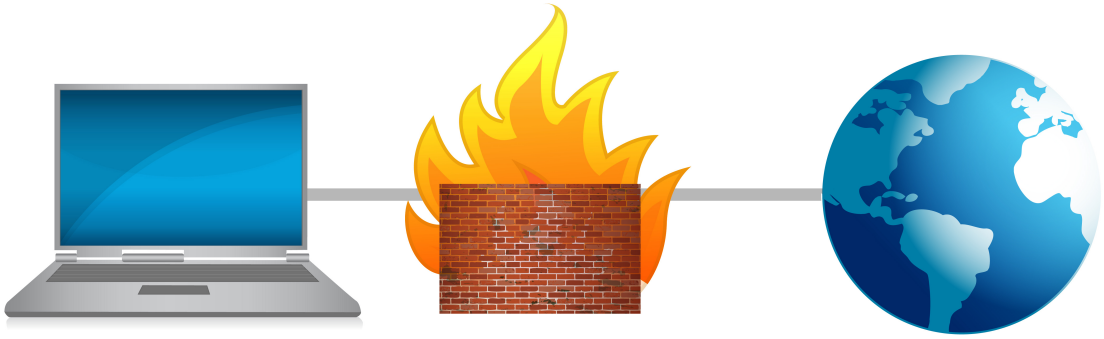
KOMPLEKSOWE ZABEZPIECZENIE SIECI

Publikacja sfinansowana z funduszy Komisji Europejskiej w ramach programu Erasmus+. Publikacja została zrealizowana przy wsparciu finansowym Komisj Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska oraz Narodowa Agencja Programu Erasmus+ nie ponoszą odpowiedzialności za jej zawartość merytoryczną. PUBLIKACJA BEZPŁATNA

Spis treści

1. FIREWALLS



- Wprowadzenie do zapór ogniowych
- Potrzeba firewall'a
- Rodzaje i charakterystyka zapór ogniowych
- Topologie i architektury firewalli
- Przykłady firewalli

1.1. Wprowadzenie do zapór ogniowych

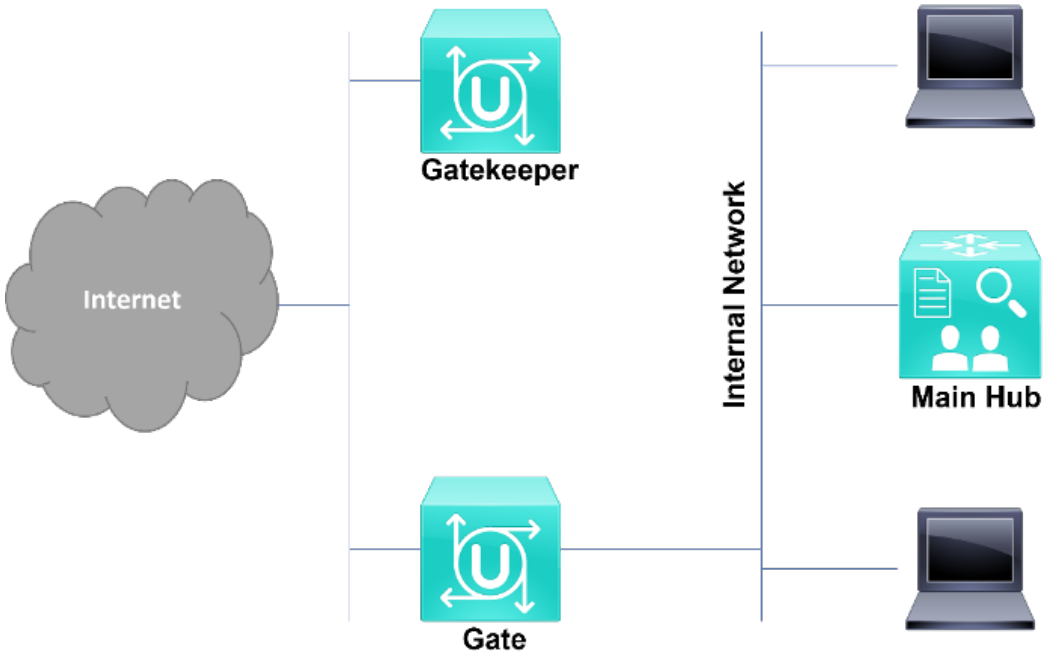
Szeroko stosowany obecnie termin firewall jest przywoływany przez wszelkiego rodzaju użytkowników technologii informatycznych, odnosząc się nie tylko do komputerów, ale również do urządzeń mobilnych, a poprzez swoje dosłowne znaczenie - ściana ognia - jest dobrze znany jako jeden z głównych mechanizmów bezpieczeństwa wdrażanych na całym świecie.

Choć jest bezpośrednio związane z technologiami informatycznymi, słowo firewall nie narodziło się wraz z internetem. Było już używane w domach, samochodach, między innymi. Jeden z głównych przykładów związany jest z drzwiami, które zapobiegają rozprzestrzenianiu się ognia po budynkach, podczas gdy strażacy próbują go opanować. Pierwsze firewalle zostały opracowane pod koniec 1980 roku, zaraz po odkryciu pierwszego wirusa komputerowego, nazwanego "Morris Worm", który zainfekował wiele dużych organizacji, takich jak NASA, Uniwersytety Berkeley i Stanford, pokazując, że Internet nie był już zamkniętą społecznością i był używany tylko przez zaufanych ludzi.

Na samym początku firewalle nie były niczym więcej niż prostymi routerami, skonfigurowanymi w celu rozdzielenia sieci prywatnej na mniejsze (Local Area Networks lub LANs), zapobiegając rozprzestrzenianiu się błędów sieciowych w całej sieci LAN, a w konsekwencji poprawiając jej globalną wydajność. Ten typ zapory był używany głównie w latach 90. i opierał się na regułach filtrowania, gdzie nacisk kładziono na adres IP, pozwalając wszystkim urządzeniom w sieci prywatnej na dostęp do Internetu lub sieci publicznej (ruch wychodzący) i blokując publiczne adresy IP przed wejściem do prywatnej sieci LAN. Zapory te nie były tak wydajne i były bardzo ograniczone, ponieważ nie zapewniały właściwego sposobu budowania silnych reguł bezpieczeństwa i dostępu, uniemożliwiając ograniczenie dostępu do określonej części aplikacji lub oprogramowania.

Druga generacja zapór ogniowych dała możliwość badania również warstwy transportowej (czwarta warstwa OSI), zamiast ograniczać się do adresu IP (trzecia warstwa OSI). Mając wiedzę o aktywnych sesjach, firewalle mogły następnie wykorzystać te informacje do zwiększenia przepustowości sieci oraz szybkości i wydajności przetwarzania pakietów. Przez to filtracja odbywała się nie tylko po adresie IP, ale także po atrybutach komunikacyjnych.

W swojej trzeciej i nowszej generacji, znanej również przez filtrowanie aplikacji, zapory ogniowe wykorzystują poprzednie dwie technologie, związane z serwerem proxy, pracującym jako agent pośredni, aby ocenić wymagania każdej komunikacji, która przychodzi lub odchodzi z naszych połączonych sieci. Ten proxy może być postrzegany jako człowiek drzwi, gdzie przepuszczane są tylko te osoby, którym przyznano uprawnienia do określonego miejsca przeznaczenia (rysunek 1).



Rysunek 1 - Trzecia generacja zapory ogniowej

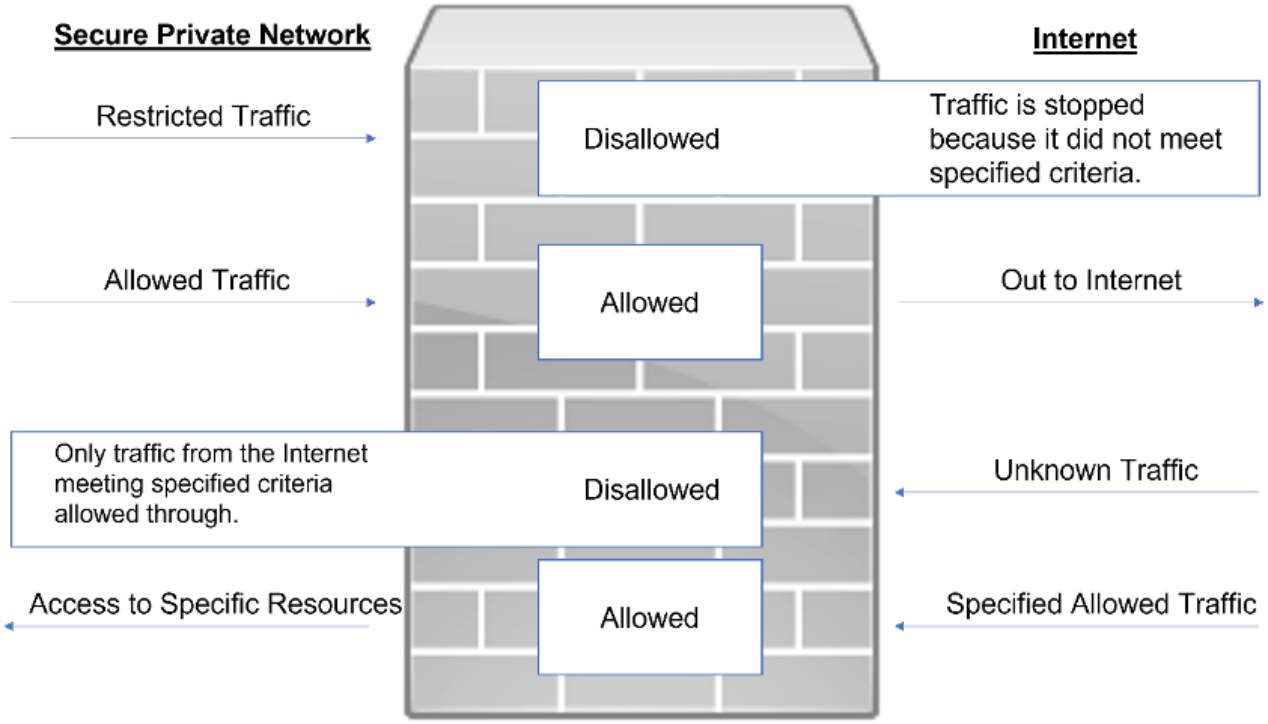
Firewall może być postrzegany jako jedno lub więcej urządzeń, obejmujących zarówno oprogramowanie, jak i sprzęt, strategicznie umieszczonych na granicy dwóch różnych sieci, zwykle nazywanych sieciami prywatnymi i publicznymi (rysunek 2).

Na podstawie jego wdrożenia, między tymi dwoma sieciami, jest w stanie sprawdzić i przeanalizować wszystkie pakiety sieciowe, które przychodzi do niego, poprzez jego różnych interfejsów, a to działa jak to było kontroler graniczny na lotnisku, sprawdzanie wszystkich paszportów i zezwoleń wizowych z tego konkretnego pakietu, pozwalając mu iść przez lub lustracji jego dostęp. Wykorzystując tę główną

zasadę, technologia ta zapobiega przedostawaniu się niepożądanych komunikatów z sieci publicznych do sieci prywatnych lub odwrotnie, a w konsekwencji chroni informacje i zasoby w naszych prywatnych systemach.

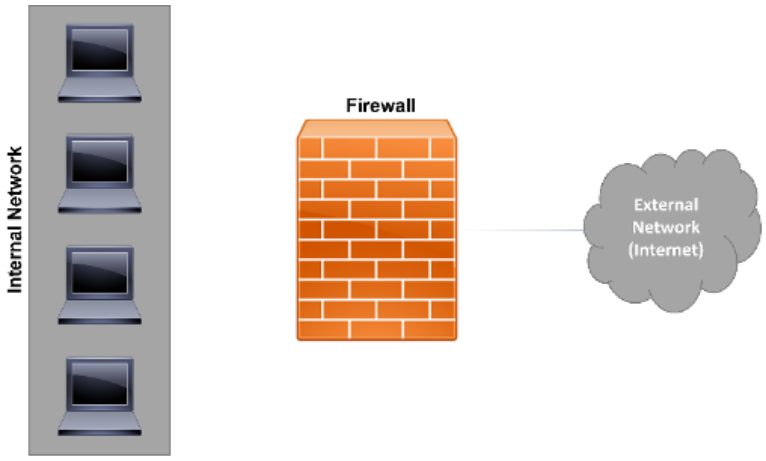
Ponadto, ten rodzaj filtrowania jest również w stanie uniknąć urządzeń wewnętrznych z dostępu do domen i informacji, które nie idą zgodnie z polityką bezpieczeństwa sieci. W przypadku prostych sieci, takich jak domowe, firewall jest zwykle implementowany w oprogramowaniu routera. W przypadku większych sieci, w tym korporacyjnych, zaleca się stosowanie solidnego firewalla sprzętowego, przeznaczonego do ochrony granic sieci, upewniając się, że dozwolona jest tylko niezbędna komunikacja i funkcje oraz zapewniając bezpieczeństwo sieci.

Należy również podkreślić, że aby uchronić sieć przed atakami, firewall musi być w stanie zapobiec atakom przeciwko sobie, na obu poziomach, wewnętrznym i zewnętrznym (sieci prywatne i publiczne).



Rysunek 2 - Rozwiązanie zabezpieczające, umieszczone pomiędzy siecią prywatną a publiczną

Jak już zostało powiedziane, firewall może być oparty zarówno na rozwiązaniach sprzętowych, jak i programowych, gdzie najczęściej spotykana jest druga opcja, nie tylko przez swój koszt i sposób implementacji, ale również dlatego, że jest obecna w niemal każdym systemie sieciowym i komputerach osobistych. Działając w oparciu o zestaw reguł lub instrukcji, firewall analizuje ruch sieciowy w celu określenia dozwolonych działań związanych z przesyłaniem lub odbieraniem danych. Również przez swoją dosłowną nazwę daje do zrozumienia, że system ten jest w zasadzie blokadą niepożądanego ruchu, dopuszczając jedynie określony ruch sieciowy, który jest zgodny ze skonfigurowanymi regułami dostępu (rysunek 3).



Rysunek 3 - Podstawowa reprezentacja wdrożenia zapory ogniowej

Podsumowując, najważniejszą koncepcją jest to, że firewall jest systemem bezpieczeństwa zdolnym do ochrony sieci prywatnej przed atakami z zewnątrz, będąc jednocześnie w stanie kontrolować komunikację, w oparciu o reguły, które są zbudowane w kierunku polityki bezpieczeństwa organizacji. Jest on obecny nie tylko w sieciach wysokiego poziomu, takich jak korporacyjne, ale również jako oprogramowanie w routerach domowych połączeń internetowych, komputerach stacjonarnych, laptopach, a nawet urządzeniach mobilnych.

1.2. Potrzeba Firewall'a

Istnieją różne powody, dla których warto stosować firewall sieciowy, gdzie najważniejszy z nich związany jest z ochroną komputerów, serwerów i innych urządzeń w sieci prywatnej. Często słyszy się, że "nie mam żadnych ważnych informacji, które mogłyby zostać skradzione", jednak ataki mogą być przeprowadzane z innych powodów, takich jak wykorzystanie mocy obliczeniowej i pamięciowej komputerów w sieci, a nawet wykorzystanie tych komputerów do kradzieży informacji online, danych kont bankowych, między innymi. Wśród najczęstszych ataków można wyróżnić:

· *Downstream Liability:*

Sieć może być wykorzystana jako dostęp do ataku na inne sieci.

· *Utrata danych:*

Niektórzy crackerzy uzyskują dostęp do sieci i usuwają pliki i informacje, nie dlatego, że są to dla nich cenne informacje, ale najczęściej po to, aby pokazać, że są w stanie to zrobić. To pokazuje potrzebę odpowiedniego zabezpieczenia danych i tworzenia kopii zapasowych informacji.

· *Wyciek poufnych danych:*

Prywatność i szczególna ochrona danych osobowych i innych poufnych danych jest obecnie jednym z głównych problemów w dziedzinie bezpieczeństwa danych. Ataki na systemy i urządzenia przechowujące poufne informacje są jednymi z najczęściej stosowanych, a ich ochrona jest głównym celem wszystkich organizacji. Celem ataków są nie tylko informacje osobiste, takie jak nazwiska i kontakty klientów, ale również poufne projekty i wrażliwe informacje. Ochrona tych systemów jest bardzo ważnym zadaniem, gdzie plan bezpieczeństwa musi być starannie zaplanowany i wdrożony.

· *Denial-of-Service:*

Bez firewalla sieci są narażone na ataki, które mogą spowodować różne poziomy uszkodzeń sieci i jej systemów. Bardzo często spotykany jest również atak denial of service, który może spowodować, że sieć stanie się nieosiągalna i nie będzie reagować na komunikację i wywołania systemowe. Biorąc za przykład szpital, gdzie ważne informacje zawsze przepływają przez sieć, i gdzie życie ludzkie zależy od łatwego i szybkiego dostępu do tych informacji, atak typu denial-of-service może spowodować poważne szkody, nie tylko dla sieci i organizacji, ale także dla życia ludzkiego.

Jak można zrozumieć w tym momencie, niezabezpieczona sieć, otwiera napastnikom możliwość uzyskania dostępu lub spowodowania uszkodzenia informacji i prywatnych systemów, przejęcia nad nimi kontroli i wykonania najszerszych możliwych zadań przeciwko samej sieci lub innym sieciom.

Firewall, choć jest ważnym i głównym urządzeniem, ma również swoje ograniczenia i wady. Główne ograniczenia związane są z typem rozwiązania i zastosowaną architekturą implementacji. Urządzenia te są rzeczywiście istotnym zabezpieczeniem, które należy stosować, jednak daleko im jeszcze do doskonałości, gdzie możemy wyróżnić następujące ograniczenia:

· Może ona zapewnić pożądany poziom bezpieczeństwa, jednak pogarszając wydajność sieci lub urządzenia.

· Polityki bezpieczeństwa muszą być regularnie aktualizowane i przeglądane, aby usługi sieciowe nie były zagrożone.

· Nowe usługi sieciowe i protokoły mogą nie być właściwie identyfikowane i traktowane przez istniejące zapory.

· Może nie być w stanie odpowiednio zabezpieczyć sieci prywatnej przed złośliwym działaniem.

· Może nie być w stanie wykryć złośliwego insidera lub złośliwej aktywności, która pochodzi od dozwolonego użytkownika.

· Firewall musi być często analizowany i konfigurowany, aby napastnicy nie mogli odkryć luk w zabezpieczeniach.

· Zapory sieciowe nie mogą kontrolować połączeń, które są przez nie wykonywane.

Pomijając te ograniczenia, firewalle są nadal jednym z betów mechanizmów bezpieczeństwa, które należy wdrożyć w sieci, aby podnieść jej poziom bezpieczeństwa, przynosząc istotne korzyści:

· **Ochrona przed usługami podatnymi na zagrożenia** - dopuszczenie tylko określonych i niezbędnych protokołów sieciowych i komunikacyjnych.

· **Kontrolowany dostęp do wewnętrznych stron i systemów** - uniemożliwia dostęp nieuprawnionym użytkownikom i napastnikom.

· **Wyśrodkowane bezpieczeństwo** - możliwe jest wyśrodkowanie wszystkich polityk bezpieczeństwa i dostępu w jednym urządzeniu lub oprogramowaniu firewall.

· **Zwiększony poziom prywatności** - Możliwość zablokowania dostępu do informacji o logowaniu.

Ponadto można wskazać również pewne wady:

· **Ograniczenie dostępu do ważnych usług sieciowych** - najczęstszą wadą stosowania firewalla jest ograniczenie dostępu do popularnych i ważnych usług, takich jak TELNET czy FTP. Choć ta wada dotyczy nie tylko firewalli, ale także innych systemów zabezpieczeń.

· **Konieczność zrównoważenia planu bezpieczeństwa** - aby właściwie umożliwić komunikację i dostęp do istotnych usług, należy znaleźć równowagę między potrzebami a polityką bezpieczeństwa. Konieczne jest ograniczenie wykorzystania portów i zapobieganie wewnętrznym atakom.

· **Ochrona** przed wirusami - ponieważ wirus może mieć różne kodyfikacje i być skompresowany na wiele różnych sposobów, firewall nie jest uważany za najlepsze rozwiązanie do ochrony sieci przed infekcją wirusową.

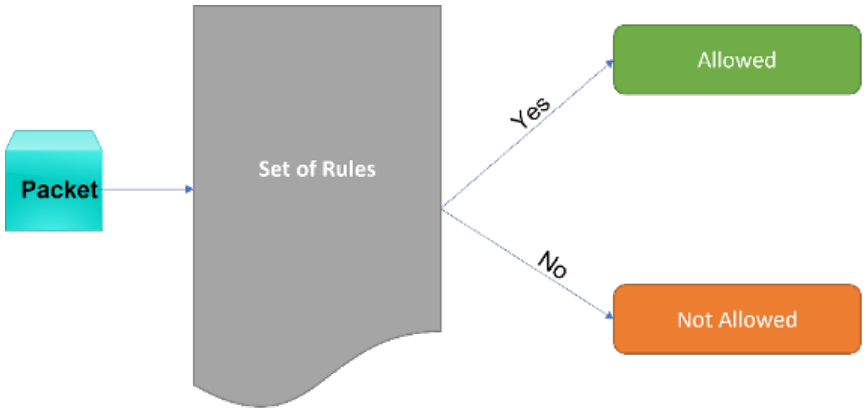
1.3. Rodzaje i charakterystyka zapór ogniowych

Firewall może działać na różne sposoby, w oparciu o metodologię twórcy, specyficzne potrzeby chronionego systemu, charakterystykę systemu operacyjnego strukturę sieci i tak dalej. Można więc spotkać różne rodzaje firewalli zaimplementowanych w naszych sieciach, w tym:

· Filtrowanie pakietów

Filtrowanie pakietów było pierwszym opracowanym typem firewalla, w którym zastosowano prostą, ale ograniczoną metodologię, skupiając analizę na adresach IP pakietów (rysunek 4).

Transmisja danych odbywała się w oparciu o protokół TCP/IP (Transmission Control Protocol/Internet Protocol), który jest zorganizowany w różne warstwy. Zazwyczaj filtrowanie pakietów ogranicza się do warstwy sieciowej i transportowej: pierwsza obejmowała adres IP ze wszystkich urządzeń w sieci i wszystkie procesy routingu; druga obejmowała protokoły transportowe, które umożliwiają ruch i transmisję danych, takie jak TCP. W oparciu o te podstawowe pojęcia, firewalle wykorzystujące filtrowanie pakietów były w stanie po pierwsze filtrować pakiety na podstawie ich adresów, zarówno źródłowych, jak i docelowych, a także filtrować pakiety na podstawie ich portów TCP i UDP (User Datagram Protocol). Jako przykład może posłużyć blokowanie ruchu z adresu IP 192.168.1.1 na porcie TCP 80. Wszystkie usługi pracujące na tym porcie byłyby dostępne z urządzenia o wspomnianym adresie IP.



Rysunek 4 - Prosta reprezentacja podejścia do filtrowania pakietów

· Filtrowanie statyczne i dynamiczne

Łącząc wszystkie funkcje z poprzedniego typu, można również spotkać firewalle realizujące filtrację pakietów na dwa różne sposoby, gdzie pierwszy z nich skupia się na filtracji statycznej, a drugi, nieco bardziej rozbudowany, na filtracji dynamicznej. W pierwszym modelu (statycznym), dane są blokowane lub dopuszczane po prostu na podstawie reguł, nie biorąc pod uwagę żadnych zależności pomiędzy pakietami czy ich połączeniem. Na początku takie podejście nie sprawiało żadnych problemów, jednak niektóre nowe usługi sieciowe lub aplikacje mogą opierać swoją poprawną komunikację i transmisję danych na zapytaniach i odpowiedziach, tworząc specyficzny przepływ pakietów, powiązany między nimi. Przez to, używając pierwszego modelu, możliwe jest spowodowanie zakłóceń w komunikacji, co skutkuje nieprawidłowym działaniem aplikacji lub usługi. Ponadto, może to być również postrzegane jako problem bezpieczeństwa, gdzie administrator sieci byłby zmuszony do tworzenia pojedynczych i konkretnych zasad, aby uniknąć tych usług z awarii, zwiększając możliwość nie blokowania pakietów, które rzeczywiście powinny być zablokowane.

Z drugiej strony, dynamiczna filtracja przyszła, aby rozwiązać takie ograniczenia. W tym modelu filtrowania pakietów, filtry biorą pod uwagę kontekst pakietów, aby stworzyć reguły zdolne do dostosowania się do sytuacji, a co za tym idzie, dopuszczające określony ruch pakietów do pracy, gdy jest to konieczne i tylko w określonym czasie. Dzięki temu szanse na zablokowanie zaufanych pakietów drastycznie maleją.

· Osobiste firewalle

Istnieją również proste zapory sieciowe przeznaczone do ochrony komputerów osobistych i urządzeń mobilnych, które mogą być używane przez zwykłego użytkownika. Dzisiejsze systemy operacyjne zawierają już oprogramowanie zapory, w tym Microsoft Windows, Linux i Mac OS X. Ponadto, istnieją pewne oprogramowanie antywirusowe, które obejmują różne poziomy ochrony i zapory. Te zapory, mają ograniczoną wydajność i ochronę, pozwalając użytkownikom zastosować proste zasady i skonfigurować dostęp z aplikacji i usług do Internetu. Chociaż zwiększają one poziom bezpieczeństwa urządzenia, nadal istnieje możliwość ich obejścia i uczynienia urządzenia celem ataku. Hakerzy mogą łatwo obejść takie zapory i wykorzystać luki w systemie. W sieci korporacyjnej zaleca się również stosowanie ramek brzegowych, takich jak wyjaśniono wcześniej.

· Firewall programowy i sprzętowy

Wspomniane wcześniej firewalle mogą być realizowane zarówno w sposób sprzętowy, jak i programowy. Sama w sobie informacja ta nie jest błędna, jednak należy dodać, że sam sprzęt to nic innego jak urządzenie, na którym zainstalowane jest oprogramowanie firewalla. Zazwyczaj nazywane urządzeniami firewall, urządzenia te są dedykowane do pełnienia wyłącznie roli firewalla i mogą zawierać różne konfiguracje i porty, aby łączyć się z różnymi sieciami. Ponadto, takie urządzenia są zwykle używane w większych sieciach, gdzie jest znaczna ilość ruchu sieciowego, lub gdzie dane są wrażliwe. Główną zaletą tych zapór jest to, że ponieważ sprzęt został opracowany specjalnie do tego celu, może poradzić sobie z większymi ilościami danych i nie są podatne na ataki, które zwykle występują w konwencjonalnym serwerze.

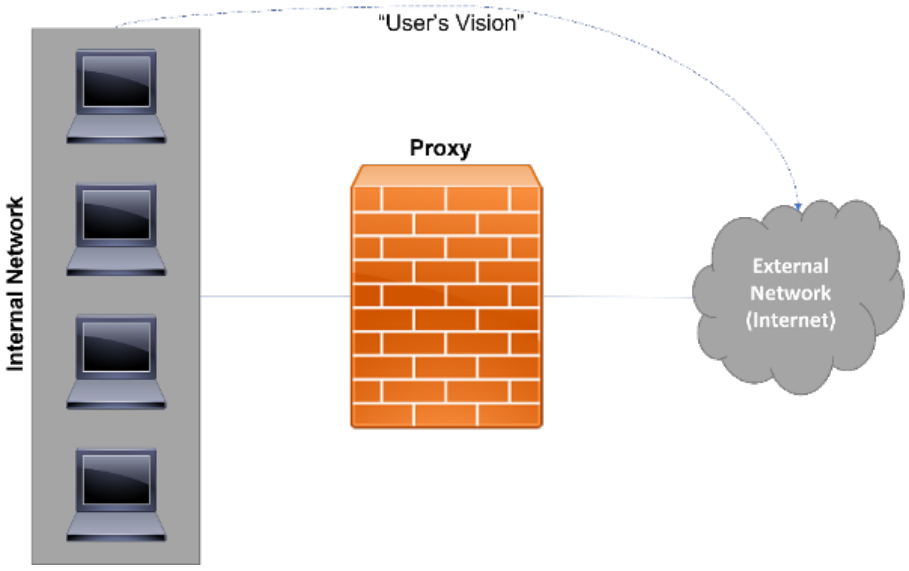
· Firewall oparty na stanie

Po prostej filtracji pakietów, przyszła technologia state-base zastosowana w firewallach. Spowodowało to niemal rewolucję w sposobie działania firewalli, ponieważ zamiast prostej analizy pakietów, gdy przechodziły one przez firewall, i blokowania lub dopuszczania ich zgodnie z prostymi regułami, firewalle oparte na stanach manipulują dynamiczną informacją i utrzymują swoje działania monitorujące, analizując pakiety nawet w trakcie ich przemieszczania się w sieci. Podczas gdy firewall typu packet filtering był w stanie jedynie blokować lub dopuszczać pakiety w oparciu o ich adresy IP i porty, firewall typu state-based może wykrywać i blokować nielegalny ruch sieciowy w oparciu o wzorce i inne zaawansowane koncepcje stanu. Należy jednak podkreślić, że ten typ zapory ma wadę związaną z koniecznością przechowywania danych o ruchu w pamięci oraz głębszej i mocniejszej analizy, która wymaga większej mocy obliczeniowej i możliwości przechowywania danych.

· Firewall aplikacji

Choć technologia ta jest stosowana do dziś, sama w sobie nie wystarcza, by odpowiednio zabezpieczyć sieć przed atakami i włamaniami. Firewalle aplikacyjne i webowe narodziły się jako kolejny wielki krok w dziedzinie bezpieczeństwa. Tradycyjne firewalle ograniczały się do ogólnej analizy i monitorowania ruchu sieciowego, nie potrafiąc odpowiednio wykryć ruchu pochodzącego z aplikacji, usług lub innego oprogramowania. Te nowe firewalle aplikacyjne zostały zaprojektowane, aby poradzić sobie z tą luką, będąc w stanie zablokować próby włamań, które wykorzystują podatności możliwe do wykorzystania. Ponadto, wiele z nich posiada kontrolę rodzicielską, będąc w stanie wykryć rodzaj treści i określić, czy jest ona odpowiednia do oglądania przez młodych ludzi.

· Proxy



Rysunek 5 - Przykład implementacji serwera proxy pomiędzy siecią zewnętrzną a wewnętrzną

Działając jako serwer proxy, filtrujący zasadniczo zawartość http i dostępy do przeglądarki, firewall może być wdrożony pomiędzy siecią prywatną a publiczną (Rysunek 5). W ten sposób cały ruch jest analizowany i monitorowany, co pozwala na lepszą kontrolę dostępu i transmisji danych. Choć można też zaimplementować go jako zwykły serwer, zmuszając do przekazywania przez niego całego ruchu http. Jest to powszechnie stosowane przez wiele organizacji, gdzie wymaga się, aby wszystkie przeglądarki internetowe były skonfigurowane tak, aby wysyłały ruch do serwera proxy w celu analizy. W konsekwencji główny firewall musi blokować cały ruch http, który nie pochodzi z serwera proxy. Tylko w ten sposób możliwa jest właściwa kontrola żądań i odpowiedzi http.

· Firewall nowej generacji

Firewall następnej generacji był ostatnią koncepcją, która została opracowana i skupia się głównie na świecie korporacyjnym. Ten nowy typ zapory łączy wszystkie poprzednie w jeden scentralizowany filtr, zdolny do analizy i monitorowania pakietów, włamań i zapobiegania aplikacjom i usługom, między innymi. Firewalle te można również znaleźć jako usługę online, jednak większość z nich jest nadal

stosowana jako urządzenie. Jako bardziej wytrzymałe i z głębszą analizą, ich wdrożenie jest bardziej złożone i musi być starannie wykonane, gdzie odpowiedni plan bezpieczeństwa powinien być opracowany i regularnie aktualizowany. Używane jako główny mechanizm bezpieczeństwa, te firewalle są często instalowane na granicy pomiędzy sieciami prywatnymi i publicznymi, kontrolując ruch przychodzący i wychodzący.

1.4. Topologie i architektury firewalli

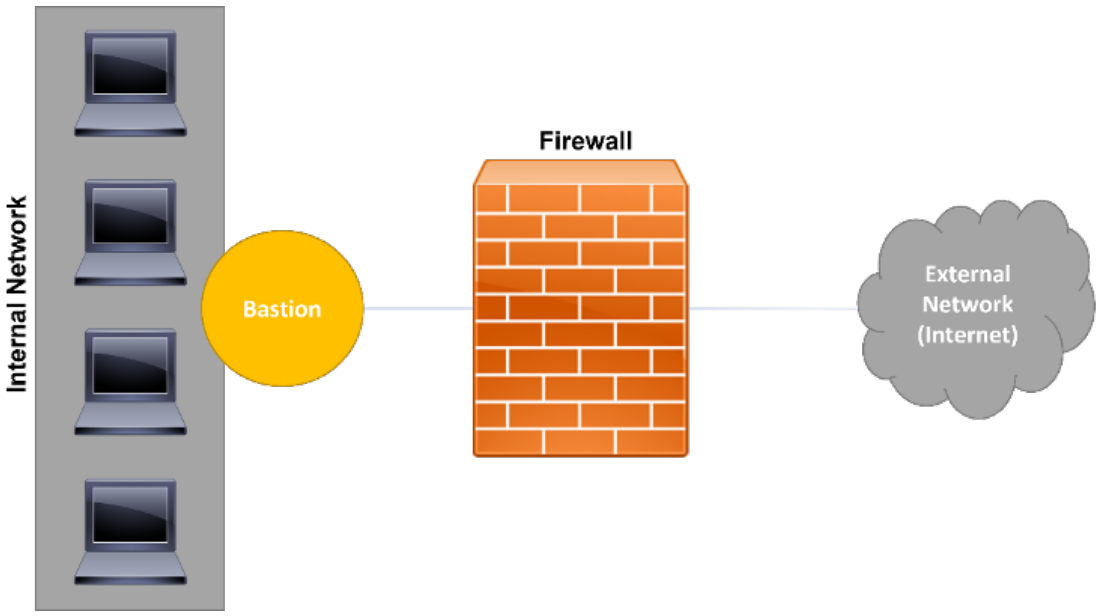
Umieszczane na ogół przy granicy, pomiędzy siecią publiczną a prywatną, zapory sieciowe mogą być jeszcze wykorzystywane do zwiększenia bezpieczeństwa konkretnych segmentów sieci w obrębie sieci. Często można je spotkać nie tylko do oddzielania prywatnych sieci LAN, ale także do oddzielania np. krytycznych systemów od Internetu i sieci korporacyjnych. W oparciu o tę ideę oraz o wiele różnych typów firewalli, istnieją również różne topologie i architektury ich implementacji:

· Host Dual-Homed

W tej architekturze wykorzystywany jest komputer, zwany "dual-homed host", umieszczony pomiędzy siecią wewnętrzną a zewnętrzną, zwykle Internetem. Nazwa nadana temu komputerowi wynika z faktu, że posiada on dwa różne interfejsy sieciowe, po jednym na każdą podłączoną sieć. Podobnie jak w pierwszym sposobie implementacji proxy, również tutaj nie ma innej ścieżki komunikacyjnej, zmuszając cały ruch do przejścia przez hosta i unikając bezpośredniego połączenia między sieciami wewnętrznymi i zewnętrznymi. Główną zaletą tego podejścia jest to, że daje większą kontrolę nad ruchem sieciowym i łatwiejsze zarządzanie. Z drugiej strony, podejście to jest podatne na atak w taki sposób, że jeśli host zostanie zaatakowany, może to spowodować krytyczny problem bezpieczeństwa. Ten typ architektury jest zwykle stosowany w firewallach proxy.

· Ekranowany gospodarz

W architekturze hosta ekranowanego, zamiast jednego hosta umieszczonego pomiędzy siecią wewnętrzną a zewnętrzną, wykorzystywane są dwa różne hosty, gdzie jeden pełni rolę routera do Internetu (screened router), a drugi routera wewnętrznego (bastion host) (rysunek 6).

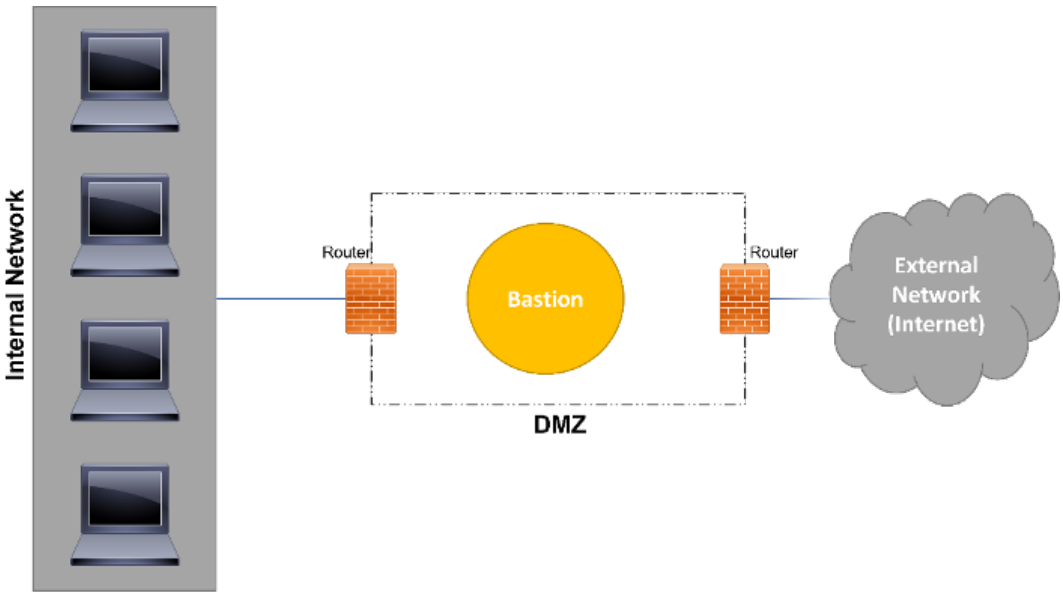


Rysunek 6 - Ekranowa reprezentacja architektury hosta

Skupiając się na hoście bastionowym, nie pozwala on na bezpośrednią komunikację po obu stronach, zmuszając do przepływu informacji w następujący sposób: sieć wewnętrzna - host bastionowy - router ekranujący - sieć zewnętrzna i odwrotnie. W tym przypadku router działa poprzez filtrowanie pakietów, gdzie filtry te są tak zaprojektowane i skonfigurowane, aby przekierować ruch do hosta bastionowego. W konsekwencji, host bastionowy będzie decydował, zgodnie ze swoimi zasadami, czy ruch jest czy nie jest dozwolony, nawet po pierwszej filtracji. Host bastionowy jest krytycznym punktem w sieci i musi być chroniony, aby nie naruszyć bezpieczeństwa całej sieci i systemów.

· Ekranowana podsieć

Ostatnią z trzech architektur jest podsieć ekranowana, która również zawierała hosta bastionowego, podobnie jak poprzednia, jednak w tej architekturze host bastionowy jest umieszczony wewnątrz izolowanego obszaru o nazwie DMZ (Demilitarized Zone). DMZ, jest umieszczona pomiędzy siecią wewnętrzną a zewnętrzną i otoczona routerami filtrującymi pakiety (rysunek 7).



Rysunek 7 - Ekranowa reprezentacja architektury podsieci

Zastosowanie DMZ zwiększa poziom bezpieczeństwa, ponieważ jeśli atakujący jest w stanie przejść przez pierwszą zaporę routera, musi jeszcze poradzić sobie z DMZ, aby uzyskać dostęp do sieci wewnętrznej. DMZ może być również skonfigurowany w różny sposób, włączając w to firewalle, proxy, więcej hostów bastionowych i inne systemy bezpieczeństwa, aby poprawić całe bezpieczeństwo. Wysoki poziom bezpieczeństwa i elastyczność konfiguracji sprawia, że architektura ekranowanej podsieci jest bardziej złożona i kosztowna.

1.5. Przykłady firewalli

Jednym z najczęstszych przykładów firewalli jest ten dostępny w dystrybucjach Linuksa, zwany przez IPTables. Firewall ten, podobnie jak większość firewalli filtrujących pakiety, oparty jest na regułach i listach kontroli dostępu (ACL), które służą do reprezentowania i egzekwowania polityki bezpieczeństwa sieci, którą chcą chronić, monitorować i kontrolować.

W IPTables, te ACL mają szczególną charakterystykę, ponieważ używają wyszukanych elementów i parametrów do budowania reguł w oparciu o kontekst bezpieczeństwa i potrzeby. Oznacza to, że administrator jest w stanie zbudować dowolny typ ACL, zgodnie ze swoimi potrzebami i w zgodzie z prywatnością i bezpieczeństwem zaprojektowanej polityki. W głębszym ujęciu firewall ten opiera się na zaprojektowanej, utworzonej przez trzy różne struktury:

· Zasady

Reguły to w zasadzie polecenia przekazywane do zapory, aby mogła wykonać określoną akcję (zezwolić lub zablokować). Muszą one być zbudowane zgodnie z językiem skonfigurowanym w oprogramowaniu firewall, aby mogło ono je zrozumieć i muszą być zgodne z określonymi wzorcami, aby mogły być prawidłowo zinterpretowane (Rysunek 8). Ogólnie rzecz biorąc, reguły są podobne wśród wielu programów i urządzeń firewall, gdzie główna koncepcja reguły jest przestrzegana przez wszystkie. Nie jest trudno wyeksportować reguły z jednego firewalla do innego, o ile język reguł jest podobny. W IPTables, reguły przechowywane są w łańcuchach i przetwarzane według kolejności. Pierwsza reguła jest pierwszą do sprawdzenia, druga jest drugą do sprawdzenia, i tak dalej aż do końca wszystkich reguł. W tym miejscu ważne jest zaplanowanie kolejności stosowania reguł, ponieważ przy złej kolejności jakaś treść może zostać zablokowana przez poprzednią regułę, podczas gdy w rzeczywistości powinna być dozwolona. Planowanie reguł zapory jest ważnym czynnikiem w administracji sieci, jednak wiele programów zapór pozwala administratorowi na reorganizację reguł po ich skonfigurowaniu i zapisaniu. Skupiając się na konkretnym przypadku IPTables, nowe reguły są przede wszystkim przechowywane w jądrze systemu operacyjnego, co oznacza, że jeśli maszyna zostanie ponownie uruchomiona, cała zawartość reguł zostanie usunięta i utracona. Ze względu na ten czynnik, wszystkie reguły powinny być zapisane w pliku, który będzie ładowany przy każdym starcie maszyny. Prawdą jest, że najczęściej używa się dedykowanych maszyn do pracy tylko jako firewall, gdzie akt ponownego uruchomienia nie jest tak częsty jak w przypadku normalnego komputera osobistego, jednakże często zdarza się, że używany jest duży zestaw reguł, gdzie konieczność konfigurowania ich wszystkich przy każdym ponownym uruchomieniu maszyny powoduje, że jest to bardzo ciężkie zadanie i czasochłonne.

Rysunek 8 - Przykładowa reguła Iptables

· Łańcuchy

Przechowywanie reguł firewalla, łańcuchy pozwalają administratorowi na określenie różnego rodzaju zabiegów, które mają być zastosowane wobec pakietów, niezależnie od tabeli, na której się skupiają. W IPTables można znaleźć dwa różne rodzaje łańcuchów, gdzie pierwszy z nich, nazwany standardowym, zawiera łańcuchy, które są już dostępne w oprogramowaniu i mogą być stosowane do ogólnego ruchu sieciowego. Drugi typ to łańcuchy tworzone przez samego administratora i przeznaczone do realizacji konkretnych potrzeb.

W przypadku standardowych łańcuchów, możliwe jest zidentyfikowanie "Prerouting", składającego się z ruchu przychodzącego do maszyny lokalnej (maszyny firewall), a także zawierającego ruch generowany lokalnie i kierowany do maszyny lokalnej. Innym standardowym łańcuchem jest "Input", który dotyczy całego ruchu, którego miejscem docelowym jest ponownie sama maszyna. Ponadto, łańcuch "Forward" jest związany z ruchem sieciowym, który przechodzi przez maszynę, a "Output" składa się z ruchu generowanego lokalnie, zarówno z lokalnym jak i zdalnym miejscem przeznaczenia. Jest to w zasadzie cały ruch, który wytwarza firewall i który jest wysyłany do sieci lub do samej maszyny. Ostatni łańcuch to "Postrounting" i skupia on ruch wychodzący z maszyny, w tym ruch sieciowy generowany lokalnie i mający również lokalne przeznaczenie).

· Tabele

Reguły są przechowywane w łańcuchach, a co za tym idzie, łańcuchy są przechowywane w tabelach, gdzie każda tabela przechowuje łańcuchy i reguły o tej samej specyfice. Tutaj również występują trzy różne typy tabel: Filter; NAT i Mangle.

"Filter" to tabela odpowiedzialna za filtrowanie wszystkich pakietów, które przechodzą przez firewall, bez względu na ich przeznaczenie.

Tabela ta służy do analizy ruchu sieciowego, zezwalając lub blokując go zgodnie z regułami zapisanymi w tabeli. Kiedy skupiamy się na firewallu, głównym zidentyfikowanym działaniem jest filtracja pakietów, mimo że pozwalają one na inne działania. W tym przypadku, to właśnie tabela "Filter" jest główną odpowiedzialną za takie filtrowanie pakietów.

Tabela "NAT" kontroluje pakiety, które przechodzą przez firewall, ale mają różne miejsca pochodzenia i przeznaczenia. NAT, czyli Network Address Translation, to mechanizm pozwalający na tłumaczenie adresów prywatnych na publiczne i odwrotnie. Tabela ta jest zwykle używana do komunikacji pomiędzy siecią prywatną a publiczną, umożliwiając komputerom w sieci prywatnej dostęp do sieci publicznej poprzez jeden lub więcej publicznych adresów IP.

Ostatni typ tabeli nosi nazwę "Mangle" i pozwala na manipulowanie cechami pakietów, takimi jak typ usługi. Pozwala to na implementację jakości usług, znanej również jako QoS.

Podsumowując, IPTables to firewall filtrujący pakiety, dostępny z dystrybucjami Linuksa i pozwalający na kontrolę i monitorowanie sieci oraz samego komputera. Zapewnia on różne akcje, w tym "akceptuj", "upuść", "odrzuć" i "zaloguj" skonfigurowane w reguły i spersonalizowane łańcuchy. Jak już wspomniano, reguły muszą być skonfigurowane w określonej kolejności i muszą być zaplanowane przed ich wdrożeniem, aby wszystkie działania były zgodne z polityką bezpieczeństwa organizacji.

2. SYSTEMY WYKRYWANIA WŁAMAŃ (IDS)

- Wprowadzenie do systemów wykrywania włamań
- Rodzaje i charakterystyka systemów wykrywania włamań
- Architektury wdrażania systemów wykrywania włamań
- Typowe rozwiązania i przykłady systemów wykrywania włamań

2.1. Wprowadzenie do systemów wykrywania włamań

Ostatnio proponuje się systemy wykrywania włamań, czyli IDS, które mają pomóc administratorom sieci w analizie zagrożeń bezpieczeństwa i wykrywaniu ataków na ich sieci i systemy. Zastosowanie technik inteligencji do wykrywania włamań sprawia, że możliwe jest poradzenie sobie z dużą ilością zgromadzonych danych, takich jak wzorce ruchu, które są trudne do samodzielnej interpretacji przez człowieka.

Big data jest obecnie postrzegana jako rozwiązanie technologiczne do monitorowania infrastruktury, gdzie analiza big data może prowadzić do zoptymalizowanych algorytmów rozwiązywania problemów związanych z siecią i systemami, takich jak problemy bezpieczeństwa, możliwe cyberataki i różne rodzaje modelowania. Zapewniając dogłębny wgląd w infrastrukturę sieciową związaną z kwestiami decyzyjnymi, big data jest realizowana poprzez wdrażanie technologii Internetu rzeczy (IoT) w całym systemie infrastruktury, takich jak sieci czujników, które są w stanie wyczuwać i przekazywać informacje.

Wiele systemów IDS opiera się na regułach eksperckich, które są ręcznie projektowane i tworzone, opisując jedynie znane sygnatury ataków. Chociaż, jeśli chodzi o wykorzystanie uczenia maszynowego opartego na IDS do implementacji w sieciach i systemach komputerowych, można wskazać dane o ruchu sieciowym jako istotny czynnik pozwalający na lepsze doskonalenie IDS-ów, analizowanie zagrożeń bezpieczeństwa i opracowywanie odpowiednich rozwiązań zabezpieczających.

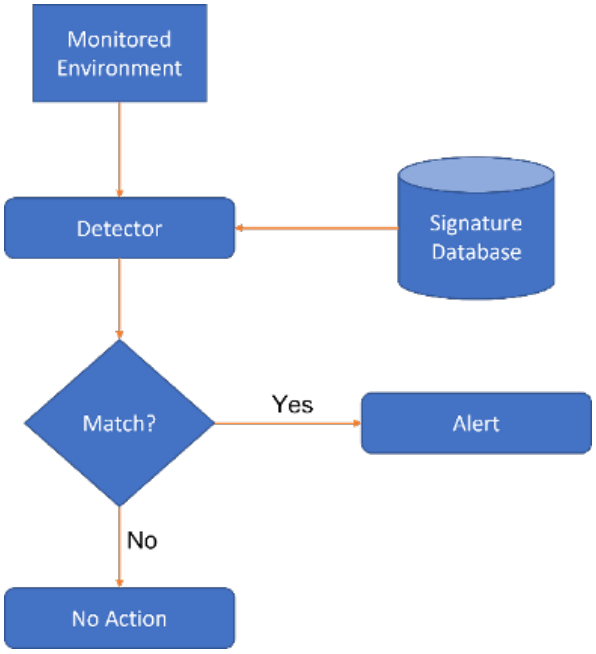
W oparciu o tę ideę, wielu naukowców uznaje systemy IDS za najważniejsze mechanizmy do śledzenia i kontrolowania złośliwych działań w sieci i systemach. Podczas gdy metody oparte na sygnaturach są ważne dla radzenia sobie z dobrze znanymi zagrożeniami, metody oparte na anomaliach są niezbędne do wykrywania i radzenia sobie z nowoczesnymi i nowymi atakami.

Wydajny system wykrywania włamań musi być w stanie zbierać i analizować wszystkie wymieniane pakiety zarówno w komunikacji lokalnej, jak i end-to-end i może być postrzegany jako kamery i czujniki, które stale monitorują dane miejsce. Zwykle składa się z konsoli zarządzającej, służącej do zarządzania i raportowania włamań, oraz z czujników, które pracują jako agenci, monitorując urządzenia sieciowe w czasie rzeczywistym.

2.2. Rodzaje i charakterystyka systemów wykrywania włamań

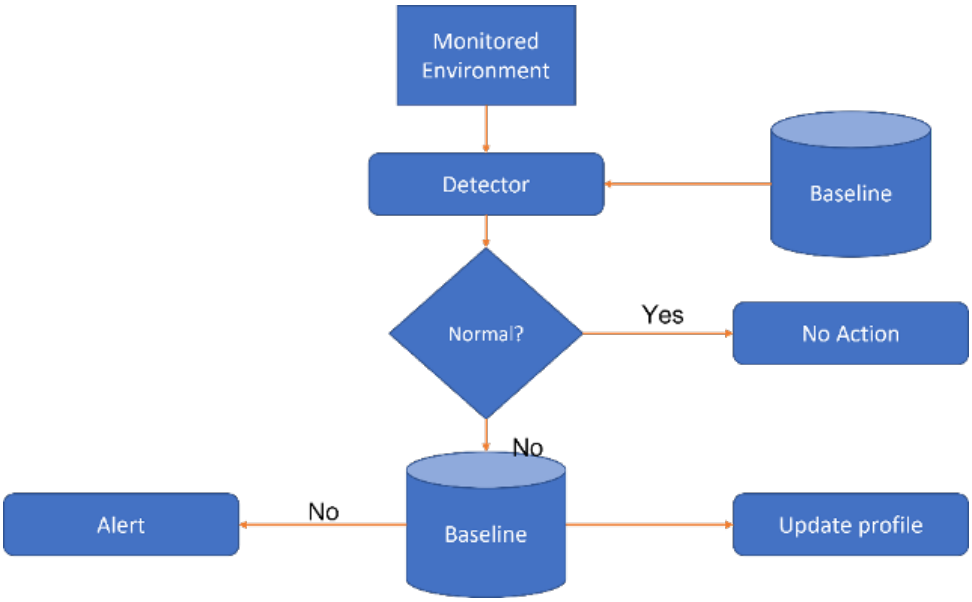
Historycznie rzecz biorąc, istnieją różne rodzaje systemów wykrywania włamań, klasyfikowane według ich charakteru i sposobu działania. Według różnych uczonych, można je podzielić na dwie główne kategorie: Signature-Based i Anomaly-Based:

· Podejścia oparte na sygnaturach są projektowane w oparciu o znane wzorce ataków i są wykorzystywane jako zestawy reguł, takie jak te używane przez Snort IDS. Ruch przychodzący jest następnie porównywany z tymi regułami, aby zidentyfikować ruch nieprawidłowy wśród normalnego (Rysunek 9).



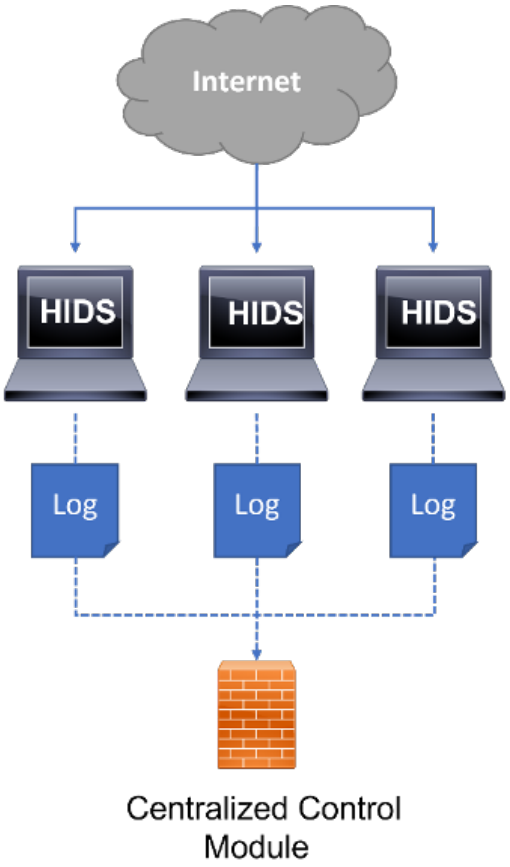
Rysunek 9 - Schemat systemu IDS opartego na sygnaturach

· W przeciwieństwie do poprzedniej kategorii, metody Anomaly-Based opierają się na idei normalnych profili behawioralnych, oznaczając podczas wykrywania włamań profile odbiegające od normy. Tego typu podejście często zwraca wysoki wskaźnik fałszywych alarmów, przy wykrywaniu nowych ataków (Rysunek 10).



Rysunek 10 - Schemat działania systemu IDS opartego na anomaliach

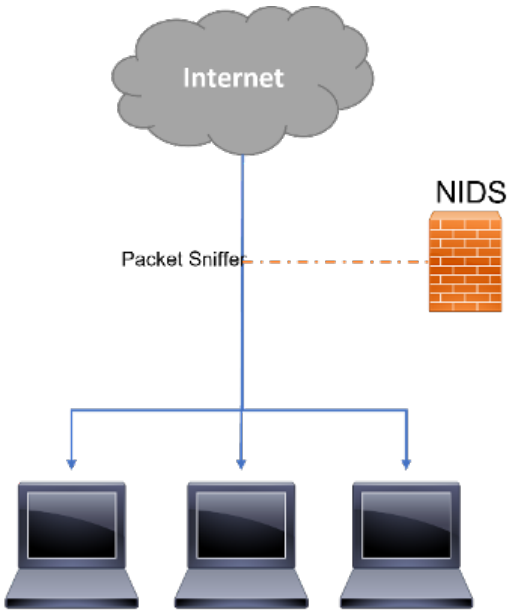
Często spotyka się również systemy IDS podzielone na kategorie Host-Based (HIDS) (Rysunek 11) i Network-Based (NIDS) (Rysunek 12). Porównując, system Host-Based IDS przyjmuje na siebie odpowiedzialność za monitorowanie zachowania pojedynczego hosta, podczas gdy system Network-Based IDS zbiera dowody poprzez dane o ruchu sieciowym. Niektórzy twórcy uważają połączenie tych dwóch kategorii IDS za najlepszy sposób ochrony sieci komputerowych przed cyberatakami, jednak są one jeszcze zbyt niedojrzałe, aby mogły być powszechnie stosowane. Można również zidentyfikować słaby punkt HIDS, który należy poprawić, gdy może on nie wykryć poprawnie włamania w przypadku, gdy host jest skompromitowany.



Rysunek 11 - Schemat działania systemu IDS opartego na hoście

W konwencjonalnych systemach IDS całkowicie akceptowany jest paradygmat odmawiania dostępu złośliwym pakietom poprzez ich upuszczanie lub ich root.

Jak w każdym innym mechanizmie zabezpieczeń komputerowych, również w systemach wykrywania włamań istnieją pewne zalety i wady, które należy wziąć pod uwagę przed ich instalacją i konfiguracją. Należy podkreślić, że tradycyjne IDS mogą nie być odpowiednie dla wszystkich systemów i sieci komputerowych. Dobrym przykładem jest tu infrastruktura krytyczna, taka jak system dystrybucji wody. Pracując 24 godziny na dobę i dostarczając wodę pitną do dużych miast i kraju, IDS musi być starannie dobrany i wdrożony, ponieważ może spowodować zakłócenia w komunikacji, a w konsekwencji zagrozić życiu ludzkiemu. W tym miejscu należy zwrócić uwagę na istniejące słabości i specyficzne cechy takich krytycznych systemów, które muszą być brane pod uwagę. Przykładowo, główne komponenty systemu SCADA, takie jak sterowniki PLC i RTU, mają zazwyczaj niskie zdolności obliczeniowe i pamięciowe, co sprawia, że nie są odpowiednie do przydzielenia HIDS, który musi być zainstalowany na samym hoście, aby mógł być analizowany. Z drugiej strony, czujniki NIDS mogą być zainstalowane w oddzielnej maszynie podłączonej do sieci, która ma być monitorowana. Takie podejście może być łatwo zintegrowane z systemem SCADA, gdzie konieczne jest zrozumienie i analiza protokołów komunikacyjnych. Jednak w obecnych implementacjach protokoły komunikacyjne SCADA, które początkowo zostały zaprojektowane do pracy w komunikacji szeregowej, są osadzone w payloadach pakietów TCP.



Rysunek 12 - Schemat działania sieciowego systemu IDS

W głębszym ujęciu, podejścia oparte na sygnaturach są projektowane w oparciu o znane wzorce ataków, które są wykorzystywane jako zestawy reguł. Ruch przychodzący jest następnie porównywany z tymi regułami, aby zidentyfikować ruch nieprawidłowy wśród normalnego. W przeciwieństwie do poprzedniej kategorii, Anomaly-Based często zwraca wysoki wskaźnik fałszywych alarmów, gdy zachowanie systemu nie jest odpowiednio skonfigurowane w systemie IDS. W szczególnym przypadku systemu krytycznego, ze względu na jego wrażliwą naturę, normalne zachowanie i konfiguracja systemu jest zawsze głęboko udokumentowana i aktualizowana.

Oprócz poprzednich klasyfikacji, często spotyka się również systemy IDS skategoryzowane jako Host-Based (HIDS) i Network-Based (NIDS). Porównując, system Host-Based IDS bierze na siebie odpowiedzialność za monitorowanie zachowania pojedynczego hosta, podczas gdy system Network-Based IDS zbiera dowody poprzez analizę danych o ruchu sieciowym. Wielu naukowców uważa, że połączenie tych dwóch kategorii IDS jest najlepszym sposobem ochrony systemów dystrybucji wody przed cyberatakami, jednak są one jeszcze zbyt niedojrzałe, aby mogły być powszechnie stosowane.

Również w tych klasyfikacjach można zidentyfikować słaby punkt HIDS, który należy poprawić, gdy może on nie wykryć poprawnie włamania w przypadku kompromitacji hosta. Co więcej, HIDS powinien być zainstalowany na samym hoście lub korzystać z agenta, co samo w sobie nie jest do końca praktyczne w krytycznym środowisku sieciowym, gdyż wiele z jego urządzeń ma niską moc obliczeniową i energetyczną. Co więcej, HIDS zwiększa również ilość ruchu w sieci, obciążając ją pakietami informacyjnymi IDS, co po raz kolejny może przysporzyć systemowi więcej problemów niż pomocy.

W konwencjonalnych systemach IDS całkowicie akceptowany jest paradygmat odmawiania dostępu złośliwym pakietom, poprzez ich upuszczanie lub ich rootowanie. Jednak ze względu na ich krytyczny charakter, taki paradygmat nie jest akceptowalny w sieciach systemów dystrybucji wody. Krytyczne systemy wymagają regularnej i ciągłej komunikacji pomiędzy urządzeniami i kontrolerami, gdzie niedostępny root lub pakiet może zagrozić całemu systemowi, powodując katastrofalne skutki.

2.3. Architektury wdrażania systemów wykrywania włamań

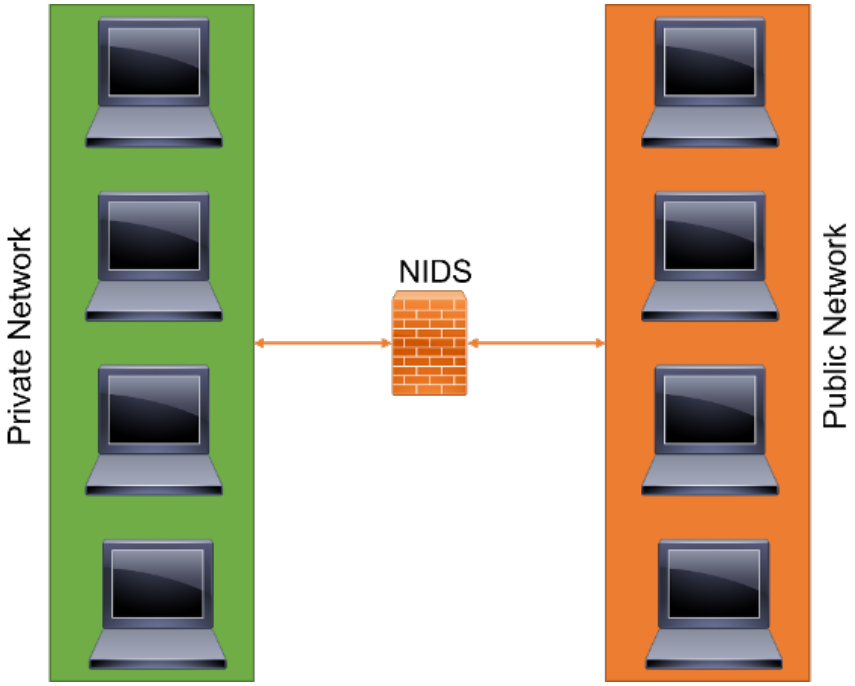
Biorąc pod uwagę różne istniejące typy IDS-ów, również ich implementacja może się różnić w zależności od systemu i sieci. Wiadomo, że IDS oparty na sygnaturach skupia się na sygnaturach znanych ataków i podatności, korzystając z dużej bazy danych, aby skompilować swoje reguły i wykryć włamanie. Jednak taka implementacja może nie być odpowiednia dla sieci, którą administrujemy. Tutaj pierwszym krokiem jest zrozumienie potrzeb ochrony sieci i systemów, określenie ich głównych priorytetów i celów.

Z drugiej strony, system IDS oparty na anomaliach wykorzystuje normalny stan pracy sieci i systemów, aby odpowiednio zidentyfikować nienormalne zachowania i stwierdzić, czy są one rzeczywiście spowodowane włamaniem, czy też są to normalne zachowania sieci. Ponownie potrzebny jest wcześniejszy plan, w którym system i sieć muszą być udokumentowane i skonfigurowane w systemie IDS, aby mógł on rozpoznać wzorce zachowań.

Powszechnie, obecnie, spotyka się również IDS-y pracujące w oparciu o uczenie maszynowe. Tutaj po raz kolejny konieczne jest zebranie informacji o normalnym funkcjonowaniu sieci i jej systemów, dzięki czemu możliwe jest nauczenie maszyny o prawidłowych i normalnych stanach pracy, przed jej ostatecznym użyciem.

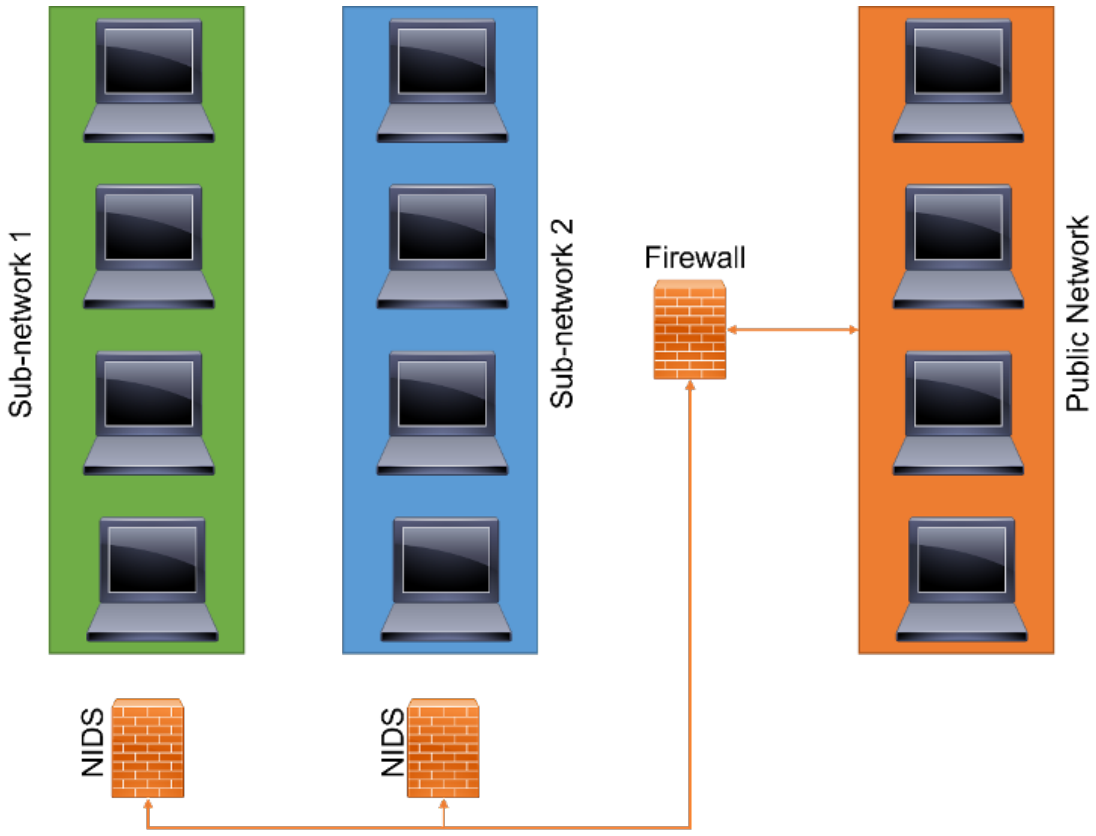
Podobnie jak implementacja firewalla, również implementacja IDS może być różna i może być zawarta na granicy lub wewnątrz sieci.

Najczęstszym wdrożeniem systemu IDS jest umieszczenie go na granicy sieci prywatnej i publicznej. Ponieważ jest to jeden z głównych punktów krytycznych sieci, jego monitorowanie i analiza jest kluczowa dla utrzymania dobrego poziomu bezpieczeństwa i zapobiegania nieautoryzowanemu dostępowi do sieci wewnętrznej i systemów (Rysunek 13). Umieszczając IDS w tym miejscu, cały ruch przychodzący i wychodzący jest monitorowany i kontrolowany, jednak wymaga to również większej mocy obliczeniowej i zdolności do radzenia sobie z dużą ilością ruchu. Ponieważ system kontroluje dostęp do sieci publicznej, niska wydajność systemu IDS będzie skutkować również niską wydajnością komunikacji z sieciami zewnętrznymi, zwykle z Internetem.



Rysunek 13 - Instalacja systemu IDS pomiędzy siecią wewnętrzną a zewnętrzną

Można również spotkać różne systemy IDS wdrożone na granicy segmentów sieci lub sieci LAN, monitorujące i analizujące ruch pomiędzy nimi. Taka implementacja jest zwykle spotykana w przypadku połączeń między sieciami korporacyjnymi i krytycznymi systemami, gdzie każdy segment może mieć swój dedykowany i specyficzny serwer IDS (rysunek 14).



Rysunek 14 - Instalacja systemu IDS na granicy segmentów sieci LAN

Podchodząc do IDS opartego na hostach, skupia się on na ochronie pojedynczego hosta. Ten typ architektury implementacji jest odpowiedni do ochrony konkretnych serwerów lub komputerów, które są łatwym celem ataków. Będąc host-based, instalacja agenta IDS odbywa się na samym serwerze lub komputerze, gdzie istnieje potrzeba, aby posiadał on dobrą moc obliczeniową i pamięciową. Taka architektura nie jest odpowiednia dla wszystkich urządzeń, ponieważ nie wszystkie są w stanie poradzić sobie z analizą dużego ruchu sieciowego i powinna być wdrażana tylko dla pojedynczych serwerów i krytycznych komputerów. Ponadto, zastosowanie architektury host-based wymaga istnienia dedykowanego serwera IDS, który komunikuje się z każdym z istniejących agentów IDS. W zależności od liczby monitorowanych hostów wzrośnie również ilość danych o ruchu sieciowym, co może spowodować zalanie sieci komunikacją IDS, obniżając jej wydajność.

Implementacja sieciowego systemu IDS przynosi bardziej efektywną analizę i monitoring, gdy sieć obejmuje większą liczbę hostów oraz gdy skupiamy się na infrastrukturze krytycznej z urządzeniami o mniejszej mocy obliczeniowej. Na podstawie samej analizy ruchu sieciowego, architektura sieciowa nie wymaga stosowania agentów IDS zaimplementowanych na hostach, a co za tym idzie, nie jest również generowany ruch komunikacyjny IDS w sieci. Ten typ architektury wykorzystuje jeden lub więcej dedykowanych serwerów, zainstalowanych wewnątrz sieci, które zbierają i analizują dane o ruchu sieciowym, identyfikując jego nieprawidłowe zachowanie lub nieprawidłowe wzorce na ruchu w celu wykrycia włamania ze strony nieautoryzowanych agentów.

Chociaż istnieją trzy główne architektury implementacji IDS, większość naukowców i badaczy w tej dziedzinie twierdzi, że najlepsze rozwiązanie IDS polega na połączeniu trzech poprzednich architektur. Wykorzystanie różnych typów i architektur implementacji przynosi wyższy współczynnik wykrywalności włamań, a w konsekwencji wyższy poziom bezpieczeństwa.

Ponadto połączenie HIDS i NIDS umożliwia monitorowanie całej sieci, ze szczególnym uwzględnieniem krytycznych serwerów lub komputerów, które przechowują lub dostarczają ważne dane i usługi użytkownikom sieci.

2.4. Typowe rozwiązania i przykłady systemów wykrywania włamań

Obecnie dostępnych jest wiele rozwiązań do wykrywania włamań, niektóre z nich są płatne, a niektóre darmowe. Również wiele rozwiązań zintegrowanych, przynosi już mechanizm wykrywania włamań w ramach swojego oprogramowania, jednak są one ograniczone do miejsca jego implementacji.

W zależności od rodzaju wdrażanego systemu IDS istnieją również różne rozwiązania, które można zastosować. W tym miejscu można wyróżnić powszechnie znane SNORT IDS oraz Suricata IDS.

Skupiając się na pierwszym z nich, SNORT, jest to płatne rozwiązanie open-source, które może być zainstalowane nie tylko przez pojedynczych użytkowników, ale także przez firmy i organizacje. Ten IDS jest skoncentrowany na zestawie reguł określających, jaki ruch sieciowy powinien być zbierany i co należy zrobić z wykrytymi złośliwymi pakietami. Działa on w oparciu o znane sygnatury podatności i ataków, aby zbudować swoją bazę reguł IDS i zidentyfikować możliwe włamania do sieci.

Wśród jego funkcji można podkreślić analizę i monitorowanie w czasie rzeczywistym, gdzie administrator sieci ma możliwość sprawdzenia wszystkich wyników monitorowania IDS w czasie rzeczywistym, identyfikując detekcje włamań i działając zgodnie z potrzebami. Dodatkowo zawiera analizę protokołów dla lepszej wydajności identyfikacji. Analizuje protokoły poprzez proces sniffingu, który przechwytuje dane w warstwach protokołu, umożliwiając administratorom dalsze badanie potencjalnie złośliwych pakietów. Ponadto SNORT gromadzi reguły według protokołów, takich jak IP i TCP, następnie według portów, a następnie według tych z zawartością lub bez. Reguły z zawartością wykorzystują multi-pattern matcher, który zwiększa wydajność, szczególnie w przypadku protokołów takich jak HTTP (Hypertext Transfer Protocol). Reguły bez zawartości są zawsze analizowane, co zmniejsza wydajność.

SNORT jest systemem IDS zdolnym do inspekcji i monitorowania nie tylko nagłówka pakietu, ale także jego ładunku, co pozwala na zmniejszenie współczynnika fałszywych pozytywnych detekcji. Jest również w stanie dostarczać alerty oraz elastyczne logi pakietów i analiz, dostarczając wszelkich informacji administratorom sieci do właściwej analizy i działania. Jego instalacja może odbywać się w systemach Unix, Windows i MacOSx, o ile pozwalają one na kompilację i instalację biblioteki lipcap, wykorzystywanej jako baza do analizy pakietów. SNORT posiada również elastyczną architekturę, pozwalającą na różne sposoby instalacji i dostosowanie do potrzeb sieci.

Podobnie jak poprzedni, również Suricata IDS to open-source'owy silnik wykrywania zagrożeń sieciowych, który jest darmowy i zapewnia różne możliwości, w tym wykrywanie włamań i monitorowanie bezpieczeństwa sieci, poprzez głęboką inspekcję pakietów i dopasowywanie wzorców.

Główną cechą wyróżniającą Suricatę w porównaniu do SNORT jest to, że Suricata zawiera dynamiczną ochronę protokołów, która jest niezależna od portów. Dzięki temu IDS może identyfikować niektóre z najbardziej popularnych protokołów warstwy aplikacji, w tym HTTP, DNS (Domain Name System), TLS (Transport Layer Security), między innymi, gdy te komunikują się przez niestandardowe porty. Zastosowany tutaj język reguł pozwala administratorowi na budowanie warunków dopasowania w protokole warstwy aplikacji, zwiększając wydajność i wykrywalność IDS.

Suricata monitoruje ruch sieciowy, korzystając z rozbudowanej bazy reguł, podobnie jak SNORT, i opiera swoje reguły również na znanych sygnaturach podatności i ataków. Chociaż Suricata została zbudowana w innej architekturze i jest znacznie nowsza niż SNORT, oba rozwiązania mogą korzystać z sygnatur zagrożeń. Kluczową różnicą jest fakt, że Suricata posiada wielowątkową architekturę, pozwalającą na wykorzystanie wielu rdzeni CPU jednocześnie, co w konsekwencji przekłada się na większą wydajność w porównaniu z innymi rozwiązaniami. Wykorzystanie wielu CPU umożliwia Suricata przetwarzanie wielu zdarzeń w tym samym czasie, bez konieczności przerywania innych żądań lub narażania innych analiz, obciążając równowagę pomiędzy CPU i poprawiając wydajność w analizie ruchu sieciowego.

To rozwiązanie IDS może być używane w trzech różnych rolach, gdzie najprostszą z nich jest skonfigurowanie go jako host-based IDS, monitorując ruch pojedynczego komputera. Można go również zaimplementować jako pasywny IDS, monitorujący cały ruch przechodzący przez sieć i powiadamiający administratora sieci, gdy natrafi na coś złośliwego. Trzecia i ostatnia rola to taka, w której Suricata jest wdrożona jako aktywny inline IDS i IPS (Intrusion Protection System), monitorujący ruch przychodzący i wychodzący, umożliwiający blokowanie złośliwego ruchu jeszcze przed jego wejściem do sieci, jednocześnie alarmując o tym administrację sieci.

Podobnie jak SNORT, Suricata jest dostępna również dla systemów UNIX, Windows i MacOSx.

Jak wspomniano wcześniej, nie wszystkie rozwiązania IDS są odpowiednie dla każdego systemu lub sieci, gdzie administrator sieci musi wybrać najlepsze rozwiązanie, aby dopasować swoje potrzeby sieciowe i pojedyncze cechy.

Poprzednie przykłady nadają się w większości do implementacji w zwykłej sieci komputerowej, będąc jednocześnie najczęstszymi rozwiązaniami stosowanymi obecnie przez organizacje i firmy. Jednakże, gdy w centrum uwagi znajduje się wykrywanie włamań w infrastrukturach krytycznych, które opierają swoją funkcję na konkretnych protokołach sieciowych i gdzie proste przerwanie komunikacji może spowodować drastyczne skutki, systemy IDS muszą być starannie dobrane i wdrożone.

Niektórzy uczeni twierdzą, że dedykowane rozwiązanie jest koniecznością, a State-Based wraz z machine learning IDSs mogą być przyszłością dla ochrony infrastruktury krytycznej. Dobrym przykładem jest rozwiązanie opracowane przez (Al-Malawi et al., 2016) które skupia się na technice grupowania danych w celu wyodrębnienia reguł opartych na stanie i wykrycia ataków w sieciach Modbus/TCP, bez wcześniejszej znajomości specyfikacji systemów. Należy jednak podkreślić, że wrażliwe i krytyczne systemy, takie jak SCADA w WDS (water distribution systems), zawsze posiadają w pełni szczegółową dokumentację.

3. SYSTEMY ZAPOBIEGANIA WŁAMANIOM (IPS)

- Wprowadzenie do systemów zapobiegania włamaniom
- Rodzaje i charakterystyka systemów ochrony przed włamaniami
- Architektury wdrażania systemów zapobiegania włamaniom

3.1. Wprowadzenie do systemów zapobiegania włamaniom

System zapobiegania włamaniom (ang. intrusion prevention system, IPS) to narzędzie bezpieczeństwa sieciowego, które w sposób ciągły monitoruje sieć pod kątem złośliwej aktywności i podejmuje działania mające na celu jej zapobieżenie, m.in. zgłasza blokowanie lub porzucanie jej, gdy już wystąpi. Jego nazwa może być podobna do poprzednio opisanego tematu (systemy wykrywania włamań), jednak poprzedni mechanizm skupia się jedynie na identyfikacji, nie stosując żadnych działań, a co za tym idzie, nie zapobiegając wystąpieniu ataku.

Ponadto, IPS jest bardziej zaawansowanym systemem niż IDS i często stanowi część firewalla nowej generacji lub rozwiązania typu unified threat management. Często spotykamy się również z tym, że IPS współpracuje z serwerem IDS, tak jak poprzednie rozwiązania (SNORT i Suricata).

Podobnie jak inne systemy zabezpieczeń, IPS można znaleźć zarówno w formie oprogramowania, jak i sprzętu, gdzie oprogramowanie może być zainstalowane w dowolnym komputerze i umieszczone w sieci w celu ochrony, zawsze biorąc pod uwagę wymagania sprzętowe maszyny. Ponadto, jak wiele innych technologii bezpieczeństwa sieciowego, IPS musi być wystarczająco silny, aby poradzić sobie z dużą ilością danych o ruchu sieciowym, bez spowalniania wydajności sieci.

System zapobiegania włamaniom jest często umieszczany w linii, w strumieniu ruchu sieciowego, pomiędzy źródłem a miejscem przeznaczenia. Podobnie jak IDS, IPS jest zwykle umieszczany pomiędzy sieciami prywatnymi i publicznymi, dzięki czemu może analizować i monitorować wszystkie transakcje komunikacji sieciowej pomiędzy tymi dwiema sieciami i prawidłowo zapobiegać atakom i innym naruszeniom bezpieczeństwa w sieci prywatnej. Jeśli jest umieszczony pomiędzy dwoma sieciami, to zazwyczaj znajduje się za zaporą ogniową.

Sam serwer IPS nie jest w stanie całkowicie zabezpieczyć sieci, niejednokrotnie współpracuje z innymi narzędziami i rozwiązaniami bezpieczeństwa, identyfikując zagrożenia, których tamte nie są w stanie zidentyfikować.

Ponadto, ponieważ serwer IPS filtruje złośliwy ruch, zanim dotrze on do innych urządzeń zabezpieczających i kontroli, zmniejsza obciążenie tych kontroli i pozwala im działać bardziej efektywnie. Ponieważ IPS jest w dużej mierze zautomatyzowany, wymaga mniejszego nakładu czasu od zespołów IT, spełniając wiele wymogów zgodności określonych przez PCI DSS, HIPAA i inne. Ponadto, system IPS dostarcza również cennych danych z audytu, które mogą być wykorzystane do dalszej analizy i wskazówek dotyczących włamania lub ataku. Takie dane są ważne w taki sposób, że mogą dać cały obraz incydentu i pomóc w identyfikacji źródła włamania i jak w przyszłości zapobiec ponownemu wystąpieniu.

Podobnie jak większość innych systemów i narzędzi bezpieczeństwa, również IPS-y mogą być dostosowywane do potrzeb i zawierać spersonalizowane polityki, aby odpowiedzieć na konkretne potrzeby organizacji i chronionej przez nią sieci.

Zapobiegając nie tylko włamaniom, rozwiązania IPS są również bardzo skuteczne w wykrywaniu i zapobieganiu wykorzystywaniu luk w zabezpieczeniach. Po wykryciu luki w zabezpieczeniach, zazwyczaj istnieje pewien okres czasu, w którym podmioty odpowiedzialne za zagrożenia mają możliwość jej wykorzystania, zanim dostępna będzie łata bezpieczeństwa umożliwiająca jej usunięcie. System zapobiegania włamaniom jest tutaj wykorzystywany do szybkiego blokowania tego typu ataków i ochrony sieci w czasie, gdy łata nie jest dostępna.

Urządzenia IPS zostały pierwotnie zbudowane i wydane jako samodzielne urządzenia, w połowie lat 2000. Funkcjonalność ta została jednak zintegrowana z narzędziami do zunifikowanego zarządzania zagrożeniami oraz innymi narzędziami i usługami bezpieczeństwa dla małych i średnich firm, a także z zaporami nowej generacji na poziomie przedsiębiorstwa.

Nowsze rozwiązania IPS są obecnie połączone z usługami obliczeniowymi i sieciowymi w chmurze, które umożliwiają im zapewnienie bardziej wyrafinowanego podejścia do ochrony przed stale rosnącymi zagrożeniami cyberbezpieczeństwa, przed którymi stoją lokalne i globalne organizacje na całym świecie.

W przeciwieństwie do systemów IDS, które działają w sposób pasywny, jedynie wykrywając i ostrzegając o możliwych włamaniach i zagrożeniach, IPS jest umieszczony w linii, sprawdzając cały przychodzący i wychodzący ruch sieciowy, pomiędzy sieciami prywatnymi i publicznymi, siedząc tuż za zaporą ogniową lub będąc jej częścią. To rozwiązanie IPS aktywnie analizuje i podejmuje automatyczne działania na wszystkich strumieniach ruchu, które wchodzą do sieci:

- Wysyłanie alarmu do administratora (podobnie jak w systemach IDS).
- Zrzucanie złośliwych pakietów.
- Blokowanie ruchu z adresu źródłowego.
- Resetowanie połączenia.
- Konfiguracja zapór ogniowych w celu zapobiegania przyszłym atakom.

Jako narzędzie bezpieczeństwa inline, IPS musi działać wydajnie, aby nie pogorszyć wydajności i efektywności sieci, gdzie musi być wystarczająco wydajny, aby odpowiednio zabezpieczyć sieć, zachowując jej normalne funkcje. Musi również pracować w trybie szybkim, ponieważ exploity mogą zdarzać się w czasie zbliżonym do rzeczywistego, a także być w stanie wykryć i zareagować dokładnie, eliminując zagrożenia i redukując fałszywe alarmy pozytywne. Aby to zrobić, istnieje kilka technik i podejść stosowanych do wyszukiwania exploitów i ochrony sieci przed nieautoryzowanym dostępem.

3.2. Rodzaje i charakterystyka systemów ochrony przed włamaniami

Istnieją różne rodzaje systemów ochrony przed włamaniami, o różnych cechach i właściwościach, podobnie jak można było to zrozumieć w przypadku systemów wykrywania włamań. Podobnie jak IDS-y, IPS-y można również sklasyfikować jako oparte na sygnaturach, anomaliach i polityce. Tutaj systemy ochrony przed włamaniami oparte na sygnaturach wykorzystują podejście oparte na znanych podatnościach i sygnaturach ataków, gdzie metodą jest dopasowanie aktywności do tych sygnatur i podniesienie lub nie alarmu i działania w razie potrzeby. Jedną z wad tej metody jest to, że jest w stanie zatrzymać tylko wcześniej zidentyfikowane ataki i nie będzie w stanie rozpoznać nowych. Ten typ IPS nie biorą pod uwagę żadnych nieznanych podatności i nie będzie umieścić żadnych działań do sieci, jeśli nowy atak występuje.

Ten typ IPS wykorzystuje słownik unikalnie identyfikowalnych wzorców, czyli sygnatur, w kodzie każdego exploita. Gdy exploit zostaje odkryty, jego sygnatura jest zapisywana i przechowywana w stale rosnącym słowniku sygnatur. Wykrywanie sygnatur dla IPS dzieli się na dwa podtypy:

· **Sygnatury ukierunkowane na exploity** - identyfikują poszczególne exploity poprzez wyzwalanie na podstawie unikalnych wzorców danej próby wykorzystania. System IPS może zidentyfikować konkretne exploity, znajdując w strumieniu ruchu dopasowanie do sygnatury ukierunkowanej na exploity.

· **Sygnatury ukierunkowane na podatność** - wykorzystanie szerszych sygnatur, które celują w podstawową podatność w systemie, który jest celem ataku. Sygnatury te pozwalają chronić sieci przed wariantami exploita, które mogły nie zostać bezpośrednio zaobserwowane w środowisku naturalnym, ale również zwiększają ryzyko wystąpienia fałszywych pozytywów.

W przeciwieństwie do poprzedniego, wdrożenie IPS opartego na anomaliach skupia się na monitorowaniu nieprawidłowych zachowań poprzez porównywanie losowych próbek ruchu sieciowego i aktywności z wzorcem bazowym. Nie koncentruje analizy na sygnaturach, lecz na zachowaniu całej sieci, identyfikując nieprawidłowe wzorce i sekwencje ruchu, aby podnieść alarm i zastosować odpowiednie działania. W porównaniu z poprzednim typem, ten jest bardziej solidny, ponieważ nie skupia się tylko na znanych podatnościach, ale także na możliwych nowych. Mimo, że jest bardziej wytrzymały, może również generować wyższy wskaźnik fałszywych wyników pozytywnych, jeśli nie zostanie odpowiednio skonfigurowany i dostosowany do polityki bezpieczeństwa. Niektóre nowsze i bardziej zaawansowane systemy ochrony przed włamaniami wykorzystują sztuczną inteligencję i technologie uczenia maszynowego do wspierania monitorowania opartego na anomaliach, jednak konieczne jest wykorzystanie zbiorów danych dotyczących normalnych zachowań, aby odpowiednio wytrenować maszynę, co w przypadku systemów krytycznych nie zawsze jest łatwym zadaniem.

Systemy IPS oparte na anomaliach pobierają próbki losowego ruchu sieciowego i porównują je z obliczonym wcześniej poziomem wydajności bazowej. Gdy próbka aktywności ruchu sieciowego znajduje się poza wybranymi parametrami lub progami wydajności bazowej, IPS podejmuje działania w celu poradzenia sobie z sytuacją.

Trzeci typ, policy-based intrusion protection system, jest mniej popularny spośród tych trzech i wykorzystuje polityki bezpieczeństwa zdefiniowane przez przedsiębiorstwo, blokując działania, które naruszają te polityki. Ten typ IPS wymaga całkowitej konfiguracji polityk bezpieczeństwa, a co za tym idzie, mocnego planowania i projektowania, jak również częstej aktualizacji i administracji.

Niektórzy uczeni, podobnie jak ma to miejsce w przypadku IDS-ów, również klasyfikują system IPS na cztery kolejne typy, zgodnie z ich naturą: network intrusion prevention system (NIPS); host intrusion prevention system (HIPS); network behaviour analysis (NBA) oraz wireless intrusion prevention system (WIPS).

Pierwsze dwa typy są znów podobne do systemów wykrywania włamań, gdzie instalowane są na poziomie sieci lub hostów. NIPS są instalowane na poziomie sieci i tylko w strategicznych punktach, aby monitorować całą sieć, lub podsieć. Proaktywnie monitoruje ruch sieciowy i skanuje w poszukiwaniu zagrożeń. HIPS instalowany jest na poziomie punktu końcowego, takiego jak komputer czy serwer i skupia się na analizie ruchu przychodzącego i wychodzącego tej konkretnej maszyny. W tym miejscu należy wziąć pod uwagę, że im większa liczba HIPS w sieci, tym większy będzie tworzony ruch IPS, a co za tym idzie, większe będzie obciążenie sieci. HIPS działa lepiej w połączeniu z NIPS, ponieważ służy jako ostatnia linia obrony dla zagrożeń, które ominęły NIPS.

Jeśli chodzi o analizę zachowania sieci, czyli NBA, to działa ona na zasadzie analizy ruchu sieciowego w celu wykrycia nietypowych przepływów ruchu, takich jak na przykład ataki DDoS (Distributed Denial of Service).

Ostatni typ IPS, WIPS, jest przeznaczony specjalnie do sieci bezprzewodowych, skanując je w poszukiwaniu nieautoryzowanych dostępów i wyrzucając z sieci nieautoryzowane urządzenia.

3.3. Architektury wdrażania systemów zapobiegania włamaniom

Aby chronić się przed stale rosnącą liczbą wyrafinowanych zagrożeń unikowych, systemy ochrony przed włamaniami powinny wdrażać uczenie głębokie (inline deep learning), które znacznie zwiększa wykrywalność i precyzyjnie identyfikuje złośliwy ruch, który nie był wcześniej widziany, bez opierania się na znanych podatnościach i sygnaturach ataków. Podobnie do sposobu działania sieci neuronowych, czyli tak jak wykorzystuje to ludzki mózg, modele głębokiego uczenia przechodzą przez kilka warstw analizy i przetwarzają miliony punktów danych w ciągu milisekund. Każda decyzja musi być wykonana w naprawdę szybki sposób, aby nie zagrozić wydajności i efektywności sieci. Te wyrafinowane systemy rozpoznawania wzorców analizują aktywność ruchu sieciowego z nieporównywalną dokładnością, identyfikując nowy złośliwy ruch, który nigdy wcześniej nie został zidentyfikowany, zgodnie z wyjątkowo niskim wskaźnikiem fałszywych wyników.

Ta dodatkowa warstwa inteligentnej ochrony, którą może zastosować narzędzie IPS, zapewnia dalszą ochronę wrażliwych informacji przedsiębiorstwa oraz zapobiega wyrafinowanym atakom i podatnościom, które mogą spowodować duże szkody w sieci, a w konsekwencji w organizacji lub firmie.

Jednym z głównych problemów dotyczących nie tylko systemów IDS, ale także wśród narzędzi IPS, jest związany z odsetkiem fałszywych pozytywów, które mogą być przez nie generowane. Każdy alarm wymaga uwagi administratora lub zespołu informatycznego, co powoduje, że jest czasochłonny i wymaga głębokiej analizy, aby upewnić się, że alarm był prawdziwie pozytywny. Takiego samego wysiłku wymagają alarmy fałszywie pozytywne, które jeśli nie są prawdziwe, mają negatywny wpływ na zespół i powodują stratę czasu i pracy.

Podobnie jak w przypadku systemu IDS, również w IPS ważne jest zrozumienie potrzeb bezpieczeństwa sieci i organizacji, zaplanowanie wdrożenia z wyprzedzeniem i upewnienie się, że wszystkie polityki bezpieczeństwa są przestrzegane. Ponadto, w przypadku IPS istnieją różne sposoby wdrożenia, z których najbardziej powszechnym i solidnym jest instalacja pomiędzy sieciami prywatnymi i publicznymi. Dobra planifikacja IPS powinna uwzględniać takie czynniki jak kompleksowa ochrona w czasie rzeczywistym przed lukami sieciowymi i złośliwym oprogramowaniem, a także nieznanymi poleceniami i kontrolami. Ponadto, rozwiązanie musi być spójne, uproszczone i pozwalać na odpowiednie zarządzanie polityką w całym obwodzie korporacyjnym, centrum danych, chmurach publicznych i prywatnych, między innymi. Ponadto, może być zaprojektowane tak, aby zawierało narzędzia inteligentne, takie jak uczenie maszynowe, aby skutecznie zapobiegać atakom, a jednocześnie pozwalało na utrzymanie wysokiej przepustowości i niskiej latencji w celu wyzerowania krytycznych zagrożeń, dzięki czemu administratorzy mogą skupić się na tym, co najważniejsze i nie tracić czasu na fałszywe pozytywne alerty.

W przypadku infrastruktury krytycznej narzędzia IPS są jeszcze mało wydajne, a ich nieprawidłowe wdrożenie może bardziej uszkodzić sieć niż ją chronić. Systemy krytyczne, pracujące 24 godziny na dobę, 7 dni w tygodniu, wymagają stałej komunikacji i przepływu ruchu sieciowego, gdzie zwykła przerwa, choćby najkrótsza, może zagrozić nie tylko systemowi, ale i zdrowiu ludzi, w zależności od rodzaju systemu krytycznego.

Z natury IPS jest w stanie zablokować i upuścić komunikację, co nie jest odpowiednie do zastosowania w krytycznym systemie, gdzie komunikacja nigdy nie może zostać przerwana. Tutaj, planowanie i projektowanie musi być jeszcze bardziej precyzyjne i ostrożne, w porównaniu do zwykłej sieci komputerowej. Systemy krytyczne są jednak również celem ataków i podatności na zagrożenia, a ich ochrona jest również koniecznością.

Podobnie jak w przypadku systemów IDS, powszechne jest również występowanie serwerów IPS zainstalowanych w sieci oraz stosowanie różnych serwerów w ramach różnych podsieci i sieci LAN.

4. ZŁOŚLIWE OPROGRAMOWANIE I ANTYWIRUS

- Wprowadzenie do złośliwego oprogramowania
- Jak dochodzi do infekcji złośliwym oprogramowaniem?
- Najczęstsze typy złośliwego oprogramowania
- Jak wykryć, usunąć i zapobiec infekcji złośliwym oprogramowaniem
- Szczególny przypadek programu antywirusowego
- Jak działa program antywirusowy
- Wybór dobrego oprogramowania antywirusowego

4.1. Wprowadzenie do złośliwego oprogramowania

Termin malware został po raz pierwszy użyty przez Yisraela Radai, informatyka i badacza bezpieczeństwa, w 1990 roku. Choć istniało ono przed tą datą.

Jednym z pierwszych znanych przykładów złośliwego oprogramowania był eksperyment inżyniera BBN Technbologies Roberta Thomasa z 1971 roku. Nazwany Creeper, został zaprojektowany do infekowania infrastruktury ARPANET. Chociaż złośliwe oprogramowanie nie zmieniało funkcji ani nie kradło danych, było w stanie przenieść się z pierwszego zainfekowanego mainframe'a na drugi, bez pozwolenia.

Aby lepiej zrozumieć, czym jest złośliwe oprogramowanie, możemy spojrzeć na nie jak na chorobę. W konkretnym przypadku grypy, jej wybuchy mają zwykle sezon, raz w roku i zwykle w czasie zimna i zimy, kiedy zaczyna się rozprzestrzeniać i zarażać ludzi. W konkretnym przypadku złośliwego oprogramowania, nie ma przewidywalnych sezonowych infekcji dla komputerów osobistych lub innych urządzeń, takich jak telefony komórkowe, tablety i infekcji korporacyjnych. Tutaj malware może być postrzegane nieco bardziej jako infekcja COVID-19, która może wystąpić w ciągu całego roku i w dowolnym czasie i miejscu. Jednak zamiast odczuwać fizyczne objawy, tak jak w przypadku grypy lub COVID-19, użytkownicy komputerów chorują na rodzaj choroby maszynowej, zwanej malware.

Istnieje wiele różnych typów infekcji malware, a każdy typ ma swoją własną metodę ataku, która może się wahać od furii do subtelnego jak młot kowalski.

W głębszym ujęciu malware, czyli inaczej złośliwe oprogramowanie, to termin określający każdy złośliwy program lub kawałek kodu, który przynosi szkody w systemach i sieciach.

Złośliwe oprogramowanie ma na celu inwigilację, uszkodzenie lub wyłączenie komputerów, systemów komputerowych, sieci i urządzeń mobilnych, zarówno przy całkowitej lub częściowej kontroli nad ich działaniem, zakłócając ich normalny sposób funkcjonowania i normalne zachowanie.

Jednak to, co w rzeczywistości stoi za atakiem złośliwego oprogramowania, może się różnić w zależności od przypadku. Złośliwe oprogramowanie może na przykład koncentrować się lub zamierzać zarabiać na użytkowniku, sabotować jego zdolność do wykonywania pracy, wygłaszać oświadczenia polityczne lub skupiać się na zwykłym przechwalaniu się. Złośliwe oprogramowanie nie jest w stanie spowodować fizycznych uszkodzeń sprzętowych w systemach lub urządzeniach sieciowych, może jednak szyfrować, kraść, a nawet usuwać dane oraz zmieniać lub przejmować podstawowe funkcje komputera, szpiegując aktywność użytkowników za wiedzą lub bez zgody.

Ale skąd użytkownik może wiedzieć, czy jego urządzenia są, czy nie są zainfekowane? Podobnie jak w przypadku ludzkiej grypy, gdzie pojawiają się objawy i pozwalają nam dostrzec obecność choroby w organizmie, również w przypadku złośliwego oprogramowania można zaobserwować wiele różnych zachowań na zainfekowanych urządzeniach:

· **Komputer zwalnia** - Jednym z głównych efektów ubocznych malware jest to, że może powodować zmniejszenie prędkości systemu operacyjnego urządzenia, które infekuje, czy to podczas dostępu do Internetu i nawigacji, czy po prostu powodując spadek prędkości aplikacji lokalnych. Można również zaobserwować, że zużycie zasobów systemu, takich jak wykorzystanie pamięci i procesora, jest nienormalnie wysokie. W niektórych przypadkach można nawet zauważyć, że wentylator komputera warkotał z pełną prędkością, tak jak procesor osiąga wysoką temperaturę z wyższego zapotrzebowania na obliczenia. Jest to dobra wskazówka, że coś wykorzystuje zasoby komputera w tle i jest to "objaw", który zwykle dzieje się, gdy komputer został związany z botnetem ("*sieć prywatnych komputerów zainfekowanych złośliwym oprogramowaniem i kontrolowanych jako grupa bez wiedzy właścicieli*").

· **Ekran jest zalany denerwującymi reklamami** - Odtwarzanie bardzo denerwującej sytuacji, i że typowo identyfikuje infekcję malware, to nieoczekiwane reklamy pop-up, które zalewają urządzenia z różnymi informacjami i w dowolnym momencie. Takie zachowanie jest rodzajem złośliwego oprogramowania, zwykle znanego jako adware, ponieważ koncentruje się na wyświetlaniu niechcianych reklam użytkownikowi i zwykle przychodzi spakowany z innymi ukrytymi zagrożeniami malware.

· **Awarie systemu** - awarie systemu występują jako zamrożenie lub niebieski ekran śmierci, podobnie jak w systemie Microsoft Windows, gdzie system zwraca niebieski ekran po napotkaniu błędu krytycznego.

· **Tajemnicza utrata miejsca na dysku** - Zazwyczaj utrata miejsca na dysku jest spowodowana przez złośliwe oprogramowanie o dużej objętości, ukrywające się na dysku twardym. Jest to również znane jako bundleware.

· **Dziwny wzrost aktywności internetowej systemu** - Aby lepiej zrozumieć ten "objaw" można wziąć za przykład trojana. W momencie, gdy trojan zainfekuje komputer, zaczyna on sięgać do serwera dowodzenia i kontroli atakującego i pobiera wtórną infekcję, którą wielokrotnie jest ransomware. Jest to jedno z możliwych wyjaśnień podniesienia aktywności internetowej. Co więcej, może się to zdarzyć również w przypadku botnetów i programów szpiegowskich, a także każdego innego zagrożenia, które wymaga stałej komunikacji z serwerami atakującymi.

· **Zmiana ustawień przeglądarki** - Wiele razy można zauważyć zmianę na stronie głównej przeglądarki lub istnienie nowych pasków narzędzi, rozszerzeń lub wtyczek, których wcześniej nie było. Może to nastąpić w wyniku wejścia na zainfekowaną stronę lub kliknięcia na zainfekowaną reklamę pop-up.

· **Oprogramowanie antywirusowe przestaje działać** - Infekcja uniemożliwia ponowne włączenie ochrony antywirusowej, pozostawia urządzenie bez ochrony i bardziej podatne na inne ataki.

· **Utrata dostępu do plików lub całego komputera** - Jest to zazwyczaj związane z infekcją ransomware, gdzie hakerzy ogłaszają się poprzez pozostawienie notatki lub wiadomości na pulpicie, a nawet zmianę tapety pulpitu na taką wiadomość. Wiadomość zazwyczaj składa się z informacji, że zaszyfrowali wszystkie dane i żądają zapłaty w zamian za ich odszyfrowanie.

Wiele złośliwych programów sprawia również, że wszystko jest niezauważalne, więc nawet jeśli wszystko wydaje się działać w normalnym zachowaniu, nadal jest możliwe, aby urządzenie zostało zainfekowane złośliwym oprogramowaniem. Potężne złośliwe oprogramowanie może ukryć się głęboko w urządzeniu, unikając wykrycia i wykonując swoje zadania bez podnoszenia jakichkolwiek alarmów. Tutaj potrzebne jest dobre oprogramowanie zabezpieczające, które będzie w stanie wykryć infekcje nawet wtedy, gdy nie dają one silnych i odczuwalnych "objawów".

4.2. Jak dochodzi do infekcji złośliwym oprogramowaniem?

Istnieją dwie najczęstsze drogi, którymi złośliwe oprogramowanie dostaje się do systemów i powoduje infekcję: Internet i poczta elektroniczna. Samo w sobie oznacza to, że za każdym razem, gdy jesteśmy podłączeni, jesteśmy narażeni na atak. W dzisiejszych czasach, ponieważ zawsze jesteśmy podłączeni do Internetu, jeśli nie na komputerze stacjonarnym lub laptopie, to przynajmniej na smartfonie lub tablecie, zawsze jesteśmy narażeni na atak.

Złośliwe oprogramowanie może przeniknąć do urządzeń podczas surfowania po zhakowanych stronach internetowych, przeglądania legalnej witryny serwującej złośliwe reklamy, pobierania zainfekowanych plików, instalowania programów lub aplikacji z nieświadomych źródeł, otwierania złośliwego załącznika do wiadomości e-mail lub prawie wszystkiego innego pobieranego z Internetu na urządzenie, które nie posiada lub posiada knotową aplikację zabezpieczającą przed złośliwym oprogramowaniem.

Złośliwe aplikacje mogą ukrywać się w pozornie legalnych aplikacjach, zwłaszcza gdy są pobierane ze stron internetowych lub bezpośrednich linków, zamiast z oficjalnego sklepu z aplikacjami. Tutaj ważne jest, aby patrzeć na komunikaty ostrzegawcze podczas instalowania aplikacji, zwłaszcza jeśli szukają one pozwolenia na dostęp do poczty elektronicznej lub innych danych osobowych. Użytkownicy mają tendencję do zawsze naciskania następnego do końca instalacji, nie czytając ważnych informacji, które są dostarczane podczas procesu. Wiele razy oprogramowanie firm trzecich jest dołączane do oryginalnej aplikacji i zostaje zainstalowane w urządzeniu. W ten sam sposób może się zdarzyć złośliwe oprogramowanie, które może być ukryte wewnątrz oryginalnego pliku aplikacji. Ważne jest, aby instalować oprogramowanie uzyskane z zaufanych źródeł i od deweloperów.

Co więcej, najlepiej trzymać się zaufanych źródeł aplikacji mobilnych, instalując tylko renomowane aplikacje firm trzecich i zawsze pobierając te aplikacje bezpośrednio od sprzedawcy, a nigdy z innych stron internetowych. Ponadto unikaj pobierania tych ofert specjalnych, które obiecują cudowną prędkość Internetu, czyszczenie dysku i inne. Wybierz te aplikacje z certyfikowanych i zaufanych źródeł.

Jak się powszechnie mówi, człowiek (użytkownik) jest głównym aktorem dla każdego rodzaju infekcji malware. Czyli ufna wersja nas samych, skłonna do otwarcia załącznika do e-maila, którego nie rozpoznajemy, lub do kliknięcia i zainstalowania czegoś z niezaufanego źródła. Nie jest to skierowane tylko do mniej doświadczonych użytkowników, ale również wykwalifikowani ludzie wpadli w tego typu pułapki i skończyli zainfekowani złośliwym oprogramowaniem.

Nawet jeśli instalujesz coś z wiarygodnego źródła, ważne jest, aby zwrócić uwagę na prośbę o pozwolenie na jednoczesną instalację innego dołączonego oprogramowania, ponieważ możliwe jest zainstalowanie również niepożądanego oprogramowania, jak wspomniano wcześniej. To dodatkowe oprogramowanie, znane również jako potencjalnie niechciany program (PUP), jest wielokrotnie przedstawiane jako niezbędny składnik, ale często nim nie jest.

Istnieje jednak również przypadek scenariusza infekcji malware bez winy. Ponieważ jest to, po raz kolejny, możliwe, aby uzyskać infekcję po prostu odwiedzając złośliwą stronę internetową i oglądając zainfekowaną stronę lub baner reklamowy, który prowadzi do pobrania złośliwego oprogramowania. Złośliwe oprogramowanie rozpowszechniane za pośrednictwem złych reklam na legalnych stronach internetowych jest znane jako malvertising.

4.3. Najczęstsze typy złośliwego oprogramowania

Wśród wielu różnych rodzajów złośliwych programów można wyróżnić następujące, najczęściej spotykane formy:

· **Adware** - Już wcześniej wspomniano, adware to niechciane oprogramowanie stworzone do wyświetlania reklam na ekranach użytkowników, wiele razy w ramach przeglądarki internetowej. Ta forma malware używa podstępnej metody, aby przebrać się za legalne lub nakłada się na inny program, aby ukryć się i oszukać użytkownika do jego instalacji.

· **Spyware** - Przez swój środek, spyware skupia swoje działanie na potajemnym obserwowaniu działań i aktywności komputera lub użytkownika bez pozwolenia, zgłaszając to do twórcy malware.

· **Wirus** - Wirus może być również postrzegany jako złośliwe oprogramowanie, ponieważ składa się również z infekcji, która dołącza się do innego programu, a po wykonaniu replikuje się poprzez modyfikację innych programów komputerowych i infekowanie ich własnymi bitami kodu. Jego zachowanie jest znów podobne do wirusa infekującego człowieka, gdzie atakuje on komórki ciała, aby wstrzyknąć swój materiał genetyczny i replikować się w organizmie.

· **Robaki** - Robaki są podobne do wirusów i tak jak one, również się samoreplikują, modyfikując inne programy komputerowe w celu stworzenia ich kopii. Różnica pomiędzy wirusem a robakiem polega na tym, że robaki mogą samodzielnie rozprzestrzeniać się w systemach, podczas gdy wirusy wymagają pewnego rodzaju działania ze strony użytkownika, aby mogły rozpocząć proces infekcji.

· **Trojan** - Znany również jako koń tro**jański**, to złośliwe oprogramowanie jest postrzegane jako jeden z najbardziej niebezpiecznych typów, ponieważ zwykle przedstawia się jako coś godnego zaufania, gdy w rzeczywistości nim nie jest. Po dotarciu do systemu, napastnicy za trojanem uzyskać nieautoryzowany dostęp do dotkniętego komputera. Stamtąd, trojan do wykonywania najbardziej różnych działań, takich jak, na przykład, kradzież informacji finansowych lub nawet zainstalować inne formy złośliwego oprogramowania.

· **Ransomware** - Jak wspomniano wcześniej, ransomware jest formą złośliwego oprogramowania, które może zablokować użytkownika z urządzenia, szyfrując wszystkie dane i pliki oraz zmuszając użytkownika do zapłacenia określonej kwoty pieniędzy, aby odzyskać dostęp. Ransomware jest jedną z najczęściej używanych form złośliwego oprogramowania, ponieważ przynosi bezpośrednie źródło zysku, zwykle w trudnej do wyśledzenia płatności, takiej jak kryptowaluta. Niestety, kod stojący za ransomware jest łatwy do zdobycia za pośrednictwem internetowych rynków przestępczych, a obrona systemów przed nim jest bardzo trudnym zadaniem.

· **Rootkit** - Ten typ złośliwego oprogramowania zapewnia atakującemu prawa administratora w zainfekowanym systemie lub sieci, znane również jako "root" w systemach Unix. Podobnie jak inne typy, rootkit jest również zaprojektowany tak, aby był ukryty i niezauważalny dla użytkownika, innego oprogramowania w systemie oraz samego systemu operacyjnego.

· **Keylogger** - Keylogger to złośliwe oprogramowanie zdolne do nagrywania wszystkich uderzeń użytkownika w klawiaturę, zbierania informacji i wysyłania ich do napastnika. Zazwyczaj napastnicy poszukują danych uwierzytelniających, w tym nazw użytkowników, haseł, danych kart kredytowych i innych.

· **Malicious Cryptomining** - Znany również jako drive-by mining lub cryptojacking, ta forma złośliwego oprogramowania jest zwykle instalowana przez trojana, umożliwiając atakującemu wykorzystanie komputera do wydobywania kryptowalut, takich jak Bitcoins lub Monero. Tutaj, zamiast pozwolić użytkownikowi spieniężyć zebrane monety, napastnicy wysyłają je na własne konto.

· **Exploits** - Ta forma złośliwego oprogramowania wykorzystuje błędy i inne istniejące luki w systemie lub sieci, aby dać napastnikowi pewnego rodzaju dostęp. Będąc tam, atakujący będzie w stanie wykraść lub uzyskać dostęp do danych, a nawet upuścić lub wstrzyknąć kod, taki jak inna forma złośliwego oprogramowania. Exploit zero-day odnosi się do luki w oprogramowaniu, dla której nie ma obecnie dostępnej obrony lub poprawki.

· **Scareware** - W tym przypadku cyberprzestępcy straszą użytkowników, sprawiając, że myślą, że ich komputery lub urządzenia mobilne zostały zainfekowane, aby przekonać ich do zakupu fałszywej aplikacji. W typowym oszustwie scareware możliwe jest zobaczenie alarmującego komunikatu podczas przeglądania stron internetowych, który mówi "Ostrzeżenie: Twój komputer jest zainfekowany!" lub "Masz wirusa!". Cyberprzestępcy wykorzystują te programy i nieetyczne praktyki reklamowe, aby przestraszyć użytkowników do zakupu nieuczciwych aplikacji.

· **Fileless Malware** - Ta forma złośliwego oprogramowania atakującego rejestr nie pozostawia plików do skanowania ani złośliwych procesów do wykrycia. Nie opiera się na plikach, a przez to nie pozostawia śladu, co czyni go trudnym do wykrycia i usunięcia. Takie złośliwe oprogramowanie wykorzystuje legalne programy do zainfekowania systemu lub sieci.

4.4. Jak wykryć, usunąć i zapobiec infekcji złośliwym oprogramowaniem

Jak wspomniano wcześniej, tylko poprzez percepcję i obserwację, czasami możliwe jest, aby użytkownicy wykryli obecność infekcji i ataków malware. Jednak nie zawsze jest to możliwe do wykrycia, a nawet w takim przypadku systemy są zagrożone. W tym przypadku, podobnie jak w przypadku zdrowia ludzkiego, również w systemach i sieciach, istnieje kilka testów, które można zastosować, aby upewnić się, że wszystko jest wolne od infekcji, a informacje są bezpieczne.

Wiele programów zabezpieczających zostało opracowanych w celu wykrywania i zapobiegania infekcjom i atakom złośliwego oprogramowania, a także w celu ich usuwania. Działając podobnie do skanowania antywirusowego, aplikacje antymalware przeprowadzają skanowanie komputera, wykrywając i identyfikując infekcje, dając użytkownikom możliwość ich usunięcia lub zatrzymania plików w kwarantannie.

Przykładem antymalware jest znany Malwarebytes, który zajmuje się zarówno wykrywaniem, jak i usuwaniem zainfekowanych plików i rejestrów. Działa on pod platformami Microsoft Windows, macOS, Android oraz iOS.

Innym dobrym przykładem jest darmowe narzędzie instalowane na maszynach z systemem Microsoft Windows powyżej wersji 10, o nazwie Windows Defender. Narzędzie to jest w stanie chronić lokalny komputer przed zagrożeniami takimi jak spyware, adware czy wirusy.

Jeśli chodzi o zapobieganie atakom złośliwego oprogramowania i infekcjom, istnieje kilka różnych sposobów ochrony systemów i sieci. W konkretnym przypadku komputera osobistego, odbywa się to poprzez instalację prostego oprogramowania antymalware, jak te wymienione powyżej. Jednak sama aplikacja nie wystarczy do utrzymania właściwej ochrony, gdzie użytkownicy muszą również praktykować bezpieczne zachowania na swoich urządzeniach. Obejmuje to nie otwieranie załączników od niezaufanych nadawców i dostęp do niezaufanych stron internetowych.

Ponadto, takie aplikacje antymalware powinny mieć okresowe aktualizacje i skanowania, ponieważ hakerzy stale dostosowują się i opracowują nowe techniki naruszania oprogramowania zabezpieczającego. Ponadto, twórcy oprogramowania zabezpieczającego również okresowo wydają aktualizacje, aby załatać te luki. Jeśli użytkownicy zaniedbają aktualizację swoich narzędzi zabezpieczających, łaty te nie zostaną zastosowane, pozostawiając ich podatnymi na możliwe do uniknięcia exploity.

W środowiskach korporacyjnych, gdzie sieci i systemy są większe niż proste sieci domowe, dotkliwość ataku ma znacznie większe szkody. W tym przypadku konieczne jest podjęcie pewnych proaktywnych kroków w celu egzekwowania ochrony przed złośliwym oprogramowaniem:

- Wdrożenie podwójnego zatwierdzenia dla transakcji między przedsiębiorstwami (B2B);
- Wdrożenie weryfikacji drugiego kanału dla transakcji business-to-consumer (B2C);
- Wdrożenie wykrywania złośliwego oprogramowania i zagrożeń w trybie offline w celu wychwycenia złośliwego oprogramowania przed jego rozprzestrzenieniem się;
- Wdrażanie zasad bezpieczeństwa typu "allow list" zawsze, gdy jest to możliwe;
- Wdrażanie silnych zabezpieczeń na poziomie przeglądarki internetowej.

4.5. Szczególny przypadek programu antywirusowego

Oprócz oprogramowania i narzędzi antymalware istnieją również programy antywirusowe potrafiące poradzić sobie z tym konkretnym typem złośliwego oprogramowania (wirusami). Antywirusy są znacznie bardziej znane i prawie każdy użytkownik ma je zainstalowane na swoich urządzeniach stacjonarnych i laptopach.

Antywirus to program służący do zapobiegania, skanowania, wykrywania i usuwania wirusów z komputera, systemu lub sieci. Po zainstalowaniu większość antywirusów działa automatycznie w tle, zapewniając w czasie rzeczywistym ochronę instalowanego systemu i zapobiegając infekcjom i atakom wirusów.

Kompleksowe programy ochronne pomagają w ochronie plików i sprzętu przed złośliwym oprogramowaniem, takim jak robaki i wirusy, ale także przed końmi trojańskimi i oprogramowaniem szpiegowskim. Dodatkowa ochrona jest jednak istotna i narzędzia te powinny działać razem z zaporami sieciowymi i narzędziami antymalware, zwiększając poziom bezpieczeństwa, a tym samym zapewniając wysoki poziom ochrony danych.

Ogólnie rzecz biorąc, programy antywirusowe i programy do ochrony komputera są opracowywane w celu analizowania danych, w tym nie tylko plików lokalnych, ale także stron internetowych, zainstalowanych aplikacji i innego oprogramowania, aby pomóc w znalezieniu i usunięciu złośliwego oprogramowania w sposób i tak szybko, jak to możliwe.

Większość narzędzi antywirusowych zapewnia ochronę w czasie rzeczywistym, działając w tle, i że jest w stanie chronić urządzenia przed przychodzącymi zagrożeniami, atakami i infekcjami wirusowymi. Stale skanuje urządzenie pod kątem znanych zagrożeń i zapewnia automatyczne aktualizacje, identyfikując, blokując i usuwając złośliwe kody i wirusy.

W dzisiejszych czasach większość czynności wykonywana jest online, a z tego powodu codziennie pojawiają się nowe zagrożenia, przez co ważne jest korzystanie z ochronnego programu antywirusowego. Na szczęście obecnie na rynku istnieje również wiele doskonałych produktów, które są w stanie poradzić sobie z takimi zagrożeniami i infekcjami. Wśród głównych twórców antywirusów można wyróżnić między innymi Norton, McAfee, TrendMicro, Checkpoint.

4.6. Jak działa program antywirusowy

Oczywiście pierwszym krokiem będzie instalacja, ale oprócz tego i po zainstalowaniu, program antywirusowy zaczyna od sprawdzenia komputera lub serwera, na którym jest zainstalowane, pod kątem programów i plików względem bazy danych znanych typów malwares. Ponieważ codziennie powstają nowe wirusy i zawsze są rozpowszechniane przez hakerów, narzędzie antywirusowe skanuje również urządzenie pod kątem możliwości wystąpienia nowych lub nieznanych zagrożeń i infekcji.

Zazwyczaj większość programów pracuje na trzech różnych trybach wykrywania, z których pierwszy to wykrywanie specyficzne, gdzie identyfikuje znane złośliwe oprogramowanie; drugi to wykrywanie ogólne, które szuka znanych części lub typów złośliwego oprogramowania lub wzorców, które pokazują związek przez wspólną bazę kodową; a trzeci skupia się na wykrywaniu heurystycznym, skanując w poszukiwaniu nieznanych wirusów i infekcji poprzez identyfikację znanych podejrzanych struktur plików. Gdy program znajdzie plik zawierający wirusa, zwykle umieszcza go w kwarantannie i oznacza do usunięcia. W procesie kwarantanny możliwa jest ocena zachowania pliku i określenie, czy należy go usunąć z urządzenia.

Ważne jest jednak, aby zrozumieć, że nawet program antywirusowy jest w stanie chronić system lub sieć, w której jest zainstalowany, nie jest w stanie chronić go przed wszystkimi rodzajami złośliwego oprogramowania. Aby lepiej to zrozumieć, należy zdać sobie sprawę, że istnieją dwa różne sposoby identyfikacji złośliwego oprogramowania przez oprogramowanie antywirusowe: wykrywanie sygnatur i wykrywanie zachowań. Podobnie jak systemy IDS i IPS, również narzędzia antywirusowe skupiają się na dwóch różnych podejściach, wykorzystując znane podatności oraz sygnatury i zachowania infekcji.

Jeśli chodzi o wykrywanie sygnatur, można je postrzegać, po raz kolejny, jak układ odpornościowy człowieka, gdzie skanuje on ciało (komputer) w poszukiwaniu specjalnych cech lub sygnatur programów, o których wiadomo, że są związane ze złośliwym kodem, infekcjami lub zagrożeniami. Robi to odwołując się do słownika znanych złośliwych programów, opracowanego na podstawie znanych sygnatur. Jeśli coś w systemie pasuje do wzorca obecnego w bazie, program próbuje to zneutralizować, poddając kwarantannie lub po prostu usuwając. Co więcej, i znów nawiązując do ludzkiego układu odpornościowego, słownik czy baza danych wymaga aktualizacji. Tak jak w zdrowiu ludzkim szczepimy się lub bierzemy tabletki z lekami, tak w komputerach aktualizacje są kluczowe dla utrzymania odpowiedniego poziomu ochrony. Dzięki tym aktualizacjom narzędzia antywirusowe rozpoznają nowe i dotąd nieznane złośliwe oprogramowanie, zagrożenia i luki.

Oprogramowanie antywirusowe może jedynie chronić system przed tym, co uznaje za szkodliwe, problem w tym, że cyberataki stale rosną i są przeprowadzane w bardziej wyrafinowany sposób każdego dnia. Ewolucja nowych exploitów i ataków jest tak duża, że producenci oprogramowania antywirusowego muszą uciekać przed czasem, aby móc nadążyć za ciągłym zapotrzebowaniem na ochronę. W rezultacie, bez względu na to, jak niedawno program antywirusowy został zaktualizowany, zawsze pojawia się jakieś nowe złośliwe oprogramowanie, które może ewentualnie obejść oprogramowanie antywirusowe i narzędzia antymalware.

Skupiając się na wykrywaniu zachowań, antywirus nie próbuje zidentyfikować znanego złośliwego oprogramowania, tak jak robi to w przypadku podejścia opartego na wykrywaniu sygnatur. Zamiast tego monitoruje zachowanie oprogramowania zainstalowanego na maszynie, którą antywirus chroni. Aby prawidłowo wytrenować narzędzie antywirusowe, konieczne jest, aby oprogramowanie posiadało wiedzę na temat tego, jak wygląda normalne zachowanie monitorowanego przez nie oprogramowania. Następnie, gdy program zachowuje się w podejrzany sposób, np. próbuje uzyskać dostęp do chronionego pliku lub modyfikuje inny program, antywirus oparty na zachowaniu dostrzeże podejrzaną aktywność i ostrzeże o niej użytkownika, umożliwiając mu podjęcie odpowiednich działań w obliczu zagrożenia. Takie podejście jest szczególnie skuteczne w ochronie systemu przed nowymi rodzajami złośliwego oprogramowania, które nie istnieją jeszcze w słownikach czy bazach danych i których sygnatury nie zostały jeszcze odkryte ani udokumentowane. Problemem jest jednak to, że takie podejście może zwiększyć liczbę fałszywych ostrzeżeń. Jako użytkownik komputera może nie mieć pewności co do właściwego działania w przypadku takich fałszywych alarmów, co umożliwia nieprawidłowe zezwolenie na działania. Ponadto w przypadku dużej liczby ostrzeżeń użytkownik może ulec pokusie zezwolenia na wszystkie, pozostawiając komputer otwarty na ataki i infekcje. Ponadto, do czasu wykrycia zachowania, również złośliwe oprogramowanie najprawdopodobniej zostało już uruchomione w systemie, co sprawia, że użytkownik nie ma pewności co do działań, jakie podjęło złośliwe oprogramowanie, zanim zostało ono zidentyfikowane przez oprogramowanie antywirusowe.

Antywirus jest ważnym elementem zabezpieczenia komputera, systemu, sieci lub urządzenia mobilnego i jest zalecany przez większość naukowców i badaczy tej dziedziny. Kluczową kwestią jest jednak to, że niezależnie od rodzaju i marki oprogramowania antywirusowego, nie jest ono w stanie ochronić systemu przed wszystkimi rodzajami złośliwego oprogramowania.

4.7. Wybór dobrego oprogramowania antywirusowego

Wśród ogromu rozwiązań antywirusowych jest kilka punktów, na które należy zwrócić uwagę nawet po wyborze najlepszego rozwiązania chroniącego nasze systemy:

1. Uzyskaj oprogramowanie antywirusowe tylko ze znanych, zaufanych źródeł i sprzedawców. Częstą sztuczką cyberataków jest rozpowszechnianie fałszywych programów antywirusowych, które w rzeczywistości są złośliwym oprogramowaniem.

2. Upewnij się, że masz zainstalowaną najnowszą wersję oprogramowania antywirusowego, że subskrypcja jest opłacona i aktywna oraz że antywirus jest skonfigurowany do automatycznej aktualizacji. Aktualizacje nigdy nie powinny być odkładane na później.

3. Upewnij się, że program antywirusowy automatycznie skanuje przenośne nośniki danych, takie jak pamięci USB, i upewnij się, że ochrona w czasie rzeczywistym jest włączona.

4. Zwracaj uwagę na ostrzeżenia i alerty generowane na ekranie przez oprogramowanie antywirusowe. Większość alertów zawiera opcję uzyskania dodatkowych informacji lub zalecenia, co należy zrobić dalej.

5. Nie należy wyłączać ani odinstalowywać oprogramowania antywirusowego, ponieważ wydaje się, że spowalnia ono komputer, blokuje stronę internetową lub uniemożliwia zainstalowanie aplikacji lub programu. Wyłączenie programu antywirusowego narazi system na niepotrzebne ryzyko i może spowodować poważny incydent bezpieczeństwa.

6. Nie należy instalować w systemie wielu programów antywirusowych jednocześnie. Robienie tego najprawdopodobniej spowoduje konflikt programów ze sobą i może faktycznie zmniejszyć bezpieczeństwo komputera.

7. Naucz się rozpoznawać ostrzeżenia, które wydaje oprogramowanie antywirusowe. Cyberatakujący mogą tworzyć złośliwe strony internetowe, które zamieszczają bardzo realistyczne, ale fałszywe ostrzeżenia antywirusowe i oferują pomoc w "naprawie" komputera. Kliknięcie łączy lub przycisków na tych stronach może w rzeczywistości zaszkodzić Twojemu komputerowi.