KOMPLEXNÍ ZABEZPEČENÍ SÍTĚ

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

KOMPLEXNÍ ZABEZPEČENÍ SÍTĚ

6.1 FIREWALLS

6.1.1 Úvod do firewallů

Pojem firewall je dnes hojně používán všemi druhy uživatelů informačních technologií, vztahuje se nejen na počítače, ale i na mobilní zařízení, a podle svého doslovného významu, ohnivé zdi, je dobře znám jako jeden z hlavních bezpečnostních mechanismů zavedených po celém světě.

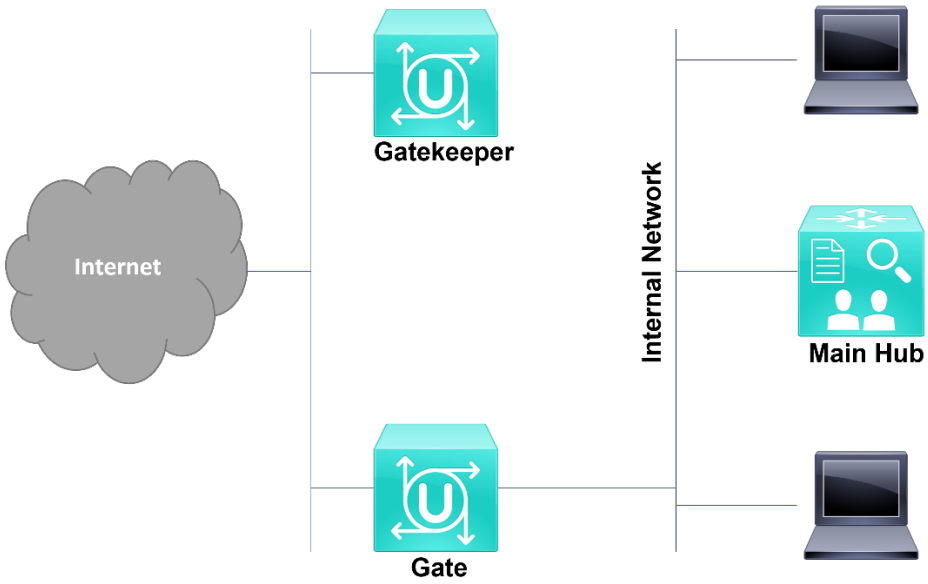
Ačkoli slovo firewall přímo souvisí s informačními technologiemi, nevzniklo s internetem. Používal se již v domech, autech, apod. Jeden z hlavních příkladů souvisí s dveřmi, které brání šíření požáru po budovách, zatímco se ho hasiči snaží dostat pod kontrolu. První firewally byly vyvinuty koncem roku 1980, hned poté, co byl objeven první počítačový virus s názvem "Morris Worm", který ohrozil mnoho velkých organizací, například NASA, univerzity v Berkeley a Stanfordu, a ukázal, že internet už není uzavřenou komunitou a používají ho jen důvěřiví lidé.

Na samém počátku nebyly firewally ničím jiným než jednoduchými směrovači, které byly nakonfigurovány tak, aby rozdělily privátní síť na menší sítě (Local Area Networks neboli LAN), čímž se zabránilo šíření chyb v síti a následně se zlepšil její globální výkon. Tento typ firewallu se používal hlavně v 90. letech a byl založen na pravidlech filtrování, kdy se kladl důraz na IP adresu, což umožňovalo všem zařízením v rámci privátní sítě přístup k internetu nebo veřejné síti (odchozí provoz) a blokovalo vstup veřejných IP adres do privátní sítě LAN. Tyto firewally nebyly tak účinné a byly velmi omezené, protože neposkytovaly vhodný způsob, jak vytvořit silná bezpečnostní a přístupová pravidla, což znemožňovalo omezit přístup konkrétní části aplikace nebo softwaru.

Druhá generace firewallů přišla s možností zkoumat také transportní vrstvu (čtvrtá vrstva OSI), místo aby se omezovala na IP adresu (třetí vrstva OSI). Díky znalostem o aktivních relacích pak firewally mohly tyto informace využít ke zlepšení

šířky pásma sítě a rychlosti a efektivity zpracování paketů. Tím se filtrace prováděla nejen podle IP adresy, ale také podle komunikačních atributů.

Třetí a novější generace firewallů, známá také pod názvem filtrování aplikací, využívá výhod předchozích dvou technologií a je spojena s proxy serverem, který pracuje jako prostředník a vyhodnocuje požadavky každé komunikace, která přichází nebo odchází z našich připojených sítí. Na tento proxy server lze pohlížet jako na vrátného, kdy je umožněno projít pouze osobám, které mají udělena oprávnění pro konkrétní cíl (obrázek 1).



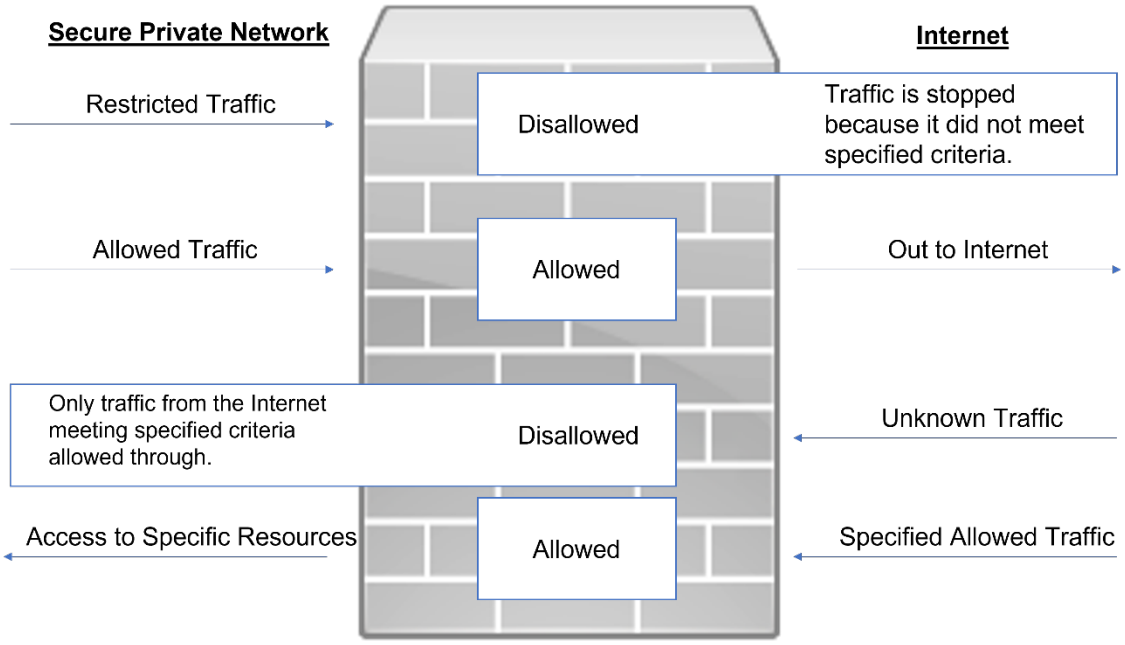
Obrázek 1 - Třetí generace brány firewall

Firewall lze chápat jako jedno nebo více zařízení, včetně softwaru i hardwaru, strategicky umístěných na hranici dvou různých sítí, obvykle nazývaných privátní a veřejná síť (obrázek 2).

Na základě své implementace mezi těmito dvěma sítěmi je schopen kontrolovat a analyzovat všechny síťové pakety, které k němu přicházejí přes různá rozhraní, a chová se jako hraniční kontrolor na letišti, který kontroluje všechny pasy a vízová oprávnění daného paketu a umožňuje mu sledovat nebo ověřovat jeho přístup. Pomocí tohoto hlavního principu tato technologie zabraňuje vstupu nežádoucí komunikace z veřejných do soukromých sítí nebo naopak a následně chrání informace a zdroje v našich soukromých systémech.

Tento typ filtrování navíc dokáže zabránit přístupu interních zařízení k doménám a informacím, které nejsou v souladu se zásadami zabezpečení sítě. U jednoduchých sítí, jako je domácí síť, je brána firewall obvykle implementována v softwaru směrovače. V případě větších sítí, včetně těch podnikových, se důrazně doporučuje použít robustní hardwarovou bránu firewall, která je určena k ochraně hranic sítě, zajišťuje, aby byla povolena pouze nezbytná komunikace a funkce, a zajišťuje bezpečnost sítě.

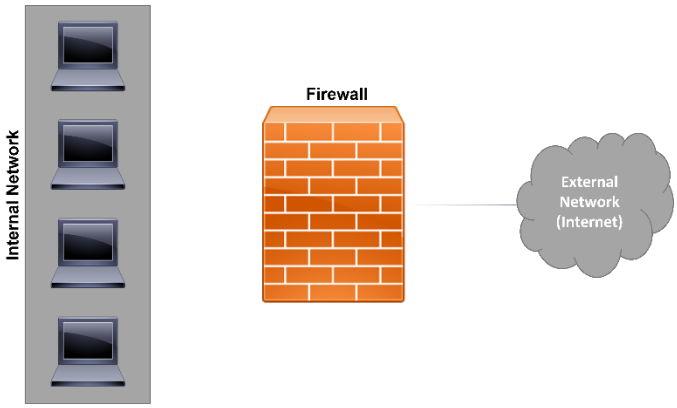
Důležité je také zdůraznit, že aby firewall zabránil útokům na síť, musí být schopen zabránit útokům na sebe sama, a to na obou úrovních, vnitřní i vnější (soukromé i veřejné sítě).



Obrázek 2 - Bezpečnostní řešení umístěné mezi soukromou a veřejnou sítí

Jak již bylo řečeno, firewall může být založen jak na hardwarovém, tak na softwarovém řešení, přičemž nejčastější je druhá možnost, a to nejen z hlediska nákladů a implementace, ale také proto, že je přítomen téměř v každém síťovém systému a osobním počítači. Firewall pracuje na základě souboru pravidel nebo instrukcí a analyzuje síťový provoz, aby určil povolené akce přenosu nebo příjmu dat. Také z jeho doslovného názvu je zřejmé, že systém je v podstatě blokátorem

nežádoucího provozu a povoluje pouze specifický síťový provoz, který se řídí nakonfigurovanými přístupovými pravidly (obrázek 3).



Obrázek 3 - Základní znázornění implementace brány firewall

Souhrnně a nejdůležitěji lze říci, že firewall je bezpečnostní systém, který je schopen chránit privátní síť před vnějšími útoky a zároveň je schopen řídit komunikaci na základě pravidel, která jsou vytvořena s ohledem na bezpečnostní politiku organizace. Je přítomen nejen ve vysokých sítích, jako jsou podnikové sítě, ale také jako software v domácích routerech pro připojení k internetu, stolních počítačích, noteboocích a dokonce i v mobilních zařízeních.

6.1.2 Potřeba brány firewall

Existují různé důvody, proč používat síťový firewall, přičemž ten nejdůležitější se týká ochrany počítačů, serverů a dalších zařízení v rámci privátní sítě. Často lze slyšet, že "nemám žádné důležité informace, které by bylo možné ukrást", ačkoli útoky mohou být prováděny na základě jiných důvodů, jako je využití výpočetního a paměťového výkonu počítačů v rámci sítě, nebo dokonce využití těchto počítačů ke krádeži online informací, přihlašovacích údajů k bankovním účtům a dalších. Mezi nejčastějšími útoky je možné vyzdvihnout např:

- *Následná odpovědnost:*

  Síť může být použita jako přístup k útoku na jiné sítě.
- *Ztráta dat:*

Někteří crackeři získají přístup k síti a mažou soubory a informace ne proto, že by to pro ně byly cenné informace, ale většinou proto, aby ukázali, že jsou toho schopni. To ukazuje na potřebu řádného zabezpečení dat a zálohování informací.

- *Únik důvěrných dat:*

  Ochrana soukromí a zvláštních osobních a jiných důvěrných údajů je v současné době jedním z hlavních problémů v oblasti bezpečnosti dat. Útoky proti systémům a zařízením, které ukládají důvěrné informace, patří k těm hlavním a na jejich ochranu se zaměřují všechny organizace. Zaměřují se nejen na osobní údaje, jako jsou jména a kontakty klientů, ale cílem útoků jsou i důvěrné projekty a citlivé informace. Ochrana těchto systémů je velmi důležitým úkolem, při kterém je třeba pečlivě naplánovat a realizovat bezpečnostní plán.

- *Odmítnutí služby:*

  Bez brány firewall jsou sítě zranitelné vůči útokům, které mohou způsobit různé úrovně poškození sítí a jejich systémů. Velmi častý je také útok typu odepření služby, který může způsobit, že se síť stane nedostupnou a nebude reagovat na komunikaci a systémová volání. Vezmeme-li si příklad nemocnice, kde sítí neustále proudí důležité informace a kde na snadném a rychlém přístupu k těmto informacím závisí lidské životy, může útok typu odepření služby způsobit vážné škody nejen na síti a organizaci, ale také na lidských životech.

Jak je možné v tomto okamžiku pochopit, nechráněná síť otevírá útočníkům možnost získat přístup nebo způsobit škody na informačních a soukromých systémech, převzít nad nimi kontrolu a provádět nejrozsáhlejší možné úkoly proti samotné síti nebo jiným sítím.

Ačkoli je firewall důležitým a významným zařízením, má také svá omezení a nevýhody. Hlavní omezení souvisejí s typem řešení a použitou architekturou implementace. Tato zařízení jsou skutečně významným bezpečnostním zařízením, které je třeba používat, nicméně k dokonalosti mají ještě daleko, přičemž můžeme zdůraznit následující omezení:

- Může zajistit požadovanou úroveň zabezpečení, avšak na úkor výkonu sítě nebo zařízení.
- Bezpečnostní zásady je třeba pravidelně aktualizovat a revidovat, aby nedošlo k ohrožení síťových služeb.
- Nové síťové služby a protokoly nemusí být správně identifikovány a ošetřeny stávajícími firewally.
- Nemusí být schopen řádně chránit soukromou síť před škodlivou činností.
- Nemusí být schopen odhalit škodlivé zasvěcené osoby nebo škodlivou činnost, která pochází od povoleného uživatele.
- Firewall musí být často analyzován a konfigurován, aby útočníci nemohli prozkoumat bezpečnostní mezery.
- Brány firewall nesmí kontrolovat připojení, která jsou přes ně prováděna.

Kromě těchto omezení jsou firewally stále jedním ze sázkových bezpečnostních mechanismů, které je třeba v síti implementovat, aby se zvýšila úroveň jejího zabezpečení, což přináší důležité výhody:

- **Ochrana před zranitelnými službami** - umožňuje pouze specifické a nezbytné síťové a komunikační protokoly.
- **Řízený přístup k interním stránkám a systémům** - zabraňuje přístupu neoprávněných uživatelů a útočníků.
- **Centralizované zabezpečení** - všechny zásady zabezpečení a přístupu je možné soustředit do jednoho zařízení nebo softwaru firewall.
- **Zvýšená úroveň ochrany osobních údajů** - možnost zablokovat přístup k informacím o protokolování.

Kromě toho lze identifikovat i některé nevýhody:

- **Omezení přístupu k důležitým síťovým službám** - nejčastější nevýhodou používání firewallu je omezení přístupu k běžným a důležitým službám, jako je TELNET a FTP. Tato nevýhoda se však netýká pouze brány firewall, ale i jiných bezpečnostních systémů.

- **Potřeba vyvážit bezpečnostní plán - pro** správné umožnění přístupu ke komunikaci a životně důležitým službám je důležité najít rovnováhu mezi potřebami a bezpečnostními zásadami. Je třeba omezit používání portů a zabránit interním útokům.
- **Ochrana před viry** - protože viry mohou mít různou kódovou podobu a mohou být komprimovány různými způsoby, nepovažuje se firewall za nejlepší řešení ochrany sítí před virovou infekcí.

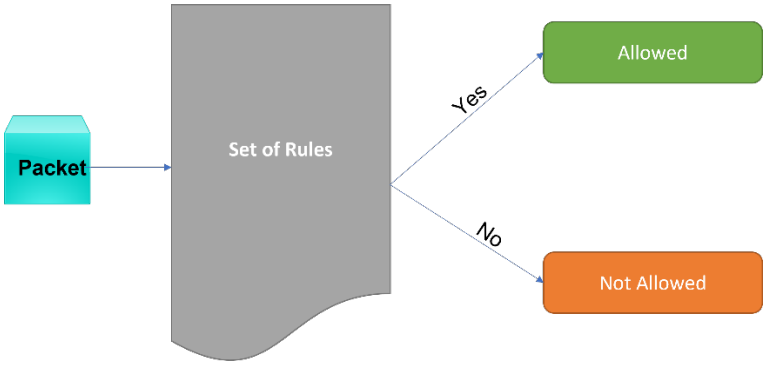
6.1.3 Typy a vlastnosti brány firewall

Firewall může fungovat různými způsoby, a to na základě metodiky vývojáře, specifických potřeb chráněného systému, vlastností operačního systému, struktury sítě atd. V našich sítích je pak možné nalézt různé typy implementovaných firewallů, mj:

- Filtrování paketů

  Filtrování paketů bylo prvním vyvinutým typem firewallu, kde byla použita jednoduchá, ale omezená metodika, zaměřená na analýzu IP adres paketů (obrázek 4).

  Přenos dat probíhal na základě protokolu TCP/IP (Transmission Control Protocol/Internet Protocol), který je rozdělen do různých vrstev. Obvykle se filtrování paketů omezuje na síťovou a transportní vrstvu: první zahrnovala IP adresu ze všech zařízení v síti a všechny směrovací procesy; druhá zahrnovala transportní protokoly, které umožňují datový provoz a přenos, jako je TCP. Na základě těchto základních konceptů byly firewally využívající filtrování paketů schopny jednak filtrovat pakety na základě jejich adres, zdrojových i cílových, a také filtrovat pakety podle jejich portů TCP a UDP (User Datagram Protocol). Jako příklad lze uvést, že by byl schopen blokovat provoz z IP adresy 192.168.1.1 na portu TCP 80. Všechny služby pracující na tomto portu by byly přístupné ze zařízení s uvedenou IP adresou.



Obrázek 4 - Jednoduché znázornění přístupu k filtrování paketů

- Statické a dynamické filtrování

  Včetně všech funkcí z předchozího typu lze také najít firewally provádějící filtraci paketů dvěma různými způsoby, přičemž první z nich se zaměřuje na statickou filtraci a druhý, který je o něco rozvinutější, se zaměřuje na dynamickou filtraci. V prvním modelu (statickém) jsou data blokována nebo povolována jednoduše na základě pravidel, aniž by se bral v úvahu jakýkoli vztah mezi pakety nebo jejich spojením. Zpočátku tento přístup neměl žádné problémy, nicméně některé nové síťové služby nebo aplikace mohou svou správnou komunikaci a přenos dat založit na požadavcích a odpovědích a vytvořit tak specifický tok paketů, které mezi sebou souvisejí. Tím je při použití prvního modelu možné způsobit narušení komunikace, což má za následek nefunkčnost aplikace nebo služby. Navíc to lze považovat i za bezpečnostní problém, kdy by správce sítě byl nucen vytvářet ojedinělá a specifická pravidla, aby nedošlo k selhání těchto služeb, čímž by se zvýšila možnost, že nebudou blokovány pakety, které by skutečně blokovány být měly.

  Na druhé straně dynamická filtrace tato omezení řeší. Tento model filtrování paketů zohledňuje kontext paketů a vytváří pravidla, která se dokáží přizpůsobit situaci a následně umožňují práci s konkrétními pakety, dokud je to nutné a pouze během určitého období. Tím se drasticky snižuje pravděpodobnost zablokování důvěryhodných paketů.

- Osobní brány firewall

  Existují také jednoduché firewally určené k ochraně osobních počítačů a mobilních zařízení, které může používat běžný uživatel. Dnešní operační systémy již obsahují softwarovou bránu firewall, včetně systémů Microsoft

Windows, Linux a Mac OS X. Existují také některé antivirové programy, které obsahují různé úrovně ochrany a bránu firewall. Tyto brány firewall, mají omezený výkon a ochranu, umožňují uživatelům aplikovat jednoduchá pravidla a konfigurovat přístup z aplikací a služeb na internet. I když zvyšují úroveň zabezpečení zařízení, stále je možné je obejít a učinit ze zařízení cíl útoku. Hackeři mohou tyto typy brány firewall snadno obejít a zneužít zranitelnosti systémů. V podnikové síti se doporučuje používat také hraniční rámce, jak bylo vysvětleno dříve.

- Softwarová a hardwarová brána firewall

  Již dříve bylo zmíněno, že firewally mohou být implementovány jak hardwarově, tak softwarově. Sama o sobě tato informace není nesprávná, je však nutné dodat, že samotný hardware není nic jiného než zařízení, na kterém je nainstalován software firewallu. Tato zařízení, obvykle označovaná jako zařízení firewall, jsou určena pouze k plnění role brány firewall a mohou obsahovat různé konfigurace a porty, aby se mohla připojit k různým sítím. Taková zařízení se navíc obvykle používají ve větších sítích, kde je značný síťový provoz nebo kde jsou citlivá data. Hlavní výhodou těchto firewallů je, že díky tomu, že hardware byl vyvinut speciálně pro tento účel, si poradí s většími objemy dat a nejsou náchylné k útokům, které se obvykle vyskytují u běžných serverů.

- Brána firewall založená na státu

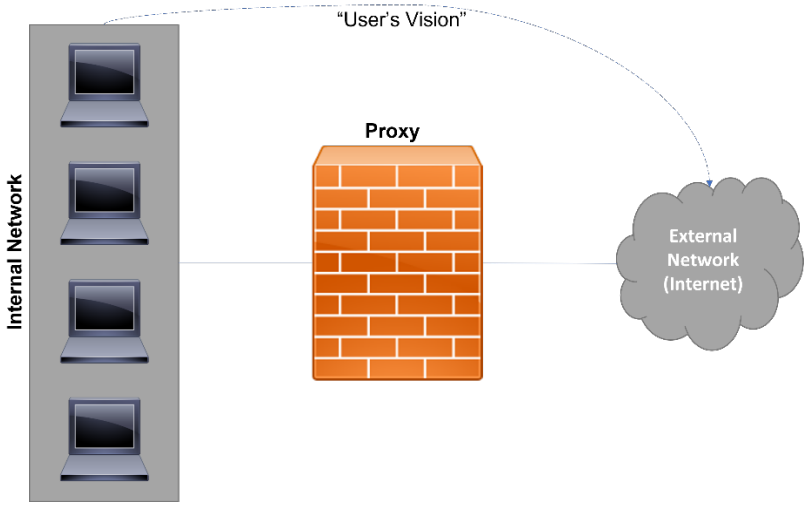
  Po jednoduché filtraci paketů přišla na řadu technologie stavové základny používaná ve firewallech. To způsobilo téměř revoluci ve fungování firewallů, protože místo jednoduché analýzy paketů při jejich průchodu firewallem a jejich blokování nebo povolování podle jednoduchých pravidel, stavové firewally manipulují s dynamickými informacemi a provádějí monitorování a analýzu paketů i během jejich průchodu sítí. Zatímco firewall typu filtrování paketů byl schopen pouze blokovat nebo povolovat pakety na základě jejich IP adres a portů, stavový firewall dokáže detekovat a blokovat nelegitimní síťový provoz na základě vzorů a dalších pokročilých stavových konceptů. Je však důležité zdůraznit, že tento typ firewallu přináší nevýhodu spojenou s nutností

ukládat data o provozu do paměti a s hlubší a silnější analýzou, která vyžaduje vyšší výpočetní výkon a úložné kapacity.

- Brána firewall pro aplikace

  Ačkoli se tato technologie v dnešní době stále používá, sama o sobě k řádné ochraně sítě před útoky a průniky nestačí. Jako další velký krok v oblasti zabezpečení se zrodily aplikační a webové aplikační brány firewall. Tradiční firewally se omezovaly na obecnou analýzu a monitorování síťového provozu a nedokázaly správně detekovat provoz pocházející z aplikací, služeb nebo jiného softwaru. Tyto nové aplikační firewally byly navrženy tak, aby se s touto mezerou vypořádaly a dokázaly blokovat pokusy o vniknutí, které využívají zranitelnosti, jež je možné zneužít. Mnohé z nich jsou navíc vybaveny rodičovskou kontrolou, která je schopna rozpoznat typ obsahu a určit, zda je vhodný pro sledování mladými lidmi.

- Proxy



Obrázek 5 - Příklad implementace proxy serveru mezi vnější a vnitřní sítí

Firewall, který funguje jako proxy server a filtruje v podstatě obsah http a přístupy prohlížeče, může být implementován mezi soukromou a veřejnou sítí (obrázek 5). Tímto způsobem je veškerý provoz analyzován a monitorován, což umožňuje lepší kontrolu přístupu a přenosů dat. Je však také možné jej implementovat jako běžný server a přinutit jej, aby veškerý provoz http byl přes něj předáván. Toho běžně využívá mnoho organizací, kde se požaduje, aby

všechny webové prohlížeče byly nakonfigurovány tak, aby odesílaly provoz na proxy server, který bude analyzován. V důsledku toho musí hlavní firewall blokovat veškerý http provoz, který nepochází z proxy serveru. Jen tak je možné řádně kontrolovat http požadavky a odpovědi.

- Firewall nové generace

  Firewall nové generace byl posledním konceptem, který byl vyvinut a zaměřen v podstatě na korporátní svět. Tento nový typ firewallu zahrnuje všechny předchozí typy do centralizovaného filtru, který je schopen mimo jiné analyzovat a monitorovat pakety, vniknutí a prevenci aplikací a služeb. Tyto firewally lze nalézt i jako online službu. Většinou se však stále používají jako zařízení. Jelikož jsou robustnější a mají hlubší analýzu, jejich implementace je složitější a musí být pečlivě provedena, přičemž by měl být vypracován a pravidelně aktualizován řádný bezpečnostní plán. Tyto firewally, používané jako hlavní bezpečnostní mechanismus, se často instalují na hranici mezi soukromou a veřejnou sítí a kontrolují příchozí a odchozí provoz.

6.1.4 Topologie a architektury brány firewall

Firewally, které se obvykle nacházejí na hranici mezi veřejnou a soukromou sítí, lze stále používat ke zvýšení bezpečnosti konkrétních síťových segmentů v rámci sítě. Běžně se s nimi setkáváme nejen k oddělení soukromých sítí LAN, ale také například k oddělení kritických systémů od internetu a firemních sítí. Na základě této myšlenky a podle mnoha různých typů firewallů existují také různé topologie a architektury implementace:

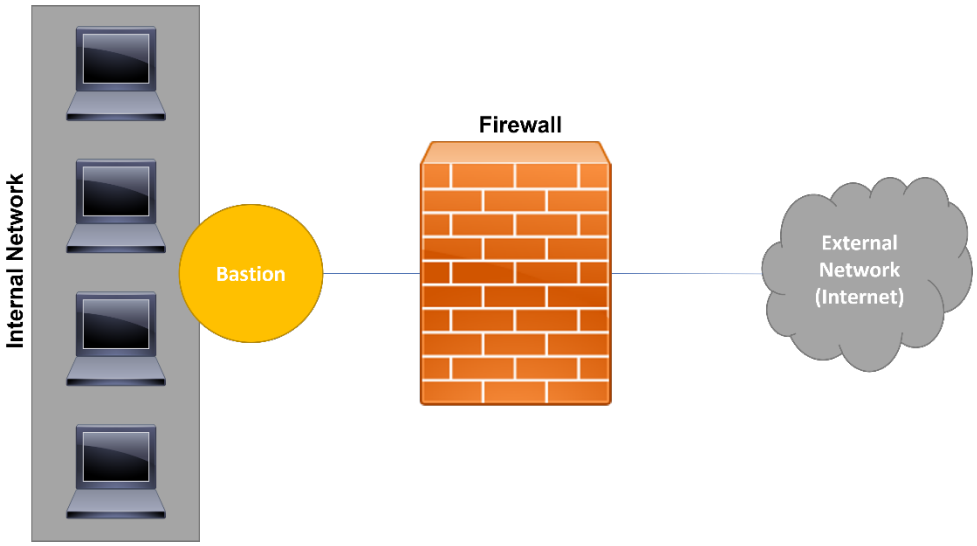
- Hostitel se dvěma domény

  V této architektuře se používá počítač s názvem "dual-homed host" umístěný mezi vnitřní a vnější sítí, obvykle Internetem. Tento počítač je tak pojmenován proto, že má dvě různá síťová rozhraní, pro každou připojenou síť jedno. Stejně jako u prvního způsobu implementace proxy, ani zde neexistuje žádná jiná komunikační cesta, což nutí veškerý provoz procházet přes hostitele a vyhnout se přímému spojení mezi vnitřní a vnější sítí. Hlavní výhodou tohoto přístupu je,

že poskytuje větší kontrolu nad síťovým provozem a snadnější správu. Na druhou stranu je tento přístup zranitelný v tom smyslu, že pokud je hostitel napaden, může to způsobit kritický bezpečnostní problém. Tento typ architektury se obvykle používá u proxy firewallů.

- Prověřený hostitel

  V architektuře stíněného hostitele se místo jednoho hostitele umístěného mezi vnitřní a vnější sítí používají dva různí hostitelé, z nichž jeden plní roli směrovače do Internetu (stíněný směrovač) a druhý roli vnitřního směrovače (bastionový hostitel) (obrázek 6).

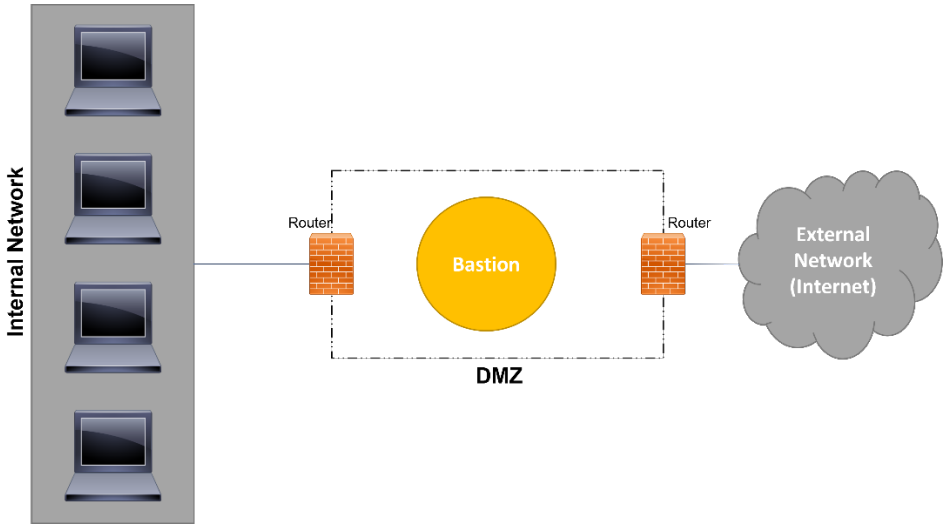


Obrázek 6 - Zobrazení architektury stíněného hostitele

Zaměřuje se na hostitele bastionu a neumožňuje přímou komunikaci na obou stranách, takže komunikace probíhá následovně: vnitřní síť - hostitel bastionu - stínící směrovač - vnější síť a naopak. V tomto případě funguje směrovač na základě filtrování paketů, přičemž tyto filtry jsou navrženy a nakonfigurovány tak, aby přesměrovaly provoz na hostitele bastionu. Následně bastionový hostitel podle svých pravidel rozhodne, zda provoz je, nebo není povolen, a to i po první filtraci. Bastionový hostitel je kritickým bodem sítě a musí být chráněn, aby nedošlo k narušení bezpečnosti celé sítě a systémů.

- Prověřená podsíť

Poslední ze tří architektur je stíněná podsíť, která rovněž zahrnuje hostitele bastionu, stejně jako předchozí architektura, avšak v této architektuře je hostitel bastionu umístěn v izolované oblasti nazvané DMZ (Demilitarized Zone). DMZ je umístěna mezi vnitřní a vnější sítí a je obklopena směrovači pro filtrování paketů (obrázek 7).



Obrázek 7 - Zobrazení architektury stíněné podsítě

Použití DMZ zvyšuje úroveň zabezpečení, protože pokud se útočníkovi podaří projít přes první firewall směrovače, musí se ještě vypořádat s DMZ, aby získal přístup do vnitřní sítě. DMZ může být také nakonfigurována různými způsoby, včetně firewallů, proxy serverů, většího počtu bastionových hostitelů a dalších bezpečnostních systémů, které zvyšují veškeré zabezpečení. Vysoká úroveň zabezpečení a flexibilita konfigurace činí ze stíněné podsítě složitější a nákladnější architekturu.

6.1.5 Příklady brány firewall

Jedním z nejběžnějších příkladů firewallů je ten, který je k dispozici v distribucích Linuxu a nazývá se IPTables. Tento firewall, stejně jako většina firewallů pro filtrování paketů, je založen na pravidlech a seznamech řízení přístupu (ACL), které slouží k reprezentaci a vynucování bezpečnostní politiky sítě, kterou chtějí chránit, monitorovat a řídit.

V tabulkách IPTables mají tyto seznamy ACL zvláštní vlastnosti, protože používají sofistikované prvky a parametry pro sestavení pravidla na základě bezpečnostního kontextu a potřeby. To znamená, že správce je schopen sestavit jakýkoli typ ACL podle svých potřeb a v souladu s ochranou soukromí a bezpečností navržené politiky. V hlubším přístupu je tento firewall založen na navrženém tvořeném třemi různými strukturami:

- Pravidla

  Pravidla jsou v podstatě příkazy předávané bráně firewall, aby mohla provést určitou akci (povolit nebo zablokovat). Musí být sestavena podle jazyka nakonfigurovaného v softwaru brány firewall, aby jim mohla porozumět, a musí se řídit specifickými vzory, aby byla správně interpretová a (obrázek 8). Obecně jsou pravidla podobná mezi mnoha softwary a zařízeními firewall, přičemž hlavní koncept pravidla dodržují všechny. Není obtížné exportovat pravidla z jednoho firewallu do jiného, pokud je jazyk pravidel podobný. V tabulkách IPTables jsou pravidla ukládána do řetězců a zpracovávána podle pořadí. První pravidlo se kontroluje jako první, druhé pravidlo se kontroluje jako druhé a tak dále až do konce všech pravidel. Zde je důležité naplánovat pořadí pravidel, která se mají použít, protože při špatném pořadí může být některý obsah blokován předchozím pravidlem, i když by ve skutečnosti měl být povolen. Plánování pravidel brány firewall je důležitým faktorem při správě sítě, nicméně mnoho softwaru brány firewall umožňuje správci pravidla po jejich konfiguraci a uložení přeorganizovat. Zaměříme-li se na konkrétní případ IPTables, nová pravidla se primárně ukládají do jádra operačního systému, což znamená, že pokud dojde k restartu počítače, veškerý obsah pravidel bude smazán a ztracen. Vzhledem k tomuto faktoru by měla být všechna pravidla uložena v souboru, který se načte při každém spuštění stroje. Je pravda, že většinou se používá vyhrazený stroj, který funguje pouze jako firewall, kde není restartování tak časté jako u běžného osobního počítače, nicméně je také běžné, že se používá velký soubor pravidel, kde je nutné je všechny konfigurovat při každém restartu stroje, což je velmi náročný úkol a časově náročné.

Obrázek 8 - Příklad pravidla Iptables

- Řetězy

  Ukládání pravidel brány firewall, řetězce umožňují správci určit různé typy ošetření, které mají být použity na pakety, nezávisle na tabulce, na kterou se zaměřuje. V tabulkách IPTables je možné nalézt dva různé typy řetězců, přičemž první, nazvaný standardní řetězce, zahrnuje řetězce, které jsou již v softwaru k dispozici a lze je aplikovat na obecný síťový provoz. Druhým typem jsou řetězce vytvořené samotným správcem a jsou určeny pro splnění specifických potřeb.

  V případě standardních řetězců je možné identifikovat "Předsměrování", které se skládá z příchozího provozu lokálního stroje (stroje firewallu) a zahrnuje také provoz generovaný lokálně a směřující do lokálního stroje. Dalším standardním řetězcem je "Vstupní", který se zaměřuje na veškerý provoz, jehož cílem je opět samotný stroj. Řetězec "Forward" se navíc týká síťového provozu, který prochází strojem, a řetězec "Output" se skládá z provozu, který je generován lokálně, a to jak s místním, tak se vzdáleným cílem. Jedná se v podstatě o veškerý provoz, který stroj firewallu vytváří a který je odesílán do sítě nebo do samotného stroje. Poslední řetězec je "Postrounting" a soustřeďuje provoz, který odchází ze stroje, včetně síťového provozu generovaného lokálně a majícího i lokální cíl).

- Tabulky

  Pravidla se ukládají do řetězců a následně řetězce do tabulek, přičemž v každé tabulce jsou uloženy řetězce a pravidla se stejnou specifickou charakteristikou. I zde existují tři různé typy tabulek: Filtr; NAT a Mangle.

  "Filtr" je tabulka odpovědná za filtrování všech paketů, které procházejí bránou firewall, bez ohledu na jejich cíl. Tato tabulka slouží k analýze síťového provozu a jeho povolení nebo zablokování podle pravidel uložených v tabulce. Při zaměření na bránu firewall je hlavní identifikovanou činností filtrace paketů,

i když umožňuje i jiné činnosti. V tomto případě je za takovou filtraci paketů zodpovědná především tabulka "Filtr".

Tabulka "NAT" řídí pakety, které procházejí bránou firewall, ale mají různý původ a cíl. NAT neboli překlad síťových adres je mechanismus, který umožňuje překlad soukromých adres na veřejné a naopak. Tato tabulka se obvykle používá pro komunikaci mezi soukromou a veřejnou sítí a umožňuje počítačům v soukromé síti přistupovat k veřejné síti prostřednictvím jedné nebo více veřejných IP adres.

Poslední typ tabulky se nazývá "Mangle" a umožňuje manipulaci s charakteristikami paketů, například s typem služby. To umožňuje implementovat kvalitu služby, známou také jako QoS.

IPTables je firewall pro filtrování paketů, který je k dispozici v distribucích Linuxu a umožňuje kontrolu a monitorování sítě i samotného počítače. Poskytuje různé akce, včetně "accept", "drop", "reject" a "log", konfigurované do pravidel a personalizovaných řetězců. Jak již bylo zmíněno, pravidla musí dodržovat určité pořadí a musí být naplánována před jejich zavedením, aby všechny akce byly respektovány a pracovaly v souladu s bezpečnostní politikou organizace.

6.2 Systémy detekce narušení (IDS)

6.2.1 Úvod do systémů detekce narušení

V poslední době jsou navrhovány systémy detekce narušení (IDS), které pomáhají správcům sítí analyzovat bezpečnostní rizika a odhalovat útoky na jejich sítě a systémy. Použití zpravodajských technik pro detekci narušení umožňuje zvládnout velké množství shromážděných dat, jako jsou například vzorce provozu, které člověk sám jen obtížně interpretuje.

Velká data jsou v současné době vnímána jako technologické řešení pro monitorování infrastruktury, kde analýza velkých dat může vést k optimalizovaným algoritmům pro řešení síťových a systémových problémů, jako jsou bezpečnostní problémy, možné kybernetické útoky a různé typy modelování. Poskytování

hloubkového vhledu do síťové infrastruktury v souvislosti s rozhodovacími otázkami se realizuje prostřednictvím nasazení technologie internetu věcí (IoT) v celém systému infrastruktury, jako jsou sítě senzorů, které jsou schopny snímat a přenášet informace.

Mnoho IDS je založeno na expertních pravidlech, která jsou navržena a vytvořena ručně a popisují pouze známé signatury útoků. Ačkoli, pokud jde o použití IDS založených na strojovém učení, které mají být implementovány v počítačových sítích a systémech, je možné identifikovat data o síťovém provozu jako zásadní faktor pro lepší zlepšení IDS, analýzu bezpečnostních rizik a vývoj vhodných bezpečnostních řešení.

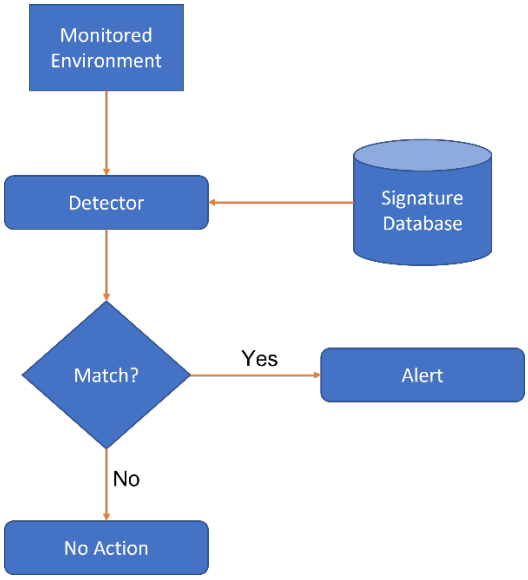
Na základě této myšlenky mnozí vědci označují IDS za nejdůležitější mechanismy pro sledování a kontrolu škodlivých aktivit v síti a systémech. Zatímco signaturní přístupy jsou důležité pro řešení dobře známých hrozeb, metody založené na anomáliích jsou nezbytné pro odhalování a řešení moderních a nových útoků.

Účinný systém detekce narušení musí být schopen shromažďovat a analyzovat všechny vyměňované pakety v místní i koncové komunikaci a lze jej chápat jako kamery a senzory, které neustále monitorují dané místo. Obvykle se skládá z konzoly pro správu, která spravuje a hlásí narušení, a senzorů, které pracují jako agenti a monitorují síťová zařízení v reálném čase.

6.2.2 Typy a charakteristiky systémů detekce narušení

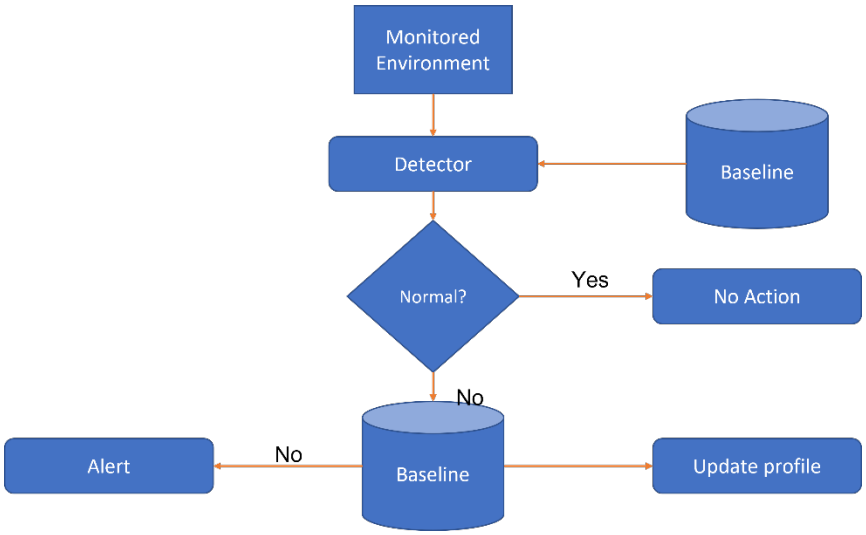
Z historického hlediska existují různé typy systémů detekce narušení, které se dělí podle své povahy a způsobu fungování. Podle různých vědců je lze rozdělit do dvou hlavních kategorií: Na základě signatur a na základě anomálií:

- Přístupy založené na signaturách jsou navrženy na základě známých vzorů útoků a používají se jako sady pravidel, například ty, které používá Snort IDS. Příchozí provoz je pak porovnáván s těmito pravidly, aby bylo možné identifikovat abnormální provoz mezi normálním provozem (obrázek 9).



Obrázek 9 - Schéma IDS založené na podpisu

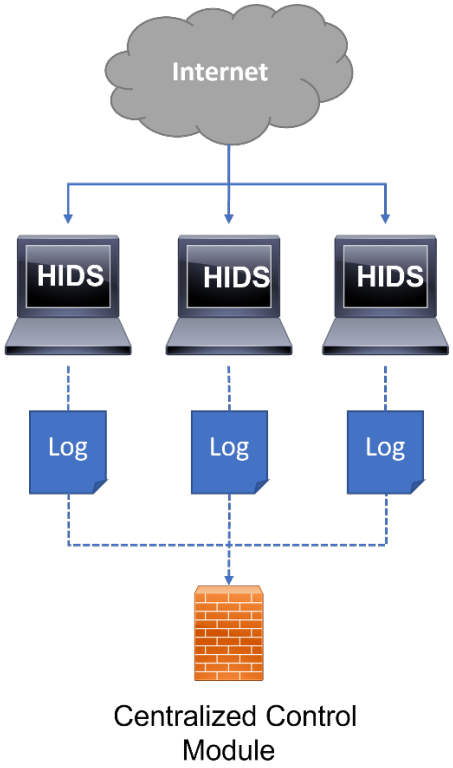
- Na rozdíl od předchozí kategorie jsou metody založené na anomáliích založeny na myšlence normálních profilů chování a při detekci narušení označují odlišné profily. Tento typ přístupu často vrací vysokou míru falešných poplachů při detekci nových útoků (obrázek 10).



Obrázek 10 - Schéma IDS založené na anomáliích

Systémy IDS se také běžně dělí na hostitelské (HIDS) (obrázek 11) a síťové (NIDS) (obrázek 12). Při porovnání je zřejmé, že systém IDS založený na hostiteli přebírá odpovědnost za sledování chování jednoho hostitele, zatímco systém IDS

založený na síti shromažďuje důkazy prostřednictvím dat o síťovém provozu. Někteří vývojáři považují kombinaci těchto dvou kategorií IDS za nejlepší způsob ochrany počítačových sítí proti kybernetickým útokům, ačkoli jsou zatím příliš nevyzrálé na to, aby byly široce nasazeny. Také je možné identifikovat slabé místo HIDS, které je třeba vylepšit, kdy v případě napadení hostitele nemusí správně odhalit narušení.

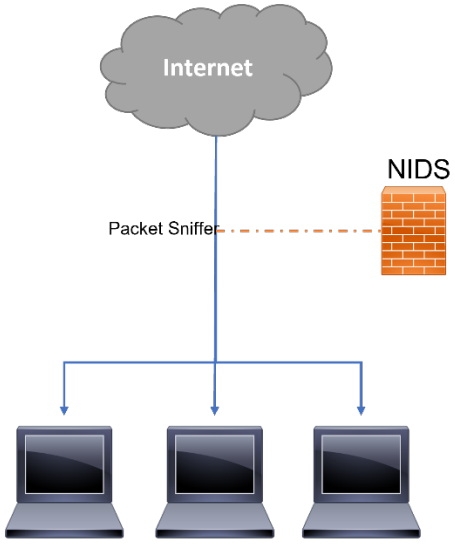


Obrázek 11 - Schéma IDS založené na hostiteli

V běžných systémech IDS je zcela akceptováno paradigma odepření přístupu ke škodlivým paketům jejich zahozením nebo jejich kořenovým kódem.

Stejně jako u jiných mechanismů počítačové bezpečnosti, i u systémů detekce narušení existují určité výhody a nevýhody, které je třeba vzít v úvahu před jejich instalací a konfigurací. Je důležité zdůraznit, že tradiční IDS nemusí být vhodné pro všechny počítačové systémy a sítě. Dobrým příkladem jsou kritické infrastruktury, jako je například systém rozvodu vody. Systém IDS, který pracuje 24 hodin denně a zásobuje pitnou vodou velká města a země, musí být pečlivě vybrán a implementován, protože může způsobit narušení komunikace a následně ohrozit lidské životy. Zde je důležité zdůraznit existující slabiny a zvláštní charakteristiky těchto kritických systémů,

které je třeba vzít v úvahu. Příklad hlavních komponent SCADA, jako jsou PLC a RTU, mají obvykle nízké výpočetní a paměťové schopnosti, takže nejsou vhodné pro přidělení HIDS, který musí být instalován na samotném hostiteli, aby mohl být analyzován. Naproti tomu snímače NIDS mohou být instalovány v odděleném stroji připojeném k síti, který má být monitorován. Takový přístup lze snadno integrovat se systémem SCADA, kde je nutné porozumět komunikačním protokolům a analyzovat je. V současných implementacích jsou však komunikační protokoly SCADA, které byly původně navrženy pro práci v sériové komunikaci, vloženy do užitečných zátěží paketů TCP.



Obrázek 12 - Schéma IDS založené na síti

Z hlubšího pohledu jsou přístupy založené na signaturách navrženy na základě známých vzorů útoků, které se používají jako sady pravidel. Příchozí provoz je pak porovnáván s těmito pravidly, aby bylo možné identifikovat abnormální provoz mezi normálním provozem. V kontrastu s předchozí kategorií se u anomálií často vrací vysoká míra falešných poplachů, pokud není chování systému v systému IDS správně nakonfigurováno. V konkrétním případě kritického systému je vzhledem k jeho citlivé povaze běžné chování a konfigurace systému vždy důkladně zdokumentována a aktualizována.

Kromě předchozích klasifikací se běžně setkáváme se systémy IDS rozdělenými na hostitelské (HIDS) a síťové (NIDS). Při porovnávání se systém IDS založený na

hostiteli stará o sledování chování jednoho hostitele, zatímco systém IDS založený na síti shromažďuje důkazy prostřednictvím analýzy dat o síťovém provozu. Mnozí vědci považují kombinaci těchto dvou kategorií IDS za nejlepší způsob ochrany vodovodních distribučních systémů před kybernetickými útoky, i když jsou zatím příliš nevyzrálé na to, aby byly široce nasazeny.

V těchto klasifikacích je také možné identifikovat slabé místo systému HIDS, které je třeba zlepšit, když může selhat při správném odhalení narušení v případě, že je hostitel kompromitován. Kromě toho by měl být HIDS nainstalován na samotném hostiteli nebo používat agenta, což samo o sobě není v kritickém síťovém prostředí zcela praktické, protože mnoho jeho zařízení má nízký výpočetní a energetický výkon. Kromě toho HIDS také zvyšuje objem provozu v síti a zatěžuje ji informačními pakety IDS, což opět může systému způsobit více problémů než pomoci.

V běžných systémech IDS je zcela akceptováno paradigma odepření přístupu ke škodlivým paketům jejich zahozením nebo jejich kořenovým kódem. V sítích vodovodních systémů je však takové paradigma vzhledem k jejich kritické povaze nepřijatelné. Kritické systémy vyžadují pravidelnou a nepřetržitou komunikaci mezi zařízeními a řídicími jednotkami, kde nedostupný kořen nebo paket může ohrozit celý systém, což může mít katastrofální následky.

6.2.3 Architektury implementace systémů detekce narušení

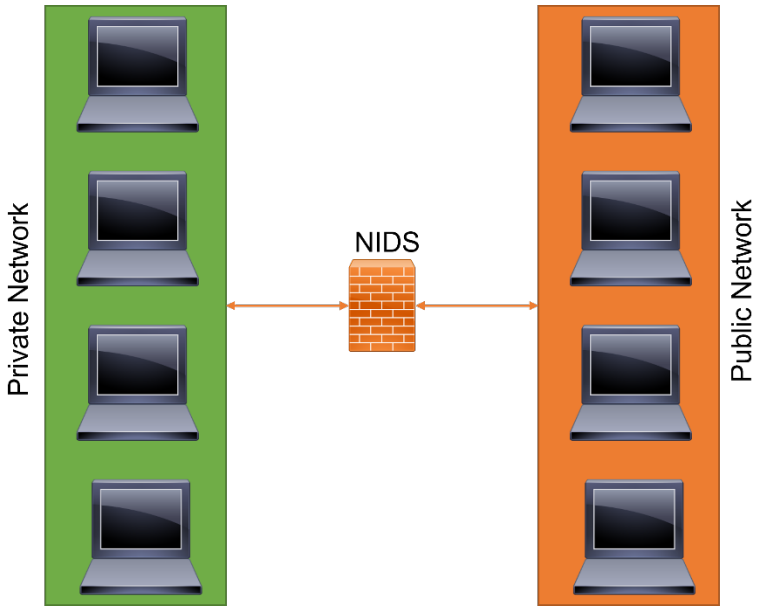
Vzhledem k různým existujícím typům IDS se jejich implementace může lišit systém od systému a síť od sítě. Je známo, že IDS založený na signaturách se zaměřuje na signatury známých útoků a zranitelností a využívá rozsáhlou databázi k sestavení svých pravidel a detekci narušení. Taková implementace však nemusí být pro námi spravovanou síť vhodná. Zde je prvním krokem pochopení potřeb ochrany sítě a systémů, určení jejich hlavních priorit a cílů.

Na druhou stranu IDS založené na anomáliích využívají běžný pracovní stav sítě a systémů, aby správně identifikovaly abnormální chování a dospěly k závěru, zda je skutečně způsobeno narušením, nebo se stále jedná o normální chování sítě. Opět je zapotřebí předchozí plán, v němž musí být systém a síť zdokumentovány a nakonfigurovány do systému IDS, aby mohl rozpoznat vzorce chování.

V dnešní době se také běžně setkáváme s IDS pracujícími se strojovým učením. Zde je opět nutné shromáždit informace o běžné funkci sítě a jejích systémů, aby bylo možné stroj naučit správným a běžným pracovním stavům ještě před jeho konečným použitím.

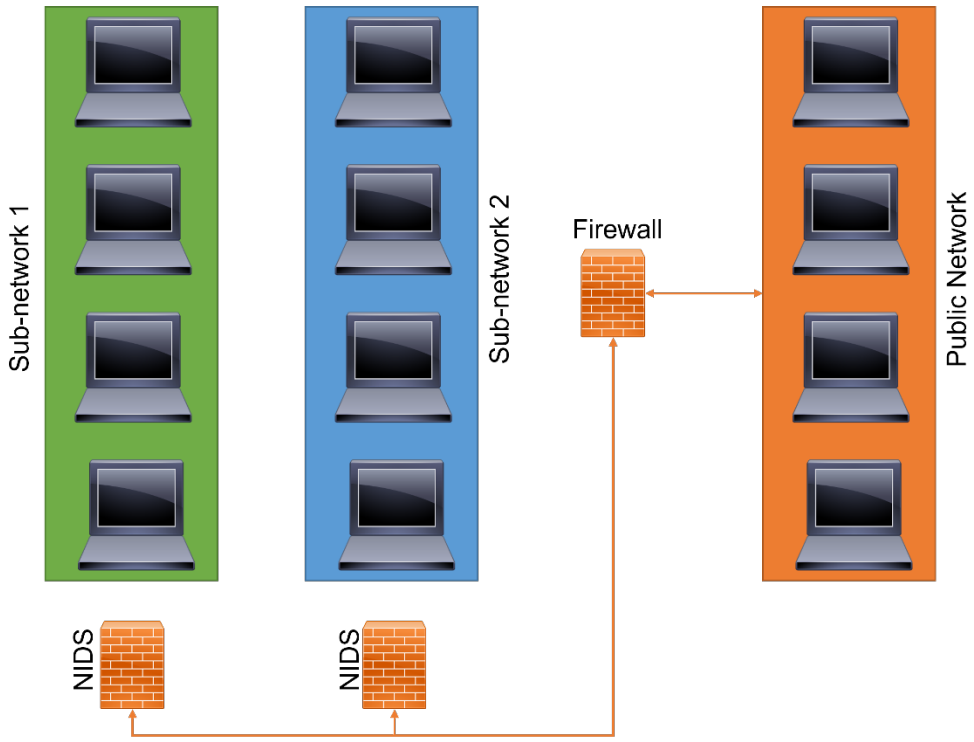
Stejně jako implementace firewallu se může lišit i implementace IDS, který může být umístěn na hranici nebo v rámci sítě.

Nejběžnější implementací IDS je jeho umístění na hranici mezi soukromou a veřejnou sítí. Jelikož se jedná o jeden z hlavních kritických bodů sítě, je jeho monitorování a analýza klíčová pro udržení dobré úrovně zabezpečení a zabránění neoprávněnému přístupu do vnitřní sítě a systémů (obrázek 13). Umístěním IDS na toto místo je monitorován a kontrolován veškerý příchozí a odchozí provoz, což však také vyžaduje vyšší výpočetní výkon a schopnost vypořádat se s velkým množstvím provozu. Protože kontroluje přístup do veřejné sítě, bude mít nízký výkon IDS za následek také nízký výkon komunikace s vnějšími sítěmi, běžně s internetem.



Obrázek 13 - Instalace systému IDS mezi vnitřní a vnější sítí

Na hranicích síťových segmentů nebo sítí LAN lze také nalézt různé systémy IDS, které monitorují a analyzují provoz mezi nimi. Toto provedení se obvykle vyskytuje v případě propojení mezi podnikovými sítěmi a sítěmi kritických systémů, kdy každý segment může mít svůj vyhrazený a specifický server IDS (obrázek 14).



Obrázek 14 - Instalace IDS na hranici segmentů LAN

V případě hostitelského IDS se zaměřuje na ochranu jednoho hostitele. Tento typ implementační architektury je vhodný pro ochranu konkrétních serverů nebo počítačů, které jsou snadným cílem útoků. Vzhledem k tomu, že se jedná o hostitelský systém, instalace agenta IDS se provádí na samotném serveru nebo počítači, kde je potřeba, aby měl dostatečný výpočetní a paměťový výkon. Tato architektura není vhodná pro všechna zařízení, protože ne všechna jsou schopna zvládnout analýzu velkého objemu síťového provozu a měla by být implementována pouze pro jednotlivé servery a kritické počítače. Použití architektury založené na hostiteli navíc vyžaduje existenci vyhrazeného serveru IDS, který by komunikoval s každým z existujících agentů IDS. V závislosti na počtu sledovaných hostitelů se zvýší i množství dat o síťovém provozu a může dojít k zahlcení sítě komunikací IDS, což sníží jeho výkonnost.

Implementace síťového IDS přináší efektivnější analýzu a monitorování, pokud síť zahrnuje větší počet hostitelů a pokud se zaměřujeme na kritické infrastruktury s nižším výpočetním výkonem zařízení. Na základě samotné analýzy síťového provozu nepotřebuje architektura založená na síti používat agenty IDS implementované na hostitelích, a v důsledku toho také není v síti generován komunikační provoz IDS. Tento

typ architektury využívá jeden nebo více vyhrazených serverů instalovaných v síti, které shromažďují a analyzují data síťového provozu a identifikují jeho abnormální chování nebo abnormální vzorce provozu, aby bylo možné odhalit narušení ze strany neautorizovaných agentů.

Přestože existují tři hlavní architektury implementace IDS, většina vědců a výzkumníků v této oblasti tvrdí, že nejlepší řešení IDS spočívá v kombinaci předchozích tří architektur. Použití různých typů a implementačních architektur přináší vyšší míru detekce narušení a následně i vyšší úroveň bezpečnosti.

Kombinace HIDS a NIDS navíc umožňuje monitorovat celou síť, přičemž zvláštní pozornost je věnována kritickým serverům nebo počítačům, které ukládají nebo poskytují důležitá data a služby uživatelům sítě.

6.2.4 Běžná řešení a příklady systémů detekce narušení

V současné době je k dispozici mnoho řešení pro detekci narušení, některá z nich jsou placená a některá bezplatná. Také mnohá integrovaná řešení již přinášejí mechanismus detekce narušení v rámci svého softwaru, jsou však omezena místem jeho implementace.

V závislosti na typu IDS, který má být implementován, lze také použít různá řešení. Zde je možné upozornit na široce známé systémy SNORT IDS a Suricata IDS.

Pokud se zaměříme na první z nich, SNORT, jedná se o placené open-source řešení, které si mohou nainstalovat nejen jednotliví uživatelé, ale také firmy a organizace. Tento IDS se soustředí na sadu pravidel, která určují, který síťový provoz má být shromažďován a co je třeba udělat se zjištěnými škodlivými pakety. Pracuje na základě známých signatur zranitelností a útoků, na jejichž základě vytváří databázi pravidel IDS a identifikuje možná narušení v síti.

Z jeho funkcí je možné vyzdvihnout analýzu a monitorování v reálném čase, kdy má správce sítě možnost kontrolovat všechny výsledky monitorování IDS v reálném čase, identifikovat detekce narušení a jednat podle potřeb. Kromě toho zahrnuje také analýzu protokolů pro lepší identifikační výkon. Analyzuje protokoly pomocí procesu sniffingu, který zachycuje data ve vrstvách protokolu, což správcům umožňuje dále zkoumat potenciálně škodlivé pakety. SNORT navíc shromažďuje pravidla podle protokolů, jako jsou IP a TCP, dále podle portů a následně podle těch s obsahem nebo

bez obsahu. Pravidla, která mají obsah, využívají vícevzorkový matcher, který zvyšuje výkon, zejména pokud jde o protokoly, jako je HTTP (Hypertext Transfer Protocol). Pravidla, která nemají obsah, se vyhodnocují vždy, a v důsledku toho se snižuje výkon.

SNORT je IDS, který dokáže kontrolovat a monitorovat nejen hlavičku paketu, ale také jeho užitečné zatížení, což umožňuje snížit míru falešně pozitivních detekcí. Je také schopen poskytovat výstrahy a flexibilní protokoly o paketech a jejich analýze, což správcům sítě poskytuje veškeré informace pro správnou analýzu a jednání. Jeho instalaci lze provést v systémech Unix, Windows a MacOSx, pokud umožňují kompilaci a instalaci knihovny lipcap, která slouží jako základ pro analýzu paketů. SNORT má také flexibilní architekturu, která umožňuje různé způsoby instalace a přizpůsobení potřebám sítě.

Podobně jako předchozí systém je i Suricata IDS open-source systém pro detekci síťových hrozeb, který je zdarma a poskytuje různé funkce, včetně detekce narušení a monitorování zabezpečení sítě, a to prostřednictvím hloubkové kontroly paketů a porovnávání vzorů.

Hlavním rozlišovacím znakem systému Suricata ve srovnání se systémem SNORT je, že systém Suricata obsahuje funkci dynamické ochrany protokolu, která je nezávislá na portu. To umožňuje systému IDS identifikovat některé z nejběžnějších protokolů aplikační vrstvy, včetně protokolů HTTP, DNS (Domain Name System), TLS (Transport Layer Security) a dalších, pokud tyto protokoly komunikují přes nestandardní porty. Zde použitý jazyk pravidel umožňuje správci sestavit podmínky shody v protokolu aplikační vrstvy, čímž se zvyšuje výkon a detekce IDS.

Suricata monitoruje síťový provoz pomocí rozsáhlé databáze pravidel, jako je SNORT, a svá pravidla zakládá také na známých signaturách zranitelností a útoků. Ačkoli byla Suricata vytvořena v jiné architektuře a je mnohem novější než SNORT, obě řešení mohou využívat signatury hrozeb. Klíčovým rozdílem je, že Suricata představuje vícevláknovou architekturu, která umožňuje využívat více jader procesoru najednou, a v důsledku toho přináší vyšší výkon ve srovnání s jinými řešeními. Použití více CPU umožňuje systému Suricata zpracovávat více událostí současně, aniž by musel přerušovat jiné požadavky nebo ohrožovat jiné analýzy, zatěžovat rovnováhu mezi CPU a zvyšovat výkon při analýze síťového provozu.

Toto řešení IDS lze použít ve třech různých rolích, přičemž nejjednodušší je nastavit jej jako hostitelský IDS, který monitoruje provoz jednotlivého počítače. Lze jej také implementovat jako pasivní IDS, který monitoruje veškerý provoz procházející sítí a upozorní správce sítě, pokud narazí na něco škodlivého. Třetí a poslední úloha spočívá v tom, že je Suricata implementována jako aktivní inline IDS a IPS (Intrusion Protection System), monitorující příchozí a odchozí provoz, což umožňuje blokovat škodlivý provoz ještě předtím, než vstoupí do sítě, a zároveň na tuto akci upozornit správce sítě.

Stejně jako SNORT je Suricata k dispozici také pro systémy UNIX, Windows a MacOSx.

Jak již bylo zmíněno, ne všechna řešení IDS jsou vhodná pro každý systém nebo síť, přičemž správce sítě musí zvolit to nejlepší řešení, které odpovídá potřebám a specifickým vlastnostem jeho sítě.

Předchozí příklady jsou většinou vhodné pro implementaci v běžné počítačové síti a jsou také nejběžnějšími řešeními, která dnes organizace a firmy používají. Pokud se však zaměříme na detekci narušení v kritických infrastrukturách, které jsou závislé na specifických síťových protokolech a kde pouhé přerušení komunikace může mít drastické následky, je třeba IDS pečlivě vybírat a implementovat.

Někteří vědci uvádějí, že specializované řešení je nutností a že IDS založené na státním systému spolu se systémem strojového učení mohou být budoucností pro ochranu kritických infrastruktur. Dobrým příkladem je řešení vyvinuté společností (Al-Malawi et al., 2016) které se zaměřuje na techniku shlukování založenou na datech pro extrakci stavových pravidel a detekci útoků v sítích Modbus/TCP bez předchozí znalosti specifikací systémů. Je však důležité zdůraznit, že citlivé a kritické systémy, jako je SCADA ve WDS (vodovodní distribuční systémy), mají vždy zcela podrobnou dokumentaci.

6.3 SYSTÉMY PREVENCE VNIKNUTÍ (IPS)

6.3.1 Úvod do systémů prevence narušení

Systém prevence narušení (IPS) je nástroj pro zabezpečení sítě, který nepřetržitě monitoruje síť, zda se v ní nevyskytuje škodlivá aktivita, a podniká kroky k jejímu zamezení, včetně hlášení o zablokování nebo odstranění, pokud k němu dojde. Jeho název může být podobný předchozímu popsanému tématu (systémy detekce narušení), nicméně předchozí mechanismus se zaměřuje pouze na identifikaci, neuplatňuje žádné akce, a tudíž nezabraňuje tomu, aby k útoku došlo.

IPS je navíc pokročilejší systém než IDS a je často součástí firewallu nové generace nebo řešení jednotné správy hrozeb. Běžně se také setkáváme s jeho spoluprací se serverem IDS, jako je tomu u předchozích řešení (SNORT a Suricata).

Stejně jako jiné bezpečnostní systémy, i IPS lze nalézt v softwarové i hardwarové podobě, kdy lze software nainstalovat do libovolného počítače a umístit jej do sítě za účelem ochrany, vždy s ohledem na hardwarové požadavky stroje. Stejně jako mnoho jiných technologií zabezpečení sítě musí být i IPS dostatečně výkonný, aby byl schopen zpracovávat velké množství dat síťového provozu, aniž by zpomaloval výkon sítě.

Systém prevence narušení se často umísťuje inline, do toku síťového provozu, mezi zdroj a cíl. Stejně jako IDS se IPS běžně nachází mezi privátní a veřejnou sítí, takže může analyzovat a monitorovat všechny síťové komunikační transakce mezi oběma sítěmi a správně zabránit privátní síti před útoky a jinými narušeními bezpečnosti. Jelikož je umístěn mezi oběma sítěmi, obvykle se nachází za firewallem.

Sám o sobě není server IPS schopen zcela ochránit síť, často pracuje ve skupině s dalšími bezpečnostními nástroji a řešeními a identifikuje hrozby, které tato řešení nedokážou identifikovat.

Protože server IPS filtruje škodlivé přenosy ještě předtím, než se dostanou k ostatním bezpečnostním zařízením a kontrolním prvkům, snižuje zátěž těchto kontrolních prvků a umožňuje jim pracovat efektivněji. Protože je IPS z velké části automatizovaný, vyžaduje od týmů IT menší časové investice, čímž splňuje mnoho požadavků na shodu s předpisy PCI DSS, HIPAA a dalšími. Kromě toho IPS poskytuje také cenná data z auditů, která lze využít k další analýze a stopě narušení nebo útoku. Taková data jsou důležitá v tom smyslu, že mohou poskytnout celkový pohled na

incident a pomoci při identifikaci zdroje narušení a způsobu, jak mu do budoucna zabránit, aby se opakoval.

Stejně jako většinu ostatních bezpečnostních systémů a nástrojů lze i IPS přizpůsobit a zahrnout do nich personalizované zásady, aby odpovídaly konkrétním potřebám organizace a sítě, kterou chrání.

Řešení IPS zabraňují nejen průnikům, ale jsou také velmi účinná při detekci a prevenci zneužití zranitelností. Po objevení zranitelnosti obvykle existuje časový rámec, ve kterém mají aktéři hrozeb příležitost ji zneužít, než je k dispozici bezpečnostní záplata pro její opravu. Systém prevence narušení zde slouží k rychlému zablokování těchto typů útoků a k ochraně sítě v době, kdy není k dispozici oprava.

Zařízení IPS byla původně vytvořena a vydána jako samostatná zařízení v polovině roku 2000. Tato funkce však byla integrována do nástrojů pro jednotnou správu hrozeb spolu s dalšími bezpečnostními nástroji a službami pro malé a střední firmy a dnes i do firewallů nové generace na podnikové úrovni.

Novější řešení IPS jsou v současné době propojena s cloudovými výpočetními a síťovými službami, které jim umožňují poskytovat sofistikovanější přístup k ochraně před stále rostoucími kybernetickými bezpečnostními hrozbami, kterým čelí místní i globální organizace po celém světě.

Na rozdíl od systémů IDS, které pracují pasivně, pouze detekují a upozorňují na možné průniky a hrozby, je IPS umístěn v síti a kontroluje veškerý příchozí a odchozí síťový provoz mezi privátními a veřejnými sítěmi, nachází se přímo za firewallem nebo je jeho součástí. Toto řešení IPS aktivně analyzuje a provádí automatizované akce na všech tocích provozu, které vstupují do sítě:

- odeslání alarmu správci (stejně jako v systémech IDS).
- Zahození škodlivých paketů.
- Blokování provozu ze zdrojové adresy.
- Obnovení připojení.
- Konfigurace brány firewall, aby se zabránilo budoucím útokům.

IPS musí jako inline bezpečnostní nástroj pracovat efektivně, aby nesnižoval výkon a efektivitu sítě, přičemž musí být dostatečně výkonný, aby síť řádně zabezpečil

a zároveň zachoval její běžné funkce. Musí také pracovat v rychlém režimu, protože ke zneužití může dojít téměř v reálném čase, a musí být schopen přesně detekovat a reagovat, eliminovat hrozby a omezit falešně pozitivní poplachy. K tomu slouží několik technik a přístupů, které se používají k vyhledávání exploitů a ochraně sítě před neoprávněným přístupem.

6.3.2 Typy a charakteristiky systémů ochrany proti narušení

Existují různé typy systémů ochrany proti vniknutí s různými vlastnostmi a funkcemi, stejně jako to bylo možné pochopit u systémů detekce vniknutí. Stejně jako systémy IDS lze i systémy IPS rozdělit na systémy založené na signaturách, anomáliích a zásadách. Systémy ochrany proti narušení založené na signaturách zde používají přístup založený na známých signaturách zranitelností a útoků, kdy je metodou přiřazení aktivity k těmto signaturám a případné vyvolání či nevyvolání poplachu a opatření. Jednou z nevýhod této metody je, že je schopna zastavit pouze dříve identifikované útoky a nebude schopna rozpoznat nové. Tento typ IPS nebere v úvahu žádné neznámé zranitelnosti a v případě výskytu nového útoku neprovede v síti žádnou akci.

Tento typ IPS používá v kódu každého exploitu slovník jednoznačně identifikovatelných vzorů neboli signatur. Jakmile je exploit objeven, jsou jeho signatury zaznamenány a uloženy do neustále rostoucího slovníku signatur. Detekce signatur pro IPS se dělí na dva podtypy:

- **Signatury zaměřené na zneužití** - identifikují jednotlivá zneužití spuštěním na základě jedinečných vzorů konkrétního pokusu o zneužití. IPS může identifikovat konkrétní exploity nalezením shody se signaturou zaměřenou na exploity v datovém toku.
- **Signatury zaměřené na zranitelnost** - použití širších signatur, které se zaměřují na základní zranitelnost v systému, který je cílem útoku. Tyto signatury umožňují chránit sítě před variantami zneužití, které nemusely být přímo pozorovány ve volné přírodě, ale také zvyšují riziko falešně pozitivních výsledků.

Na rozdíl od předchozí implementace IPS založené na anomáliích se sledování abnormálního chování zaměřuje na porovnávání náhodných vzorků síťového provozu a aktivity se základním standardem. Nesoustřeďuje analýzu na signatury, místo toho se zaměřuje na chování celé sítě, identifikuje abnormální vzory a abnormální sekvence provozu, aby mohla vyvolat poplach a použít odpovídající opatření. Ve srovnání s předchozím typem je tento typ robustnější v tom smyslu, že se nezaměřuje pouze na dobře známé zranitelnosti, ale také na možné nové. Ačkoli je robustnější, může také produkovat vyšší míru falešně pozitivních výsledků, pokud není správně nakonfigurován a přizpůsoben bezpečnostní politice. Některé novější a pokročilejší systémy ochrany proti narušení využívají technologie umělé inteligence a strojového učení k podpoře monitorování na základě anomálií, je však nutné použít soubory dat o uvažovaném běžném chování k řádnému vyškolení stroje, což v konkrétním případě kritických systémů není vždy snadný úkol.

IPS založené na anomáliích odebírají vzorky náhodného síťového provozu a porovnávají je s předem vypočtenou základní úrovní výkonu. Pokud je vzorek síťové provozní aktivity mimo zvolené parametry nebo prahové hodnoty základní výkonnosti, IPS přijme opatření k řešení situace.

Třetí typ, systém ochrany proti narušení založený na zásadách, je z těchto tří typů méně častý a využívá bezpečnostní zásady definované podnikem a blokuje činnosti, které tyto zásady porušují. Tento typ IPS vyžaduje celkovou konfiguraci bezpečnostních politik, a tedy důkladné plánování a návrh, stejně jako častou aktualizaci a správu.

Někteří vědci, podobně jako je tomu u IDS, dělí systém IPS podle jeho povahy na další čtyři typy: systém prevence narušení sítě (NIPS), systém prevence narušení hostitele (HIPS), systém analýzy chování sítě (NBA) a systém prevence narušení bezdrátové sítě (WIPS).

První dva typy se opět podobají systémům detekce narušení, které jsou instalovány na úrovni sítě nebo hostitele. Systémy NIPS jsou instalovány na úrovni sítě a pouze na strategických místech, aby monitorovaly celou síť, případně dílčí sítě. Proaktivně sledují síťový provoz a vyhledávají hrozby. HIPS se instaluje na úrovni koncového bodu, například počítače nebo serveru, a zaměřuje se na analýzu příchozího a odchozího provozu daného počítače. Zde je třeba vzít v úvahu, že čím vyšší je počet

HIPS v síti, tím vyšší je vytvořený provoz IPS, a v důsledku toho bude vyšší i zatížení sítě. HIPS funguje lépe v kombinaci s NIPS, protože slouží jako poslední linie obrany proti hrozbám, které pronikly přes NIPS.

Pokud jde o analýzu síťového chování neboli NBA, pracuje s analýzou síťového provozu s cílem odhalit neobvyklé toky provozu, jako jsou například útoky DDoS (Distributed Denial of Service).

Poslední typ IPS, WIPS, je určen speciálně pro bezdrátové sítě, které skenuje a zjišťuje neoprávněné přístupy a vyřazuje neoprávněná zařízení ze sítě.

6.3.3 Architektury implementace systémů prevence narušení

Aby bylo možné chránit před neustále rostoucím počtem sofistikovaných únikových hrozeb, měly by systémy ochrany proti narušení nasadit inline hloubkové učení, které výrazně zlepšuje detekci a přesně identifikuje škodlivý provoz, který nebyl dříve zaznamenán, aniž by se spoléhaly na známé signatury zranitelností a útoků. Podobně jako neuronové sítě nebo jako pracuje lidský mozek, procházejí modely hlubokého učení několika vrstvami analýzy a zpracovávají miliony datových bodů v řádu milisekund. Každé rozhodnutí musí být provedeno opravdu rychle, aby nebyl ohrožen výkon a efektivita sítě. Tyto sofistikované systémy rozpoznávání vzorů analyzují aktivitu síťového provozu s bezkonkurenční přesností a identifikují nový škodlivý provoz, který nikdy předtím nebyl identifikován, v souladu s extrémně nízkou mírou falešně pozitivních výsledků.

Tato další vrstva inteligentní ochrany, kterou může nástroj IPS využívat, poskytuje další ochranu citlivých podnikových informací a zabraňuje sofistikovaným útokům a zranitelnostem, které mohou způsobit velké škody na síti, a tedy i na organizaci nebo společnosti.

Jednou z hlavních obav nejen systémů IDS, ale i nástrojů IPS je míra falešných pozitivních nálezů, kterou mohou produkovat. Každý poplach vyžaduje pozornost správce nebo týmu informačních technologií, což je časově náročné a vyžaduje hlubokou analýzu, aby bylo jisté, že poplach byl skutečně pozitivní. Stejné úsilí vyžadují i falešně pozitivní alarmy, které, pokud nejsou pravdivé, mají negativní dopad na tým a vedou ke ztrátě času a práce.

Stejně jako u systému IDS je i u IPS důležité porozumět bezpečnostním potřebám sítě a organizace, předem naplánovat implementaci a zajistit, aby byly dodrženy všechny bezpečnostní zásady. Také u systému IPS existují různé způsoby implementace, přičemž nejběžnější a nejrobustnější je jeho instalace mezi privátní a veřejnou sítí. Dobré plánování IPS by mělo brát v úvahu faktory, jako je komplexní ochrana v reálném čase proti zranitelnostem sítě a malwaru, stejně jako neznámé příkazy a kontroly. Řešení navíc musí být konzistentní, zjednodušené a umožňovat správnou správu zásad napříč podnikovým perimetrem, datovým centrem, veřejnými a privátními cloudy, mezi dalšími. Kromě toho může být také navrženo tak, aby zahrnovalo nástroje inteligence, jako je strojové učení, pro úspěšné předcházení útokům, a zároveň umožňovalo zachovat vysokou propustnost a nízkou latenci pro nulový výběr kritických hrozeb, aby se správci mohli soustředit na to nejdůležitější a nemarnili čas falešně pozitivními výstrahami.

Pokud jde o kritické infrastruktury, nástroje IPS ještě nejsou účinné a nesprávná implementace může síť více poškodit než ochránit. Kritické systémy, které pracují 24 hodin denně, 7 dní v týdnu, potřebují neustálou komunikaci a tok síťového provozu, přičemž pouhá, byť krátká přestávka může ohrozit nejen systém, ale v závislosti na typu kritického systému i lidské zdraví.

Systém IPS je ze své podstaty schopen blokovat a přerušovat komunikaci, což není vhodné pro použití v kritickém systému, kde komunikace nemůže být nikdy přerušena. Zde musí být plánování a návrh ve srovnání s běžnou počítačovou sítí ještě přesnější a pečlivější. Kritické systémy jsou však také cílem útoků a zranitelností a jejich ochrana je rovněž nutná.

Stejně jako u systémů IDS je běžné, že v síti jsou nainstalovány servery IPS a v různých dílčích sítích a LAN se používají různé servery.

6.4 MALWARE A ANTIVIRUS

6.4.1 Úvod do malwaru

Termín malware poprvé použil Yisrael Radai, počítačový vědec a bezpečnostní výzkumník, v roce 1990. Ačkoli ", existoval již před tímto datem.

Jedním z prvních známých příkladů malwaru byl experiment inženýra společnosti BBN Technbologies Roberta Thomase z roku 1971. Byl pojmenován Creeper a byl určen k infikování infrastruktury ARPANET. Ačkoli malware neměnil funkce ani nekradl data, dokázal se bez povolení přesunout z prvního infikovaného mainframu na druhý.

Abychom lépe pochopili, co je to malware, můžeme se na něj dívat jako na nemoc. V konkrétním případě chřipky má její propuknutí obvykle sezónu, jednou za rok, a obvykle v období chladu a zimy, kdy se začne šířit a infikovat lidi. V konkrétním případě malwaru neexistují žádné předvídatelné sezónní infekce pro osobní počítač nebo jiná zařízení, jako jsou mobilní telefony, tablety a podnikové infekce. Zde lze na malware nahlížet trochu více jako na infekci COVID-19, ke které může dojít v průběhu celého roku a kdykoli a kdekoli. Avšak místo toho, aby uživatelé počítačů pociťovali fyzické příznaky, stejně jako chřipka nebo COVID-19, onemocní jakousi nemocí stroje, která se nazývá malware.

Existuje mnoho různých typů malwarových infekcí a každý typ má svůj vlastní způsob útoku, který se může lišit od skrytého až po nenápadný jako úder kladivem.

Hlouběji definovaný malware nebo také škodlivý software je termín používaný pro označení jakéhokoli škodlivého programu nebo kusu kódu, který poškozuje systémy a sítě.

Záměrem malwaru je napadnout, poškodit nebo vyřadit z provozu počítače, počítačové systémy, sítě a mobilní zařízení, a to jak úplnou, tak částečnou kontrolou nad jejich provozem, narušením jejich běžného fungování a normálního chování.

I když to, co ve skutečnosti stojí za útokem malwaru, se může případ od případu lišit. Malware se může například zaměřit nebo zamýšlet vydělat na uživateli peníze, sabotovat jeho schopnost vykonávat práci, učinit politické prohlášení nebo se zaměřit na prosté chlubení. Malware totiž není schopen vytvořit fyzické hardwarové škody na systémech nebo síťových zařízeních, může šifrovat, krást nebo dokonce mazat data a měnit nebo přebírat základní funkce počítače, špehovat činnost uživatelů s jejich vědomím nebo bez jejich svolení.

Jak ale může uživatel zjistit, zda je jeho zařízení infikované, nebo ne? Stejně jako je tomu u lidské chřipky, kdy se projeví příznaky, které nám umožňují vnímat přítomnost

nemoci v těle, i u malwaru je možné pozorovat mnoho různých projevů chování na infikovaných zařízeních:

- **Zpomalení počítače** - Jedním z hlavních vedlejších účinků malwaru je, že může způsobit snížení rychlosti operačního systému infikovaného zařízení, ať už při přístupu na internet a navigaci, nebo jednoduše způsobuje snížení rychlosti místních aplikací. Také je možné pozorovat, že využití systémových prostředků, jako je využití paměti a procesoru, je abnormálně vysoké. V některých případech je dokonce možné si všimnout, že ventilátor počítače vrčí na plné obrátky, stejně jako že procesor dosahuje vysoké teploty z vyšších nároků na výpočet. To je dobré vodítko, že něco využívá prostředky počítače na pozadí, a je to "příznak", který se obvykle vyskytuje, když byl počítač zapojen do botnetu ("*síť soukromých počítačů infikovaných škodlivým softwarem a ovládaných jako skupina bez vědomí majitelů*").
- **Obrazovka je zaplavena obtěžujícími reklamami** - Velmi nepříjemnou situací, která obvykle identifikuje infekci malwarem, jsou neočekávané vyskakovací reklamy, které zaplavují zařízení různými informacemi a kdykoli. Toto chování je typem malwaru, obvykle známého jako adware, protože se zaměřuje na zobrazování nežádoucích reklam uživateli a obvykle přichází v balení s dalšími skrytými hrozbami malwaru.

- **Pády systému** - Pády systému se projevují zamrznutím nebo modrou obrazovkou smrti, podobně jako v systému Microsoft Windows, kdy se po výskytu fatální chyby zobrazí modrá obrazovka.
- **Záhadná ztráta místa na disku** - Ztráta místa na disku je obvykle způsobena velkým objemem malwaru, který se skrývá na pevném disku. Ten je také známý jako bundleware.
- **Podivné zvýšení aktivity systému na internetu - Pro** lepší pochopení tohoto "příznaku" je možné si vzít za příklad trojského koně. V okamžiku, kdy trojský kůň infikuje počítač, začne se spojovat s útočníkovým řídicím serverem a stahuje sekundární infekci, kterou je mnohdy ransomware. To je jedno z možných vysvětlení zvýšení internetové aktivity. Kromě toho k tomu může dojít

také u botnetů a spywaru, stejně jako u jakékoli jiné hrozby, která vyžaduje neustálou komunikaci se servery útočníka.

- **Změna nastavení prohlížeče** - Mnohokrát je možné si všimnout změny domovské stránky prohlížeče nebo existence nových panelů nástrojů, rozšíření nebo zásuvných modulů, které tam dříve nebyly. K tomu může dojít v důsledku přístupu na infikované stránky nebo kliknutí na infikovanou vyskakovací reklamu.
- **Antivirový software přestane fungovat** - Infekce znemožní opětovné zapnutí antivirové ochrany, zařízení zůstane nechráněné a zranitelnější vůči dalším útokům.
- **Ztráta přístupu k souborům nebo celému počítači** - obvykle souvisí s infekcí ransomwarem, kdy se hackeři ohlásí zanecháním vzkazu nebo zprávy na ploše, případně i změnou tapety plochy na tuto zprávu. Zpráva obvykle obsahuje informaci, že zašifrovali všechna data a výměnou za jejich dešifrování požadují platbu.

Mnoho malwarů také vše zneviditelňuje, takže i když se zdá, že vše funguje normálně, je možné, že je zařízení infikováno malwarem. Výkonný malware se může skrývat hluboko v zařízení, vyhýbat se detekci a vykonávat svou činnost, aniž by vyvolal jakékoli upozornění. Zde je potřeba dobrý bezpečnostní software, který dokáže odhalit infekce, i když nevytvářejí silné a znatelné "příznaky".

6.4.2 Jak se nakazíme malwarem?

Existují dva nejčastější způsoby, jak se malware dostává do systémů a způsobuje infekci: Internet a e-mail. Samo o sobě to znamená, že pokaždé, když jsme připojeni, jsme zranitelní. V dnešní době, kdy jsme neustále připojeni k internetu, když ne na stolním počítači nebo notebooku, tak alespoň na chytrém telefonu nebo tabletu, jsme zranitelní vždy.

Malware může do zařízení proniknout při surfování na hacknutých webových stránkách, při prohlížení legitimních stránek zobrazujících škodlivé reklamy, při stahování infikovaných souborů, při instalaci programů nebo aplikací z neznámých

zdrojů, při otevření škodlivé přílohy e-mailu nebo téměř při všem ostatním, co se stáhne z internetu do zařízení, které nemá nebo má knotovou aplikaci zabezpečení proti malwaru.

Škodlivé aplikace se mohou skrývat ve zdánlivě legitimních aplikacích, zejména pokud jsou stahovány z webových stránek nebo přímých odkazů namísto oficiálního obchodu s aplikacemi. Zde je důležité sledovat varovná hlášení při instalaci aplikací, zejména pokud požadují povolení k přístupu k vašemu e-mailu nebo jiným osobním údajům. Uživatelé mají tendenci vždy stisknout tlačítko další až do konce instalace a nepřečtou si důležité informace, které jsou v průběhu procesu uvedeny. Mnohdy je software třetích stran součástí původní aplikace a nainstaluje se do zařízení. Stejným způsobem se může stát i malware, který může být skrytý uvnitř souboru původní aplikace. Je důležité instalovat software získaný z důvěryhodných zdrojů a od důvěryhodných vývojářů.

Kromě toho je nejlepší držet se také důvěryhodných zdrojů mobilních aplikací, instalovat pouze renomované aplikace třetích stran a vždy stahovat tyto aplikace přímo od výrobce, nikdy ne z jiných webových stránek. Kromě toho se vyhněte stahování těch speciálních nabídek, které slibují zázračnou rychlost internetu, čistič disku a další. Vybírejte takové aplikace z certifikovaných a důvěryhodných zdrojů.

Jak se běžně říká, člověk (uživatel) je hlavním aktérem jakéhokoli typu malwarové infekce. Tedy důvěřivá verze nás samých, která je ochotna otevřít přílohu e-mailu, kterou nepozná, nebo kliknout a nainstalovat něco z nedůvěryhodného zdroje. To není zaměřeno pouze na méně zkušené uživatele, ale i zkušení lidé se do tohoto typu pastí chytili a skončili infikováni malwarem.

I když instalujete něco z důvěryhodného zdroje, je důležité věnovat pozornost žádosti o povolení instalovat současně další přibalený software, protože je možné nainstalovat i nežádoucí software, jak bylo uvedeno výše. Tento dodatečný software, známý také jako potenciálně nežádoucí program (PUP), je mnohokrát prezentován jako nezbytná součást, ale často tomu tak není.

Existuje však také případ, kdy dojde k infekci malwarem bez zavinění. Opět je totiž možné se nakazit pouhou návštěvou škodlivého webu a zobrazením infikované stránky nebo reklamního banneru, který vede ke stažení malwaru. Malware šířený

prostřednictvím špatných reklam na legitimních webových stránkách je tzv. malvertising.

6.4.3 Nejčastější typy malwaru

Mezi mnoha různými typy malwaru je možné identifikovat následující nejčastější formy:

- **Adware** - již dříve zmíněný adware je nechtěný software vyvinutý za účelem zobrazování reklam na obrazovkách uživatelů, často v rámci webového prohlížeče. Tato forma škodlivého softwaru používá podloudnou metodu, která se maskuje jako legitimní nebo se překrývá s jiným programem, aby se skryla a oklamala uživatele pro jeho instalaci.
- **Spyware** - spyware se zaměřuje na tajné sledování činností a aktivit počítače nebo uživatele bez jeho svolení, což hlásí tvůrci malwaru.
- **Virus** - Virus lze také považovat za škodlivý software, protože se rovněž skládá z infekce, která se připojí k jinému programu a po spuštění se replikuje tím, že modifikuje jiné počítačové programy a infikuje je vlastními částmi kódu. Jeho chování je opět podobné viru, který infikuje člověka, kdy napadá tělní buňky, aby do nich vnesl svůj genetický materiál a replikoval se v těle.
- **Červi** - červi jsou podobní virům a stejně jako oni se i červi sami replikují tím, že modifikují jiné počítačové programy a vytvářejí jejich kopie. Rozdíl mezi virem a červem spočívá v tom, že červi se mohou šířit po systémech sami, zatímco viry potřebují nějakou akci ze strany uživatele, aby mohly zahájit proces infekce.
- **Trojský kůň** - Tento malware, známý také jako trojský kůň, je považován za jeden z nejnebezpečnějších typů, protože se obvykle tváří jako něco důvěryhodného, i když tomu tak ve skutečnosti není. Jakmile se dostane do systému, útočníci, kteří za trojským koněm stojí, získají neoprávněný přístup k napadenému počítači. Odtud trojský kůň provádět nejrůznější akce, jako je například krádež finančních informací nebo dokonce instalace dalších forem malwaru.

- **Ransomware** - jak již bylo zmíněno, ransomware je forma malwaru, která může zablokovat přístup uživatele k zařízení, zašifrovat všechna data a soubory a donutit uživatele zaplatit určitou částku peněz, aby získal přístup zpět. Ransomware je jednou z nejpoužívanějších forem malwaru, protože přináší přímý zdroj zisku, obvykle v podobě těžko dohledatelné platby, například v kryptoměně. Bohužel kód, který stojí za ransomwarem, lze snadno získat prostřednictvím online kriminálních tržišť a obrana systémů proti němu je velmi obtížným úkolem.
- **Rootkit** - Tento typ malwaru poskytuje útočníkovi práva správce infikovaného systému nebo sítě, v systémech Unix známá také jako "root". Podobně jako ostatní typy je i rootkit navržen tak, aby byl skrytý a nepostřehnutelný pro uživatele, ostatní software v systému i samotný operační systém.
- **Keylogger** - Keylogger je malware schopný zaznamenávat všechny stisky kláves uživatele na klávesnici, shromažďovat informace a odesílat je útočníkovi. Obvykle tito útočníci hledají autentizační údaje, včetně uživatelských jmen, hesel, údajů o kreditních kartách a dalších.
- **Škodlivé těžení kryptoměn** - Tato forma malwaru, známá také jako "drive-by mining" nebo "cryptojacking", se obvykle instaluje pomocí trojského koně a umožňuje útočníkovi používat počítač k těžbě kryptoměn, jako jsou Bitcoiny nebo Monero. Zde útočníci namísto toho, aby nechali uživatele získané mince zpeněžit, posílají je na svůj vlastní účet.
- **Exploity** - Tato forma malwaru využívá chyb a jiných existujících zranitelností systému nebo sítě k tomu, aby útočníkovi umožnila určitý druh přístupu. Útočník je schopen ukrást data, získat k nim přístup nebo dokonce spustit či injektovat kód, například jinou formu malwaru. Zneužití nultého dne označuje zranitelnost softwaru, pro kterou v současné době neexistuje žádná dostupná obrana nebo oprava.

- **Scareware** - v tomto případě kyberzločinci zastrašují uživatele, aby si mysleli, že jejich počítač nebo mobilní zařízení jsou infikovány, a přesvědčují je, aby si zakoupili falešnou aplikaci. Při typickém scarewarovém podvodu je možné při procházení webu vidět poplašnou

zprávu, která říká: "Varování: "Váš počítač je infikován!" nebo "Máte virus!". Kyberzločinci využívají tyto programy a neetické reklamní praktiky k tomu, aby uživatele vyděsili a přiměli je k nákupu podvodných aplikací.

- **Bezsouborový malware** - Tato forma malwarových útoků na registr nezanechává žádné soubory malwaru, které by bylo možné skenovat, ani škodlivý proces, který by bylo možné detekovat. Nespoléhá se na soubory, a tím nezanechává žádnou stopu, což z něj činí výzvu k odhalení a odstranění. Takový malware využívá k infikování systému nebo sítě legitimní programy.

6.4.4 Jak zjistit, odstranit a zabránit nákaze malwarem

Jak již bylo zmíněno, někdy je možné, aby uživatelé zjistili přítomnost malwarových infekcí a útoků pouhým vnímáním a pozorováním. Ne vždy se to však podaří odhalit a i tak jsou systémy ohroženy. V tomto případě, stejně jako v případě lidského zdraví, i v případě systémů a sítí existuje několik testů, které lze použít, aby bylo zajištěno, že vše je bez infekcí a informace jsou bezpečné.

Mnoho bezpečnostních programů je vyvinuto tak, aby detekovaly malwarové infekce a útoky, předcházely jim a dokázaly je také odstranit. Fungují podobně jako antivirová kontrola, antimalwarové aplikace provádějí skenování počítače, zjišťují a identifikují infekce a poskytují uživatelům možnost je odstranit nebo ponechat soubory v karanténě.

Příkladem antimalwaru je známý Malwarebytes, který zvládá detekci i odstraňování infikovaných souborů a registrů. Funguje pod platformami Microsoft Windows, MacOS, Android a iOS.

Dalším dobrým příkladem je bezplatný nástroj Windows Defender, který se instaluje do počítačů se systémem Microsoft Windows od verze 10 výše. Tento nástroj dokáže chránit místní počítač před hrozbami, jako jsou spyware, adware a viry.

Pokud jde o prevenci útoků malwaru a infekcí, existuje několik různých způsobů ochrany systémů a sítí. V konkrétním případě osobního počítače se provádí instalací jednoduchého antimalwarového softwaru, jako jsou ty výše uvedené. Aplikace sama o sobě však k řádné ochraně nestačí, uživatelé musí na svých zařízeních také dodržovat zásady bezpečného chování. To zahrnuje neotevírání příloh od nedůvěryhodných odesílatelů a přístupy na nedůvěryhodné webové stránky.

Tyto antimalwarové aplikace by navíc měly být pravidelně aktualizovány a kontrolovány, protože hackeři se neustále přizpůsobují a vyvíjejí nové techniky prolamování bezpečnostního softwaru. Kromě toho vývojáři bezpečnostního softwaru také pravidelně vydávají aktualizace, které tyto zranitelnosti opravují. Pokud uživatelé zanedbají aktualizaci svých bezpečnostních nástrojů, tyto záplaty se neaplikují, což je činí zranitelnými vůči zneužití, kterému lze předejít.

V podnikovém prostředí, kde jsou sítě a systémy rozsáhlejší než jednoduché domácí sítě, má závažnost útoku mnohem větší škody. Zde jsou některé proaktivní kroky k prosazení ochrany před malwarem nutností:

- Zavedení dvojího schvalování transakcí mezi podniky (B2B);
- Zavedení ověřování druhým kanálem pro transakce mezi podniky a spotřebiteli (B2C);
- Zavedení offline detekce malwaru a hrozeb pro zachycení škodlivého softwaru dříve, než se rozšíří;
- Implementace zásad zabezpečení seznamu povolených položek, kdykoli je to možné;
- Implementace silného zabezpečení na úrovni webového prohlížeče.

6.4.5 Specifický případ antiviru

Kromě antimalwarového softwaru a nástrojů existují také antivirové programy, které si poradí s konkrétním typem malwaru (viry). Antiviry jsou mnohem známější a téměř každý uživatel je má nainstalované na svých stolních počítačích a noteboocích. Antivirus je program, který slouží k prevenci, skenování, detekci a odstraňování virů z počítače, systému nebo sítě. Většina antivirových programů se po instalaci spouští automaticky na pozadí a poskytuje ochranu instalovaného systému v reálném čase, čímž zabraňuje virovým infekcím a útokům.

Komplexní ochranné programy pomáhají chránit soubory a hardware před škodlivým softwarem, jako jsou červi a viry, ale také před trojskými koni a spywarem. Další ochrana je však důležitá a tyto nástroje by měly fungovat společně s firewally a

antimalwarovými nástroji, čímž se zvýší úroveň zabezpečení, a tím se zajistí vysoká úroveň ochrany dat.

Antivirové programy a software na ochranu počítače jsou obecně vyvinuty tak, aby analyzovaly data, včetně nejen místních souborů, ale také webových stránek, nainstalovaných aplikací a dalšího softwaru, a pomohly tak co nejrychleji najít a odstranit škodlivý software.

Většina antivirových nástrojů poskytuje ochranu v reálném čase, běží na pozadí a je schopna chránit zařízení před příchozími hrozbami, útoky a virovými infekcemi. Neustále skenuje zařízení na známé hrozby a poskytuje automatické aktualizace, identifikuje, blokuje a odstraňuje škodlivé kódy a viry.

V dnešní době se většina činností provádí online, a proto se každý den objevují nové hrozby, a proto je důležité používat ochranný antivirový program. Naštěstí je dnes na trhu také mnoho vynikajících produktů, které si s těmito hrozbami a infekcemi dokážou poradit. Mezi hlavními vývojáři antivirových programů je možné vyzdvihnout mimo jiné společnosti Norton, McAfee, TrendMicro a Checkpoint.

6.4.6 Jak funguje antivirus

Prvním krokem je samozřejmě instalace, ale kromě ní a po instalaci začne antivirový program kontrolovat počítač nebo server, na kterém je nainstalován, na přítomnost programů a souborů v databázi známých typů malwaru. Vzhledem k tomu, že každý den vznikají nové viry, které stále šíří hackeři, antivirový nástroj také kontroluje zařízení na možnost výskytu nových nebo neznámých hrozeb a infekcí.

Většina programů obvykle pracuje ve třech různých režimech detekce, z nichž první je specifická detekce, kdy identifikuje známý malware, druhý je generická detekce, která hledá známé části nebo typy malwaru nebo vzory, které vykazují souvislost se společnou kódovou základnou, a třetí se zaměřuje na heuristickou detekci, kdy vyhledává neznámé viry a infekce pomocí identifikace známých podezřelých struktur souborů. Když program najde soubor, který obsahuje virus, obvykle jej umístí do karantény a označí jej k odstranění. V karanténě je možné vyhodnotit chování souboru a určit, zda je nutné jej ze zařízení odstranit.

Je však důležité si uvědomit, že i když je antivirový program schopen chránit systém nebo síť, ve které je nainstalován, není schopen ji ochránit před všemi typy

malwaru. Pro lepší pochopení je nutné si uvědomit, že antivirový software může malware identifikovat dvěma různými způsoby: detekcí signatur a detekcí chování. Stejně jako systémy IDS a IPS se i antivirové nástroje zaměřují na dva různé přístupy, přičemž využívají známých zranitelností a signatur a chování infekcí.

Pokud jde o detekci signatur, lze ji opět chápat jako lidský imunitní systém, který skenuje tělo (počítač) a hledá zvláštní charakteristiky nebo signatury programů, o nichž je známo, že souvisejí se škodlivým kódem, infekcí nebo hrozbou. Dělá to tak, že se odvolává na slovník známého škodlivého softwaru, vytvořený na základě známých signatur. Pokud něco v systému odpovídá vzoru přítomnému v databázi, program se to pokusí zneškodnit, umístí do karantény nebo jednoduše odstraní. Kromě toho, a opět s odkazem na lidský imunitní systém, slovník nebo databáze vyžaduje aktualizace. Když se v oblasti lidského zdraví necháváme očkovat nebo užíváme léky v tabletách, v počítačích jsou aktualizace rozhodující pro udržení správné úrovně ochrany. Tyto aktualizace umožňují antivirovým nástrojům rozpoznat nový a dosud neznámý škodlivý software, hrozby a zranitelnosti.

Antivirový software může chránit systém pouze před tím, co rozpozná jako škodlivé, přičemž problémem je, že kybernetických útoků neustále přibývá a jsou prováděny každým dnem sofistikovanějším způsobem. Vývoj nových zneužití a útoků je tak velký, že výrobci antivirových programů musí běžet proti času, aby byli schopni dohnat neustálé požadavky na ochranu. Výsledkem je, že bez ohledu na to, jak nedávno byl antivirový program aktualizován, se vždy objeví nějaký nový malware, který případně dokáže antivirový a antimalwarový software a nástroje obejít.

Při zaměření na detekci chování se antivirový program nesnaží identifikovat známý malware, stejně jako při použití metody detekce signatur. Místo toho sleduje chování softwaru nainstalovaného v počítači, který antivir chrání. Aby bylo možné antivirový nástroj správně vycvičit, je nutné, aby software měl znalosti o tom, jak vypadá běžné chování softwaru, který sleduje. Když se pak program chová podezřele, například se pokouší získat přístup k chráněnému souboru nebo modifikovat jiný program, antivirový program založený na chování podezřelou aktivitu odhalí a upozorní na ni uživatele, který tak může na hrozbu odpovídajícím způsobem reagovat. Tento přístup je zvláště úspěšný při ochraně systému proti novým typům škodlivého softwaru, které dosud neexistují ve slovnících nebo databázích a jejichž signatury

dosud nebyly objeveny ani zdokumentovány. Problémem však je, že tento přístup může zvýšit počet falešných varování. Je možné, že si jako uživatel počítače nebudete jisti správným postupem při takových falešných poplaších, což vám umožní nesprávně povolit akce. Navíc při velkém počtu varování může být uživatel v pokušení povolit všechny, čímž ponechá počítač otevřený útokům a infekcím. Kromě toho v době, kdy je chování zjištěno, se již v systému s největší pravděpodobností spustil také škodlivý software, takže si uživatel není jistý, jaké akce malware provedl předtím, než jej antivirový software identifikoval.

Antivirus je důležitou součástí zabezpečení počítače, systému, sítě nebo mobilního zařízení a doporučuje ho většina vědců a výzkumníků v této oblasti. Klíčové však je, že bez ohledu na typ a značku antivirového softwaru není schopen ochránit systém před všemi typy malwaru.

6.4.7 Výběr dobrého antivirového softwaru

Mezi rozsáhlým množstvím antivirových řešení existuje několik bodů, které bychom měli vzít v úvahu i po výběru nejlepšího řešení pro ochranu našich systémů:

1. Antivirový software pořizujte pouze ze známých, důvěryhodných zdrojů a od důvěryhodných dodavatelů. Častým trikem kybernetických útočníků je šíření falešných antivirových programů, které jsou ve skutečnosti malwarem.
2. Ujistěte se, že máte nainstalovanou nejnovější verzi antivirového softwaru, že máte zaplacené a aktivní předplatné a že je antivirový program nastaven na automatickou aktualizaci. Aktualizace by nikdy neměly být odkládány.
3. Ujistěte se, že antivirový program automaticky skenuje přenosná média, například USB klíčenky, a zajistěte, aby byla zapnuta ochrana v reálném čase.
4. Věnujte pozornost varováním a výstrahám na obrazovce, které antivirový software generuje. Většina výstrah obsahuje možnost získat další informace nebo doporučení, co dělat dál.
5. Nevypínejte nebo neodinstalovávejte antivirový software, protože má pocit, že zpomaluje počítač, blokuje webové stránky nebo brání instalaci aplikace či programu. Vypnutím antivirového programu vystavíte systém zbytečnému riziku a mohlo by dojít k závažnému bezpečnostnímu incidentu.

6. Neinstalujte do systému více antivirových programů najednou. Je pravděpodobné, že to způsobí vzájemné konflikty programů a může to skutečně snížit zabezpečení počítače.
7. Naučte se rozpoznávat varování, která antivirový software vydává. Kybernetičtí útočníci mohou vytvořit škodlivé webové stránky, které zveřejňují velmi realistická, ale falešná antivirová varování a nabízejí vám pomoc při "opravě" vašeho počítače. Kliknutí na odkazy nebo tlačítka na těchto webových stránkách může ve skutečnosti poškodit váš počítač.