.
9. Pathan, A. K. (2016). *O estado da arte na prevenção e detecção de intrusões*. Publicações Auerbach.
10. Verissimo, P. E. (2003). *Intrusion-Tolerant Architectures: Concepts and Design* [Tese de Mestrado]. https://www.di.fc.ul.pt/~nuno/PAPERS/TR-03-5.pdf