Usługi i protokoły bezpieczeństwa

- Zabezpieczanie sieci
- Rodzaje ataków i exploity
- Ochrona systemów
- Metody szyfrowania
- System bezpieczeństwa sieciowego Kerberos

- Sieć jest atakowana na coraz bardziej wyrafinowane sposoby, które nieustannie są rozwijane.
- Wydaje się, że bieżące wiadomości zawsze mogą zawierać najnowszego wirusa, konia trojańskiego lub robaka, a w wiadomości e-mail z banku może znajdować się ostrzeżenie dla danego klienta, że ktoś przechwycił informacje związane z jego kartą kredytową.
- Jeżeli funkcjonowanie sieci wydaje się dziwne lub działa w niej jakiś system, to użytkownik jest usprawiedliwiony, kiedy zachowuje się jak paranoik.
- Żyjemy w niepewnych czasach, ale zawsze istnieje możliwość zniechęcenia potencjalnych atakujących przez lepsze zabezpieczenie sieci, a tym samym zmuszenie ich do poszukania łatwiejszego celu ataku.

- Nie ma jednej skutecznej metody ochrony sieci.
- Każdy system bezpieczeństwa może zostać złamany, jeżeli nie z zewnątrz, to z wewnątrz.
- Najlepszym sposobem zapewnienia bezpieczeństwa sieci jest stosowanie różnych warstw zabezpieczeń. W takim przypadku, zanim atakujący uzyska dostęp, będzie musiał pokonać co najmniej dwa systemy zabezpieczeń.
- Regularna zmiana parametrów bezpieczeństwa, na przykład haseł, oraz podział sieci na części to dwie kolejne metody, które są nieocenione.

Luki w zabezpieczeniach sieci

- Luki w zabezpieczeniach sieci to słabe punkty, które można wykorzystać w celu uzyskania dostępu do danego systemu.
- Przyczyny złamania zabezpieczeń mogą być różne:
  - stosowanie słabych haseł przez użytkowników,
  - wirusy i konie trojańskie,
  - błędy w oprogramowaniu,
  - pliki wykonywalne lub skrypty uruchomione w systemie, a także umieszczenie fragmentów kodu w systemie.
- Kiedy luka w zabezpieczeniach staje się znana, są tworzone programy, które ją wykorzystują. Programy takie określa się exploitami, rozpowszechniają się równie szybko jak wirusy.

- Każdy program zawiera jakieś błędy bądź procedury, które można złamać.
- Aktualizacje regularnie dostarczane przez firmy, na przykład infrastruktura Microsoft Update, mają za zadanie usuwać odkryte luki.
- Ujawnienie luki w systemie przed opracowaniem aktualizacji poprawiającej dany błąd naraża system na ataki z wykorzystaniem tej luki.
- Ataki tego rodzaju są nazywane Zero Day Exploit. Można w to wierzyć bądź nie, ale istnieją firmy dostarczające usługę subskrypcji, która informuje klientów o sposobie wykorzystania Zero Day

- Exploit do atakowania systemów. Oczywiście istnieją też inne firmy, które z kolei informują klientów, jak się bronić przed tego rodzaju atakami.
- Jesteśmy więc świadkami nieustanne go wyścigu między atakującymi i atakowanymi.

- Najlepszym zaleceniem dotyczącym Zero Day Exploit jest stosowanie we wszystkich systemach uaktualnień tuż po ich wydaniu.
- Wielu administratorów wzdraga się przed traktowaniem tej sugestii jako przykładu najlepszego rozwiązania, ponieważ aktualizacje mogą wyeliminować pewne błędy, ale jednocześnie wprowadzić nowe.
- Automatyczne uaktualnianie systemów produkcyjnych wprowadza element niepewności, który by nie występował, gdyby oprogramowanie systemowe nie ulegało zmianom.

- Jedną z metod stosowanych do wykrywania luk w zabezpieczeniach sieci jest próbkowanie sieci za pomocą narzędzia analizy ryzyka — skanera luk w zabezpieczeniach.
- Tego rodzaju skanery działają w ten sposób, że skanują sieć dla wszystkich przypisanych adresów IP, określają otwarte porty, a następnie budują listę programów i systemów operacyjnych, które funkcjonują w różnych systemach.
- Skanerami tego typu są skanery portów, skanery sieciowe, skanery witryn internetowych oraz dedykowane narzędzia znajdujące się w platformach struktur przeznaczonych do zarządzania.
- Po zakończeniu badania początkowego skaner może zbudować mapę sieci albo utworzyć raport. Jeżeli skaner używa SNMP, WMI lub innego protokołu zarządzania, to ma możliwość sprawdzania systemów i aplikacji w celu określenia nie tylko ich rodzaju, ale także numerów wersji i poziomu aktualizacji.
- Mogą być stosowane oznaczenia poziomów zagrożenia oraz listy zaleceń i działań, które administratorzy powinni podjąć w celu dalszego zabezpieczenia sieci.

- Przemysłowy standard określania podatności systemu komputerowego na luki w zabezpieczeniach ma nazwę Common Vulnerability Scoring System (CVSS).
- Ocena bazuje na zestawie pomiarów i dotyczy podstawowych lub poważnych luk w zabezpieczeniach, wskazuje zagrożenia oraz uwzględnia czynniki związane z implementacją bądź środowiskiem.
- CVSS FIRST (ang. Forum of Incident Response and Security Teams),
  - Standard ten (obecnie w wersji 2.) został opracowany przez grupę CVSS Special Interest Group — SIG.
  - Do kalkulatora online dostarczanego przez bazę danych National Vulnerability Database w sekcji SVSS Scoring można wprowadzić różne dane w celu otrzymania określonych ocen

- Powszechnie dostępne są również inne narzędzia.
  - Jednym z przykładów jest Microsoft Ba seline Security Analyzer. Narzędzie MBSA używa infrastruktury Microsoft Update oraz agenta lokalnego w celu określenia, czy system Windows jest bezpieczny i uaktualniony.
  - Według firmy Microsoft ta bazująca na internecie usługa przeprowadza tygodniowo sprawdzanie trzech milionów systemów pod kątem istnienia luk w zabezpieczeniach.
  - MBSA może skanować systemy nie tylko takie jak Windows 10, ale również Windows CE i Embedded, serwery Microsoft SQL Server oraz Microsoft Internet Information Server.

- Skanowanie pod kątem luk w zabezpieczeniach oraz rozpoznawanie sieci to techniki stosowane również przez **atakujących**, którzy próbują uzyskać dostęp do sieci, a także funkcje niektórych robaków.

Baza danych National Vulnerability Database

- CVE (ang. Common Vulnerabilities and Exposures) — słownik zagrożeń bezpieczeństwa obsługiwany przez MITRE Corporation dla wydziału National Cyber Security Division Departamentu Bezpieczeństwa Krajowego Stanów Zjednoczonych.
- CVE używa systemu identyfikatorów, które unikalnie identyfikują znane zagrożenia. Czynniki zagrożenia są czasami określanejako identyfikatory CVE, nazwy, numery, identyfikatory lub po prostu CVE.
- Umieszcza się je w bazie danych po zidentyfikowaniu ich przez firmy trzecie jako potencjalnych czynników zagrożenia.
- Czynnik taki otrzymuje numer CAN (ang. Candidate Number), następnie jest analizowany oraz potwierdzany i staje się oficjalnym wpisem na liście CVE.

- Funkcją MITRE Corporation w obsłudze tej bazy danych jest opisywanie zagrożeń, nadawanie im numerów CAN oraz publiczne udostępnianie zebranych informacji.
- Baza danych CVE zawiera znane zagrożenia zebrane z całego świata i jest dostępna bezpłatnie.
- Z punktu widzenia CVE luka w zabezpieczeniach jest błędem w oprogramowaniu, który umożliwia uzyskanie nieuprawnionego dostępu do systemu bądź sieci.
- Błąd w prawidłowym stosowaniu oprogramowania lub pozostawienie systemu otwartego nie jest uznawany za lukę w zabezpieczeniach, a tym samym nie znajduje się w bazie danych.
- Jeżeli na przykład sieciowy system operacyjny pozwala na ustalanie silnych haseł, ale użytkownik nie jest zmuszany do ich stosowania lub w ogóle nie musi stosować hasła, to w takim przypadku nie mówimy o luce w zabezpieczeniach.

- Luka w zabezpieczeniach występuje, gdy:
- atakujący może uzyskać dostęp do danych, do których nie ma uprawnień,
- atakujący może podszyć się pod innego użytkownika,
- atakujący może doprowadzić do sytuacji, w której usługa będzie niedostępna dla innych użytkowników.

- Istnieje możliwość przeszukania listy CVE w bazie danych National Vulnerability Database (NVD) przy wykorzystaniu witryny internetowej http://nvd.nist.gov/.
- Obecnie baza danych zawiera informacje o ponad 50 tys znanych lukach w zabezpieczeniach i może zostać pobrana w celu jej przeglądania online.
- Dane znajdujące się w bazie obsługują program ISAP (ang. U.S. Information Security Program) oraz działają w charakterze repozytorium dla protokołu Security Content Automation Protocol, używanego do monitorowania bezpieczeństwa sieci i szacowania poziomu zagrożenia.

- Baza danych NVD wykorzystuje strukturalny system nazw dla różnych typów systemów informatycznych, oprogramowania oraz innych pakietów.
- System ten ma składnię podobną do używanej w adresach URI (ang. Uniform Resource Identifiers) stosowanych w internecie; ma nazwę Common Product Enumeration (CPE) (katalog produktów) i jest dostarczany w formacie możliwego do pobrania pliku XML jako część bazy danych.

Miejsca ataku

- Bezpieczeństwo sieci najczęściej jest naruszane z zewnątrz.
- Typowy atak dotyczy luk w zabezpieczeniach, w oprogramowaniu bądź sprzęcie.
- Jednak luki w bezpieczeństwie, które pozwalają na dostanie się do wewnątrz sieci, bardzo często są najskuteczniejsze, ponieważ mogą działać niewykryte.

- Najczęstszymi obszarami ataków są:
- Zewnętrzne — dostępność systemu. System może być przeciążony przez rozgłoszenie w sieci z dużą liczbą komputerów sfałszowanego pakietu ICMP, w którym zmieniono adres źródła na adres atakowanego systemu, co skutkuje dużą ilością odpowiedzi ECHO do atakowanego systemu. W takim przypadku mamy do czynienia z **tzw. atakiem smerfów (ang. Smurf Attack).**
- Zewnętrzne — odmowa usług (DoS, Denial of Service). Atak, w którym usługa sieciowa jest zasypana żądaniami, nazywa się odmową usług (DoS). Najbardziej znanym przykładem ataku **DoS** jest atak na serwer nazw domeny (DNS). Kiedy taki atak się powiedzie, to dla systemów obsługiwanych przez zaatakowany DNS adresy innych systemów w internecie lub intranecie będą niemożliwe do ustalenia, a tym samym niedostępne.
  - Atak Distributed Denial of Service (**DDoS**) oznacza atak przeprowadzony przez ogromną liczbę złamanych systemów, które działają jak tzw. komputery zombies i mogą być zamienione w botnety, czyli „roboty sieciowe”.

- Zewnętrzne lub wewnętrzne — uwierzytelnianie. Atakujący podszywa się pod tożsamość innego użytkownika.
- Dane w trakcie transportu. Ruch sieciowy jest przechwytywany w trakcie transmisji, modyfikowany, a następnie wysyłany do miejsca przeznaczenia. Taki atak nazywa się **„atakiem z osobą pośrodku”** (ang. man-in-the-middle attack); jego efektem może być podsłuchanie danych.
- Wewnętrzne — robaki, konie trojańskie oraz inne programy otwierające tylne drzwi. Wymienione programy dostarczają atakującemu metod kontrolowania systemów wewnątrz sieci oraz możliwość zmiany komputerów na zombies. Tylne drzwi mogą być programami wykonywalnymi lub algorytmami, które mogą omijać mechanizm uwierzytelniania sieciowego, przeprowadzać różne operacje i pozostawać w ukryciu.
  - Rootkit to rodzaj programu otwierającego tylne drzwi — potrafi ukrywać się jako sterownik niskiego poziomu lub moduł jądra. Rootkit nie pojawia się w systemie plików, a na liście procesów może widnieć jako zwykły proces systemowy.
- Bezpośredni dostęp wewnątrz. Atak może nastąpić z nośnika takiego jak dysk optyczny, pamięć USB, napęd przenośny itp.

- W trakcie opracowywania oprogramowania firma Microsoft używa modelu szacowania zagrożenia, który został nazwany podejściem STRIDE. Skrót STRIDE oznacza:
- Spoofing Identity (authentication), czyli podszywanie się pod inną osobę (uwierzytelnianie) — atakujący może podszyć się pod innego użytkownika. Użytkownicy i systemy muszą stosować uwierzytelnianie za pomocą haseł, certyfikatów cyfrowych bądź innych metod.
- Tampering with Data (integrity), czyli złośliwa modyfikacja danych (spójność)- atakujący modyfikuje dane. Metody stosowane do zapewnienia spójności danych obejmują między innymi procedury sprawdzania błędów w danych.
- Repudiation (non-repudiation), czyli wyparcie się (brak możliwości wyparcia się) - poszczególne osoby odrzucają odpowiedzialność za przeprowadzane operacje.
- Information Disclosure (confidentiality), czyli dotarcie do informacji przez osobę niemającą odpowiednich uprawnień (zapewnienie poufności). W tym przypadku atakujący zyskuje dostęp do informacji poufnych. Sieci stosują ograniczenia dostępu za pomocą list dostępu, domen, usług katalogowych oraz innych funkcji sieciowych systemów operacyjnych, aby dostęp mogły uzyskać tylko te osoby, które mają do tego uprawnienia.

- Denial of Service (availability), czyli odmowa usług (dostępność). Atak typu DoS może doprowadzić do tego, że określona usługa stanie się niedostępna. Użytkownicy i systemy muszą być w niezawodny sposób połączeni z inicjowanymi zdarzeniami. Istnieje możliwość stosowania dzienników rejestrujących wszelkie zdarzenia, dołączenia danych uwierzytelniających użytkownika i systemu do danych, a także zapewnienia bezpiecznych kanałów komunikacji w celu transferu danych. W przypadku ważnych systemów powinny istnieć kopie bezpieczeństwa, które zapewniają możliwość działania po wystąpieniu awarii.
- Elevation of Privilege (authorization), czyli nieautoryzowane zwiększenie uprawnień (uwierzytelnianie). W tej sytuacji użytkownik systemu zyskuje większe uprawnienia, niż powinien mieć. Zasoby muszą być dostępne, kiedy jest to wymagane. Systemy odpowiedzialne za zarządzanie dostępem do zasobów muszą być bezpieczne. Natomiast użytkownicy powinni mieć najmniejszy poziom uprawnień, który pozwoli im na wykonywanie pracy.

Reguły tworzenia bezpiecznej sieci

- Środki bezpieczeństwa powinny koncentrować się na trzech oddzielnych poziomach:
  - Szacowanie ryzyka i ochrona przed zagrożeniem. Do najefektywniejszych technologii ochrony przed zagrożeniami zalicza się kontrolę dostępu użytkownika, szyfrowanie i zapory sieciowe.
  - Wykrywanie zagrożeń. Systemy wykrywania zagrożeń obejmują skanery antywirusowe i antyspyware'owe, systemy wykrywania włamań (ang. Intrusion Detection System, IDS), badanie zdarzeń oraz heurystyczną analizę zdarzeń w dziennikach zdarzeń.
  - Odpowiedź. Odpowiedzią na wykrycie włamania do systemu może być kwarantanna systemu bądź podsieci, przywrócenie stanu z ostatniej dobrej kopii zapasowej, naprawa i uaktualnienie mechanizmu ochrony.

- Z punktu widzenia kosztów i trudności implementacji każdy z trzech wymienionych poziomów bezpieczeństwa jest zwykle o rząd wielkości droższy niż poziom niższy.
- Dlatego wykrywanie zagrożeń może kosztować dziesięciokrotnie więcej niż szacowanie zagrożenia, natomiast odpowiedź może być już stukrotnie droższa od ochrony przed zagrożeniem.
- Warto zastanowić się nad kosztem instalacji oprogramowania skanowania antywirusowego i antyspyware'owego lub zapory sieciowej w stosunku do ilości czasu i kosztu związanego z naprawą wielu systemów, które padły ofiarą ataku.

- Jedną z najważniejszych reguł bezpiecznego projektu sieci jest minimalizacja „obszaru ataku” w systemie lub sieci. Obszar ataku to ujawniony profil systemu, który jest dostępny do przeglądania przez użytkownika bądź atakującego, zawierający na przykład następujące informacje:
  - protokoły działające w danej sieci bądź systemie,
  - interfejsy sieciowe, które mogą odpowiadać na zapytania lub wiadomości,
  - otwarte porty,
  - usługi działające w dostępnym systemie,
  - pola danych wejściowych użytkownika.

- Im mniejsza liczba dróg, którymi atakujący może spenetrować system, tym większe bezpieczeństwo.
- Jednak kiedy atakujący dostanie się do systemu, to mniejszy obszar ataku wcale nie ogranicza ilości zniszczeń, których intruz może dokonać.

- 14 najlepszych wskazówek dotyczących bezpieczeństwa sieci:

1) Używaj zapory sieciowej. Zawsze należy pracować za zaporą sieciową. Warto wybierać sprzętową zaporę sieciową zamiast programowej i upewnić się, że oferuje ona izolację zarówno fizyczną, jak i protokołu. System połączony z internetem i pozbawiony zapory sieciowej może być złamany w ciągu kilku minut.
2) Wymuszaj stosowanie silnych haseł. Zawsze trzeba zmieniać każde hasło domyślne. Należy stosować hasła o długości minimum ośmiu znaków, łączące małe i duże litery, cyfry oraz znaki w ciągi tekstowe, które nie występują w słowniku.
3) Zainstaluj oprogramowanie antywirusowe i antyspyware'owe. Szczególnie dotyczy to bram sieci.
4) Stosuj niezawodną politykę tworzenia kopii zapasowej systemu. Obrazy systemu należy przechowywać dla wszystkich systemów.
5) Aktualizuj oprogramowanie. Zawsze należy aktualizować oprogramowanie tuż po wydaniu aktualizacji, ale warto mieć kopię zapasową na wypadek wystąpienia jakichkolwiek problemów związanych z aktualizacją. Szczególną uwagę trzeba poświęcić każdemu programowi, który ma styczność z siecią publiczną. Bardzo ważne jest aktualizowanie na przykład serwera WWW i przeglądarki internetowej.
6) Podziel sieć na podsieci. To zapewnia fizyczną izolację sieci dzięki adresom IP.
7) Szyfruj poufne dane i używaj bezpiecznych protokołów podczas transmisji danych. Danych, których nigdy nie opublikowalibyśmy w dzienniku ogólnokrajowym, nie należy wysyłać w postaci zwykłego tekstu.

8) Uważaj na pobieraną treść, łącza internetowe oraz niechciane wiadomości e-mail. Należy wyłączyć domyślne wykonywanie skryptów.

9) Zminimalizuj liczbę sposobów ataku na system. Trzeba zamknąć wszystkie niepotrzebne porty i wyłączyć wszystkie nieużywane protokoły sieciowe.

10) Uważaj na udziały sieciowe i na udzielanie pełnych praw dostępu do współdzielonych zasobów. Udziały stanowią potencjalny mechanizm rozprzestrzenienia w sieci wirusów, robaków, koni trojańskich i innego złośliwego oprogramowania. Należy stosować silną politykę list kontroli dostępu w sieciowym systemie operacyjnym.

11) Uważaj na systemy mobilne i nośniki. Trzeba izolować laptopy, które są używane poza firmą, do chwili, gdy zostaną dokładnie sprawdzone. Należy się upewnić, że systemy poufne mają zablokowaną możliwość obsługi nośników, na przykład pamięci USB.

12) Bezpieczny oznacza bezpieczny. Trzeba się upewnić, że połączenia w trakcie używania formularzy bądź połączenia HTTPS są bezpieczne. Należy weryfikować połączenia przez sprawdzanie certyfikatów bezpieczeństwa na witrynach internetowych. Trzeba zamykać przeglądarkę internetową po zakończeniu sesji; nie wystarczy jedynie zamknięcie karty bądź okna przeglądarki.

13) Poświęć czas na opracowanie polityki bezpieczeństwa. Należy we właściwy sposób wykorzystywać polityki bezpieczeństwa oferowane przez używany sieciowy system operacyjny.

- Gdy wszystkie wymienione powyżej wskazówki będą przestrzegane, sieć będzie dla intruzów trudniejszym celem.

- Polityki bezpieczeństwa w Windows Server mogą
  - blokować dostęp do zasobów na podstawie użytkowników lub grup,
  - uniemożliwiać instalację oprogramowania bądź sterowników urządzeń,
  - uniemożliwiać wykorzystywanie różnych klas urządzeń, blokować pulpit i przeglądarki internetowe,
  - Kontrolować dostęp do załączników poczty elektronicznej,
  - uniemożliwiać zapisywanie płyt DVD,
  - przeprowadzać kwarantannę sieciową,
  - ustalać działania związane z ochroną konta użytkownika
  - oraz przeprowadzać inne operacje.
- Prawdopodobnie około 40% z 2400 ustawień polityk w Windows Server dotyczy bezpieczeństwa. Inne sieciowe systemy operacyjne i produkty związane z politykami bezpieczeństwa, takie jak Novell ZenWare, także oferują szerokie możliwości konfiguracji.

Technologie NLA oraz NAP

- Istnieje tak wiele sposobów, na które sieć może zostać zaatakowana, że tym, co tak naprawdę trzeba mieć przygotowane do obrony przed zagrożeniami, jest adaptacyjna strategia sieciowa.
- Firma Microsoft opracowała kilka takich strategii i dostarcza je wraz z systemami Windows Server.
  - Pierwsza technologia to Network Location Awareness (NLA)- powoduje ona, że Windows Server ma możliwość wykrywania systemów, połączeń i stanu sesji oraz odpowiedniego zastosowania właściwej polityki względem klienta.

- W wielu przypadkach klient sieciowy używa polecenia ping albo wysyła pakiet ICMP w celu sprawdzenia, czy po drugiej stronie znajduje się zasób sieciowy, z którym można się połączyć.
- Kiedy laptop nawiązuje połączenie z domeną Windows, używając polecenia ping, to stanowi ono mechanizm, który domena wykorzysta w celu określenia stanu klienta.
- Dlatego jeżeli działanie polecenia ping zakończy się niepowodzeniem, domena nie będzie mogła zastosować swojej polityki grupy.
- Reagowanie na pakiet ICMP jest często wyłączane w zaporze sieciowej, więc ten mechanizm również nie będzie niezawodny w modyfikacji połączenia klienta.
- W celu rozwiązania tych problemów opracowano technologię NLA, a informacje klienta są wymieniane za pomocą połączenia VPN. W trakcie każdego odświeżania połączenia VPN odświeżeniu ulega również polityka grupy zarówno dla użytkowników, jak i komputerów.

- Wykorzystując technologię Network Location Awareness, w systemie klienta można wprowadzić następujące zmiany:
- Opcje mogą być ustawiane automatycznie na etapie PXE (ang. Pre-Execution Environment).
- Polityka grupy klienta może być uaktualniana automatycznie, kiedy nawiązuje on połączenie z domeną. Inne zdarzenia, na przykład połączenie urządzenia mobilnego, nawiązanie sesji VPN, wybudzenie klienta ze stanu hibernacji bądź wstrzymania lub przeniesienie systemu odizolowanego w kwarantannie do sieci produkcyjnej, również powoduje odświeżenie polityki grupy.
- Istnieje możliwość konfiguracji klientów na podstawie wykrytych zasobów. Jeśli karta interfejsu sieciowego nie zostanie wykryta, to sterownik dla tej karty nie będzie automatycznie wczytany. Zawieszenie wczytywania niepotrzebnych sterowników urządzeń powoduje skrócenie czasu rozruchu.
- Przepustowość łącza do klienta również może być częścią polityki, która jest stosowana, gdy klient nawiązuje połączenie z domeną.

- Istnieje także drugie podejście do ochrony sieci — Network Access Protection (NAP). Ono także opiera się na zarządzaniu zasobami na podstawie zdefiniowanych polityk. Mechanizm NAP sprawdza stan dostępnych klientów, kiedy próbują zalogować się do domeny. Zanim klient zostanie uwierzytelniony i otrzyma dostęp do połączenia sieciowego, mechanizm NAP próbuje określić, czy nastąpiło złamanie którejkolwiek z wymienionych poniżej polityk:
- zapora sieciowa klienta jest włączona;
- oprogramowanie antywirusowe i antyspyware'owe działa, jego definicje są aktualne, a skanowanie było przeprowadzone niedawno;
- zainstalowane zostały wszystkie aktualizacje udostępniane przez Microsoft;
- inne polityki charakterystyczne dla danej sieci.

- Niespełnienie tych warunków powoduje poddanie systemu kwarantannie aż do jego naprawienia i spełnienia przez niego wszystkich wymagań.
- NAP dostarcza dodatkowych kryteriów, których spełnienie jest wymagane do zagwarantowania, że bezpieczeństwo nie będzie naruszone z wewnątrz sieci.
- Technologia ta przedstawia nowy kierunek, który wiele sieciowych systemów operacyjnych zaadaptuje, aby sieci stały się bezpieczniejsze.

- Tego typu mechanizmy mogą być zmodyfikowane jako polityki systemowe stosowane następnie do określonych konfiguracji sieciowych.
- W poprawnie skonfigurowanej usłudze NAP oprogramowanie odpowiedzialne za politykę NAP jest obsługiwane przez serwery Health Requirement oraz Trusted Health Registration Authority.
- Obsługą identyfikacji i uwierzytelniania klientów zajmują się serwery usług katalogowych i certyfikatów. Kiedy klient NAP nie spełni wymagań polityki dotyczącej jego kondycji, zostanie zalogowany do oddzielnej podsieci, gdzie będzie zarządzany przez serwer naprawczy, który zajmie się jego mankamentami.

Bezpieczne protokoły w internecie

- Internet to niewątpliwie niebezpieczne środowisko. W większości przypadków każdy odbywający się w nim ruch sieciowy może być przechwycony i buforowany.
- W celu zagwarantowania poufności danych wysyłanych przez internet opracowano kilka różnych protokołów komunikacyjnych, dzięki którym można chronić dane.
  - IPsec,
  - Transport Layer Security (poprzednio Secure Sockets Layer),
  - HTTPS.

IPsec

- Internet Protocol Security (IPsec) to metoda szyfrowania i weryfikowania ruchu sieciowego wysyłanego przez sieci TCP/IP będąca standardem otwartym, zdefiniowanym w dokumencie IETF RFC 2401
- Zestaw protokołów zawiera bazujący na kluczu mechanizm szyfrujący do ustanawiania unikalnej identyfikacji punktów końcowych połączenia.
- W celu użycia IPsec oba węzły muszą mieć lokalnie uruchomiony ten protokół. Za pomocą protokołu IPsec można korzystać z emisji pojedynczej lub multiemisji.
- W trakcie multiemisji wszystkie węzły docelowe muszą współdzielić te same informacje bezpieczeństwa.

- IPsec może operować w dwóch trybach:
  - transportowym,
  - Tunelu.
- W trybie transportowym w pakiecie pozostaje oryginalny nagłówek IP w przeciwieństwie do trybu tunelu, gdzie nagłówek ten jest zamieniany na nowy, a oryginalny jest enkapsulowany.
- Tryb transportowy jest zazwyczaj stosowany w komunikacji pomiędzy urządzeniami końcowymi,
- tryb tunelu jest głównie stosowany do łączenia dwóch sieci. Tryb tunelu jest często używany w tworzeniu sieci VPN (ang. Virtual Private Network — wirtualna sieć prywatna).

- Istnieje również możliwość używania IPsec, kiedy tylko jeden punkt końcowy połączenia obsługuje protokół IPsec.
- W takim przypadku pakiet IPsec jest szyfrowany i enkapsulowany w routerze brzegowym (lub w innym zewnętrznym), a następnie deszyfrowany i wyodrębniany w routerze granicznym dla systemu docelowego.
- Po skonfigurowaniu IPsec w taki właśnie sposób ruch sieciowy jest widoczny dla obu punktów końcowych w sieci, ale bezpieczny po opuszczeniu podsieci, w której znajduje się system wysyłający pakiet.

- W modelu OSI IPsec jest protokołem warstwy sieciowej (poziom 3.), natomiast w modelu TCP/IP protokołem warstwy internetu.
- W zestawie protokołu IPsec najważniejsze są trzy protokoły:
- Authentication Header (AH). Protokół AH dostarcza mechanizm gwarantujący uwierzytelnianie i integralność pakietów IP w IPsec. W tym celu stosuje wartość kontrolną ICV (ang. Integrity Check Value), której wartość protokół AH oblicza, używając algorytmu kodującego oraz współdzielonego klucza. Wartość kontrolna ICV pełni taką samą funkcję jak sprawdzanie danych CRC. Odbiorca pakietu deszyfruje dane, uruchamia te same algorytmy i sprawdza, czy obliczona wartość kontrolna ICV jest taka sama jak w datagramie, co zapewnia uwierzytelnienie nadawcy.

- Encapsulating Security Payload (ESP). Protokół ESP szyfruje dane używane w komunikacji IPsec i zapewnia formę uwierzytelniania, integralności danych (wartość kontrolna ICV) oraz ochrony treści danych IPv4 lub IPv6. ESP można stosować w trybie tylko szyfrowania albo tylko uwierzytelniania, ale najczęściej włączone są obie funkcje. ESP w przeciwieństwie do AH nie zapewnia integralnej ochrony nagłówka IP.
- Internet Key Exchange (IKE) v1 oraz v2. Protokół IKE dostarcza mechanizm współpracy między dwoma punktami końcowymi połączenia, ustala dostępne protokoły bezpieczeństwa i określa, które z nich będą używane. Następnie przeprowadza szyfrowanie i tworzy klucze uwierzytelnienia wysyłane do systemu docelowego, aby wysyłany pakiet mógł być poprawnie zidentyfikowany i odszyfrowany. Protokół IKE został zdefiniowany w dokumencie IETF RFC 2409

- Do wymiany danych i negocjacji parametrów bezpieczeństwa (SA, ang. Security Association) IKE używa protokołu Internet Security Association and Key Management Protocol (ISCAMP).
- ISCAMP pozwala na obsługę różnych metod wymiany kluczy. Dwa najczęściej stosowane protokoły wymiany kluczy to OAKLEY i SKEME. Ten pierwszy jest najczęściej używany jako technologia wymiany kluczy w IKE, natomiast od drugiego (SKEME) IKE „pożycza” pewne funkcje, na przykład technologię szyfrowania klucza publicznego.

- Ponieważ IPsec operuje na tym samym poziomie co sam protokół IP, pozostaje niezależny od aplikacji i może być używany do bezpiecznego wysyłania pakietów z dowolnej aplikacji.
- Taka sytuacja nie ma miejsca w przypadku innych protokołów bezpieczeństwa, na przykład SSL, które operują na wyższych poziomach i wymagają od aplikacji wbudowania ich obsługi.

- IPsec negocjuje metodę stosowaną do przekazywania datagramów w danym formacie między punktami końcowymi.
- Dwa punkty końcowe wraz z wynegocjowaną polityką bezpieczeństwa są przechowywane w SA.
- Polityka bezpieczeństwa określa, które pakiety są zabezpieczane i kiedy wykorzystują protokół AH lub ESP.
- Algorytmy używane do szyfrowania oraz do uwierzytelniania są wybierane z listy, a następnie współdzielone, podobnie jak klucze niezbędne do odszyfrowania danych w obu procesach.
- Polityki są przechowywane lokalnie w bazie danych SPD (ang. Security Policy Database) każdego urządzenia.
- Natomiast SA są przechowywane w bazie danych SAD (ang. Security Association Database) każdego urządzenia.

- Wprawdzie IPsec jest komponentem opcjonalnym w komunikacji IPv4, jest jednak wymagany i stanowi zintegrowaną część IPv6

Zestaw protokołów Transport Layer Security

- Transport Layer Security (TLS) to zestaw protokołów kryptograficznych wykorzystywanych do szyfrowania danych wysyłanych na poziomie warstwy transportowej w sieci TCP/IP.
- Ten rozwijany standard został zdefiniowany w dokumencie IETF RFC 5246.
- TLS obsługuje nadzbiór doskonale znanego protokołu SSL (ang. Secure Socket Layer), opracowanego przez firmę Netscape i używanego przez wiele lat.
- Protokół SSL 3.0 był pierwszym protokołem sieciowym wybranym przez firmy obsługujące płatności przeprowadzane za pomocą kart internetowych do bezpiecznej obsługi transakcji w internecie.

- Protokół TLS zarówno szyfruje, jak i uwierzytelnia dane wysyłane z serwera do uwierzytelnionego klienta, tak więc zapewniane jest bezpieczeństwo komunikacji.
- Protokół ten jest najczęściej wykorzystywany w celu umożliwienia serwerom WWW komunikacji z klientami, na przykład przeglądarkami internetowymi.
- Jednak może być też stosowany w przypadku ruchu sieciowego TCP/IP, generowanego przez dowolne aplikacje.

- W swojej najprostszej postaci TLS używa serwera uwierzytelnionego oraz klienta nieuwierzytelnionego.
- Jeżeli została zainstalowana infrastruktura klucza publicznego (ang. Public Key Infrastructure — PKI), TLS można skonfigurować w taki sposób, aby oba punkty końcowe połączenia mogły być wzajemnie uwierzytelniane.

- Proces ten opiera się na trzech krokach:

1)Obsługa negocjacji protokołu. Klient wysyła do serwera TLS listę obsługiwanych metod szyfrowania oraz funkcji kodujących, serwer wybiera najmocniejszą. Krok ten określa się „uściskiem dłoni TLS” (ang. TLS handshake); może on być prostym procesem bez uwierzytelniania klienta.

2) Wymiana klucza i system pojedynczego bądź wzajemnego uwierzytelniania. Serwer zwraca klientowi certyfikat cyfrowy zawierający nazwę serwera oraz dane uwierzytelniające z centrum certyfikacji (ang. Certificate Authority, CA). Klient może zweryfikować te informacje w serwerze centrum certyfikacji.

3) Szyfrowanie symetryczne i uwierzytelnianie wiadomości. Klient szyfruje losowo wybraną liczbę za pomocą klucza publicznego serwera i wysyła ten klucz sesji serwerowi, gdzie będzie odszyfrowany za pomocą klucza prywatnego. Zarówno serwer, jak i klient powinny wygenerować losowe liczby, które następnie będą użyte przez różne algorytmy do wygenerowania odpowiednich kluczy.

- TLS obsługuje pewną liczbę różnych algorytmów kryptograficznych zarówno w celu tworzenia i wymiany klucza, jak i uwierzytelniania.
- Kiedy dwa punkty końcowe prowadzą negocjacje, dochodzi do wyboru algorytmu wymiany klucza oraz algorytmu uwierzytelniania.
- Uwierzytelnianie wiadomości obejmuje także użycie kodów uwierzytelniania wiadomości (ang. Message Authentication Code, MAC), które są tworzone za pomocą funkcji kryptograficznych.
- Z kolei SSL do utworzenia swoich kodów MAC wykorzystuje pseudolosową funkcję.
- Ogólnie rzecz ujmując, negocjacje TLS polegają na wyborze algorytmów z pakietu kryptograficznego.

- Aby aplikacja mogła używać TLS, musi mieć wbudowaną obsługę protokołu TLS.
- Wprawdzie protokół TLS jest stosowany przede wszystkim dla ruchu HTTP podczas transportu przez TCP, ale jest wykorzystywany również do zabezpieczania ruchu SMTP, FTP, NNTP oraz XMPP. OpenVPN.
- Innym obszarem, na którym TLS jest szeroko wykorzystywany, jest ruch VoIP (ang. Voice over IP), gdzie protokół sygnalizacyjny SIP (ang. Session Initiation Protocol) jest szyfrowany i uwierzytelniany.

- Dla wielu aplikacji pozbawionych obsługi TLS istnieją produkty firm trzecich enkapsulujące ruch TLS i transportujące go między punktami końcowymi.
- Jeden z takich programów to stunnel. Jest to działająca na wielu platformach bezpłatna (typu open source) aplikacja tunelowania TLS/SSL.
- Działa na zasadzie enkapsulacji danych do TLS i może używać infrastruktury PKI do tworzenia bezpiecznych połączeń.

Protokół HTTPS

- HyperText Transfer Protocol Secure (HTTPS) łączy w sobie protokół HyperText Transfer Protocol (HTTP) z protokołami Transport Layer Security (TLS) albo Secure Sockets Layer (SSL).
- Uwierzytelniony serwer WWW używa HTTPS w celu nawiązania bezpiecznego połączenia z przeglądarką inter netową klienta.
- Podczas nawiązywania połączenia w pasku adresu URL zamiast standardowego prefiksu http:// podaje się https://.
- O ile nie zostanie to zmodyfikowane, domyślnie ruch sieciowy HTTP będzie używał portu numer 443.

- Certyfikaty stosowane przez serwery WWW są certyfikatami klucza publicznego, które zostały utworzone przez oprogramowanie i wysłane do centrum certyfikacji w celu ich weryfikacji.
- Taki certyfikat jest cyfrowo podpisywany przez centrum certyfikacji, co oznacza, że każdemu zainteresowanemu dostarcza klucza publicznego niezbędnego do weryfikacji i sprawdzenia, czy informacje podawane przez serwer WWW są prawidłowe.
- Aby przeglądarka internetowa mogła zweryfikować certyfikat, musi dysponować podpisanym certyfikatem centrum autoryzacji. Ponieważ taka funkcja będzie bezużyteczna bez certyfikatów, certyfikaty większości głównych centrów certyfikacji są dostępne we wszystkich najważniejszych przeglądarkach internetowych.

- Firmy i użytkownicy prywatni mogą ustanawiać własne centra certyfikacji, ale będą one nadawały się jedynie do szyfrowania ruchu sieciowego, tak aby inni nie mogli podglądać danych.
- Certyfikat prywatny lub firmowy nie uwierzytelnia nadawcy. Jednak jeżeli firma wysyła dane ze swojego serwera WWW do swoich przeglądarek internetowych, to w takim przypadku certyfikat tej firmy potwierdzi prawdziwość nadawcy.
- Oprócz certyfikatów dla serwerów firmy mogą tworzyć certyfikaty dla klientów i umieszczać je w przeglądarkach internetowych poszczególnych użytkowników.
- Certyfikat klienta może zweryfikować w serwerze dane użytkownika bez konieczności jego logowania i pozwala serwerowi na sprawdzenie tej informacji podczas każdego połączenia z klientem.

Szyfrowanie i kryptografia

- Kryptografia to nauka o metodach szyfrowania (ukrywania) informacji.
- Związane z nią zagadnienia mieszczą się w obrębie zarówno informatyki, jak i matematyki.
- Istnieje wiele metod kryptograficznego zabezpieczania informacji, między innymi używanie haseł, biometryk lub innych urządzeń, szyfrowanie danych za pomocą algorytmów, używanie kluczy itp.

- Szyfrowanie oznacza proces przekształcania informacji na postać danych, które tracą swój kontekst.
- Deszyfrowanie to proces całkowicie odwrotny, to znaczy przekształcanie danych z powrotem na postać informacji, które mogą być odczytane i zrozumiane.
- Oba procesy, tj. dwa algorytmy odpowiedzialne za szyfrowanie i deszyfrowanie, nazywamy kodowaniem.
- Niektóre systemy kodowania wymagają używania klucza, który stanowi informację wykorzystywaną do modyfikacji operacji kodowania.
  - W takich przypadkach nadawca i odbiorca mogą współdzielić klucz publiczny, ale nie wymieniają kluczy prywatnych koniecznych do przeprowadzenia procesu kodowania. Aby zachować pełną poufność, klucz powinien być zmienny (to znaczy generowany na nowo w trakcie każdego użycia), w przeciwnym razie traci swoją możliwość ochrony kodu przed osobami z zewnątrz.
- Wszystkie wymienione elementy komunikacji — kodowanie, klucze i zaszyfrowane dane — są przedmiotem działania dla metod uwierzytelniających, które weryfikują, czy informacje zostały dostarczone prawidłowo, i ustalają źródło ich pochodzenia.

- Nowoczesne metody kodowania są wyjątkowo dobre i bardzo trudne do złamania. Trzy najlepiej znane algorytmy kryptograficzne stosowane w informatyce to:
  - Data Encryption Standard (DES)
  - Algorytm Diffie-Hellman Key Agreement
  - Algorytm klucza publicznego RSA

Kerberos

- Protokół Kerberos to system uwierzytelniania sieciowego, który bazuje na infrastrukturze klucza symetrycznego oraz zaufanym systemie firmy trzeciej.
- Na tej podstawie ustala tożsamość stron komunikacji i gwarantuje, że dane zostaną dostarczone bez ingerencji lub przejęcia.
- System Kerberos został utworzony w celu umożliwienia wysyłania danych przez niezabezpieczone połączenia (na przykład internet) przy jednoczesnym zagwarantowaniu, że nie zostaną podejrzane lub ponownie przetransmitowane jako część ataku z osobą pośrodku (ang. man-in-the-middle attack) lub ataku powtórzeniowego (ang. replay attack).
- Od chwili opracowania na uczelni MIT Kerberos został rozszerzony na wiele sposobów i zawiera uwierzytelnianie z użyciem algorytmu klucza asymetrycznego.

- Kerberos podczas uwierzytelniania działa w następujący sposób:

1)Klient loguje się do sieci, a informacje logowania są wysyłane do systemu lokalnego centrum bezpieczeństwa (ang. Local Security Authority, LSA).

2)System LSA przekazuje żądanie do usługi uwierzytelniania wraz z żądaniem uwierzytelnienia klienta przez LSA.

3)Żądanie jest przekazywane do polecenia Pobranie danych uwierzytelniających z systemu LSA, a system LSA wysyła klientowi odpowiednie dane uwierzytelniające.

4)Klient rozpoczyna sesję.

5) Bilet żądania dla danej aplikacji, sesji lub operacji jest przekazywany do LSA przez klienta, a następnie przesyłany dalej do serwera przyznającego bilety (ang. Ticket Granting Service, TGS). Bilet utworzony w TGS jest zwracany klientowi.

6) Żądanie jest przekazywane do serwera WWW w celu bezpiecznego pobrania informacji z systemu e-commerce.

7)Serwer WWW może przekazać żądanie do serwera E-Commerce, a następnie wysłać polecenie Pobranie danych uwierzytelniających do systemu LSA, który z kolei przekazuje żądanie do usługi certyfikatu (ang. Certificate Service).

8)Usługa certyfikatu wysyła dane uwierzytelniające do systemu LSA, który następnie wykonuje polecenie Zezwolenie na sesję.

9)Serwer WWW wysyła informacje żądane przez klienta.

- Nazwa „Kerberos” pochodzi od Cerbera (Cerberus), mitycznego trzygłowego psa, który strzegł Hadesu.
- Kerberos został opracowany jako część projektu Athena na uczelni MIT i po raz pierwszy pojawił się w wersji 4. w roku 1988.
- Wersja 5. pojawiła się w roku 1993 i została opublikowana przez IETF jako dokument RFC 1510.
- Standard MIT Kerberos jest dostępny bezpłatnie i wielu ważnych graczy w internecie, między innymi Sun Microsystems, Microsoft, Google, Apple oraz inne firmy, utworzyło konsorcjum Kerberos Consortium w celu kontynuowania prac w MIT nad tym standardem.
- Kerberos jest używany w wielu sieciowych systemach operacyjnych, takich jak Solaris, BSD UNIX, sieci Windows (od wersji 2000 wzwyż), Mac OS X czy Red Hat Linux (v.4 i późniejsze).

- Kerberos pierwotnie używał szyfrowania DES, co doprowadziło do tego, że władze Stanów Zjednoczonych zakazały eksportu tej technologii do innych krajów w ramach przepisów o zakazie eksportu uzbrojenia, obowiązujących do roku 2000.
- Windows Server 2000 to pierwszy ważniejszy sieciowy system operacyjny, który zawierał technologię Kerberos wraz z DES-56.
- Od tej chwili Microsoft korzysta z algorytmu RC4 w swoim szyfrowaniu Kerberos.
- Poza Stanami Zjednoczonymi opracowano inne wersje systemu Kerberos, które nie stosowały algorytmu DES. Do najbardziej znanych implementacji zaliczają się eBones i Heimdal.

- Kerberos używa dwóch protokołów komunikacji opracowanych przez Rogera Needhama i Michaela Schroedera.
  - Protokół Symmetric Key Protocol wykorzystuje algorytm szyfrowania symetrycznego w celu utworzenia klucza sesji między punktami końcowymi połączenia.
  - Protokół Public Key Protocol stosowany w systemie Kerberos służy do ustanowienia wspólnego uwierzytelnienia między punktami końcowymi.
- Zaufaną firmę trzecią w systemie Kerberos określa się mianem centrum dystrybucji kluczy (ang. Key Distribution Center, KDC);
  - jest ona umieszczona w dwóch oddzielnych usługach: serwerze uwierzytelniania (AS) oraz
  - serwerze przyznającym bilety (TGS).

- Bilety są rozpowszechniane w celu umożliwienia klientowi samoidentyfikacji w sesji.
- Centrum dystrybucji kluczy ma zbiór tajnych kluczy zapisanych w magazynie danych dla każdego węzła sieciowego.
- Tajny klucz jest znany tylko węzłowi oraz centrum dystrybucji kluczy, nikt inny go nie zna.
- Kiedy nawiązywane jest połączenie, centrum dystrybucji kluczy generuje klucz sesji używany do uwierzytelnienia punktów końcowych połączenia.

- Wprawdzie mechanizm Kerberos angażuje co najmniej osiem różnych wiadomości między klientem, serwerem przyznającym bilety i usługą serwera, ale wiadomości te pozwalają każdemu węzłowi w systemie zarówno na samoidentyfikację, jak i weryfikację wiadomości pochodzących z innego węzła.

- Sukces każdej operacji
  - logowania klienta,
  - uwierzytelniania klienta,
  - autoryzacji usługi klienta,
  - żądania usługi klienta
- zależy zarówno od dwóch wiadomości wymieniających bilety, jak i dopasowania kluczy sesji.
- Żadna wiadomość nie zawiera obu tych informacji. Kerberos powoduje obciążenie sieci, ale system jest bezpieczny.

- Kerberos jednak nie jest pozbawiony problemów. Jeden z nich to serwer przyznający bilety — to pojedynczy punkt systemu, który w przypadku awarii powoduje błędne działanie całości.
- Dlatego też trzeba umożliwić mu funkcjonowanie w przypadku awarii.

- Ponadto Kerberos zależy od znaczników czasu umieszczanych w wiadomościach na każdym etapie, więc wszystkie systemy muszą pozostać zsynchronizowane za pomocą usługi takiej jak NTP (ang. Network Time Protocol) lub WTS (ang. Windows Time Service).
- Kerberos może tolerować drobny brak synchronizacji, zwykle do około dziesięciu minut. Większa asynchroniczność prowadzi do tego, że bilety stają się nieważne.
- Wymienione czynniki można dostosować jako część polityk domeny oraz w ustawieniach mechanizmu Kerberos.

- Ostatnia niedogodność wiąże się z faktem, że serwer uwierzytelniania przechowuje wszystkie tajne klucze.
- Jeżeli ktoś uzyska dostęp do tego serwera, to bezpieczeństwo całej sieci będzie zagrożone.
- Na poziomie poszczególnych klientów złamanie systemu może doprowadzić do ujawnienia hasła klienta.
- Mimo to Kerberos jest obecnie najnowocześniejszą technologią uwierzytelniania sieciowego i usługą identyfikacji.

Zapory sieciowe

- W sieci komputerowej odpowiednikiem ściany przeciwpożarowej jest zapora sieciowa — bariera ochronna, którą stanowi zbiór procedur bezpieczeństwa izolujących i chroniących systemy danej sieci przed podejrzaną aktywnością.
- Może to być oddzielenie sieci za pomocą odrębnych urządzeń sprzętowych (fizycznych interfejsów sieciowych), zawierających wiele połączeń z siecią. Taki mechanizm nazywa się izolacją fizyczną.
- Zapora sieciowa może kontaktować się z siecią zewnętrzną, używając jednego protokołu sieciowego, natomiast z siecią wewnętrzną — za pomocą innego protokołu sieciowego. Określa się to izolacją protokołu.
- W dzisiejszych czasach posiadanie systemów połączonych z internetem bez żadnej zapory sieciowej jest bardzo nierozważne.

- Zapora sieciowa może być zarówno bardzo prosta, jak i niezwykle skomplikowana.
- Może być zaimplementowana w oprogramowaniu lub być oprogramowaniem zainstalowanym na dedykowanych serwerach i urządzeniach.
- Może działać w ramach używanego systemu operacyjnego, na przykład Linuksa, Uniksa lub Windows, albo być rodzajem „czarnego pudełka”, czyli samodzielną jednostką działającą pod kontrolą własnego systemu operacyjnego.

- Zapory sieciowe mogą być podzielone na następujące kategorie:
  - osobiste zapory sieciowe takie jak zapora sieciowa w systemie Windows, ZoneAlarm i inne,
  - zapory sieciowe w routerach,
  - sprzętowe zapory sieciowe zarówno proste, jak i bardzo skomplikowane,
  - zapory sieciowe w postaci proxy,
  - zapory sieciowe w postaci serwerów

- Zapora sieciowa najczęściej oferuje funkcje, które można zaliczyć do więcej niż tylko jednej z wymienionych kategorii.
- Podczas porównywania zapór sieciowych trzeba wziąć pod uwagę trzy czynniki: oferowane funkcje, wydajność (mierzoną przepustowością) oraz cenę.
- Zapory sieciowe to urządzenia sieciowe, dla których nie istnieją standaryzowane testy wydajności.
- Producenci wiedzą, że klienci używają zapór sieciowych na wiele różnych sposobów, i nie znoszą przedstawiania testów wydajności potencjalnym nabywcom.

Funkcje zapory sieciowej

- Niezależnie od natury zaimplementowanej zapory sieciowej jej działanie polega na stosowaniu zestawu filtrów ruchu sieciowego przechodzącego przez tę zaporę sieciową.
- Zapora sieciowa może przekazać dalej albo odrzucić dany ruch sieciowy.
- W modelu OSI zapora sieciowa może być filtrem warstwy sieci (warstwa 3.) bądź aplikacji (warstwa 7.) lub dowolnej warstwy między trzecią i siódmą.

- Wybrane funkcje, na które warto zwrócić uwagę podczas porównywania zapór sieciowych:
  - Filtrowanie pakietów. Operacja filtrowania pakietów odczytuje pola nagłówka pakietu IP i używa zdefiniowanych reguł w celu zezwolenia na ruch przychodzący do systemu lub zablokowania tego ruchu. Filtrowanie pakietów można również zastosować wobec ruchu wychodzącego.

- Filtry danych wejściowych interfejsu sieciowego. Filtry te blokują ruch sieciowy na podstawie parametrów takich jak źródłowy adres IP lub zakres adresów, numer portu czy użyty protokół.
- Mechanizm tłumaczenia adresów sieciowych (NAT). NAT to system konwersji, którego zadaniem jest zmiana źródłowych lub docelowych adresów IP, zazwyczaj również portów TCP/UDP w przepływających pakietach. Mechanizm NAT wykorzystuje tablice translacji i współpracuje z nieroutowalnymi w sieci publicznej sieciami prywatnymi. Mechanizm NAT to nie jest, ściśle rzecz biorąc, funkcja zapory sieciowej — znacznie częściej jest powiązany z routerami i serwerami proxy — jednak dostarcza technologię pozwalającą na ukrycie adresu IP systemów sieci prywatnej, co jest cenną funkcją.

- Stateful Inspection. Filtry typu Stateful Inspection przeprowadzają analizę wszystkich pakietów wychodzących i rejestrują ich adresy docelowe w tabeli stanu. Kiedy ruch sieciowy jest wysyłany z powrotem z systemu zewnętrznego, zapora sieciowa używa tabeli stanu w celu określenia, czy pakiety powinny być przekazywane. Ogólna reguła jest taka, że filtry typu Stateful Inspection są o wiele większym obciążeniem dla zapory sieciowej i działają znacznie wolniej niż statyczne filtrowanie pakietów.

- Analiza połączeń. W filtrze tego typu sesje są zarządzane, zamiast po prostu odwoływać się do pakietów lub połączenia w tabeli stanu. Sesje wymagają żądania pochodzącego z systemu znajdującego się za zaporą sieciową i mogą obsługiwać aplikacje tworzące wiele połączeń. Protokoły z wieloma połączeniami obejmują między innymi sesje HTTP przeglądarki internetowej, pobieranie plików za pomocą FTP oraz strumieniowanie multimediów.
  - Funkcja analizy połączeń znacznie utrudnia przeprowadzenie udanego ataku typu IP spoofing (fałszowanie źródłowego adresu IP), DoS (ang. Denial of Service — odmowa usług) i prób rozpoznania sieci. Filtry powiązane z funkcją analizy połączeń stanowią mniej efektywną ochronę przed atakami typu DoS.

- Zapora sieciowa w postaci proxy. Zapora sieciowa w postaci proxy działa w charakterze pośrednika między klientem znajdującym się wewnątrz zapory sieciowej i systemem lub serwerem na zewnątrz. Między obiema stronami nie ma bezpośredniego połączenia przez zaporę sieciową. Zapora sieciowa w postaci proxy tworzy dwa oddzielne połączenia, po jednym dla każdej strony zapory sieciowej. Klient wewnątrz komunikuje się jedynie z proxy, które z perspektywy klienta jest jego punktem docelowym. Serwer proxy może zwiększyć wydajność działania przez buforowanie najczęściej lub ostatnio używanych danych. Ma również możliwość weryfikacji protokołów przekazywanych przez zaporę sieciową. Pozwala także na zarządzanie w taki sposób, aby żądania były przekazywane na bazie identyfikatora użytkownika i (lub) członków grupy.

- Filtrowanie aplikacji. Filtrowanie na poziomie aplikacji to technologia tzw. Głębokiej analizy pakietów (ang. deep packet inspection). Metoda ta jest najbardziej skomplikowana i najwolniejsza z wymienionych na tej liście. Filtry tej metody analizują pakiety pod kątem zawartych w nich danych, a następnie modyfikują je, jeśli zachodzi taka potrzeba.

Bramy bezpieczeństwa

- Brama jest urządzeniem warstwy aplikacji (warstwa 7.) działającym w charakterze interfejsu między sieciami.
- Bramy mogą być zaimplementowane jako urządzenia sprzętowe bądź jako oprogramowanie.
- Pojęcie „brama” jest ogólne i generalnie oznacza występowanie pewnego rodzaju konwersji protokołów.
- W warstwie aplikacji brama musi przekształcać jeden rodzaj pliku na inny, w warstwie prezentacji konwersja może zastępować dany rodzaj szyfrowania innym lub wykonywać inne funkcje.
- Bramy mogą przeprowadzać konwersje na poziomie transportowym (warstwa sieci) z IP na AppleTalk.
- Ogólnie rzecz ujmując, brama to urządzenie, które może działać na dowolnym poziomie modelu OSI. W wyniku tego bardzo często można się spotkać z bramami opisywanymi jako „brama pocztowa”, „brama WWW” lub nawet „brama bezpieczeństwa”.

- Aby brama mogła funkcjonować między sieciami, bardzo często musi mieć możliwość działania jako router dostarczający funkcji mapowania adresów.
- Bardzo często bramy pełnią funkcję serwera proxy lub zapory sieciowej.

Domyślnie odmawiaj

- Standardową regułą używaną przez każdą technologię zapewniającą wysoki poziom bezpieczeństwa jest inicjalizacja urządzenia wraz ze stanem domyślnie odmawiaj.
- Wiele zapór sieciowych, serwerów proxy oraz innych systemów bezpieczeństwa jest standardowo dostarczanych w postaci całkowicie zamkniętej.
- Może to wywołać zdziwienie u kogoś, kto wcześniej nie spotkał się z taką sytuacją. W przypadku całkowicie zamkniętego systemu zaleca się, aby administrator włączał jednorazowo po jednej wymaganej usłudze.

- Typowe jest stosowanie poniższej sekwencji reguł:
  - **Odrzucaj każdy ruch sieciowy, chyba że istnieje odpowiednia reguła, która dopuszcza ten rodzaj ruchu.** To jest właśnie stan domyślnie odmawiaj.
  - **Zablokuj wszystkie pakiety przychodzące z adresami sieci wewnętrznej oraz wszystkie pakiety wychodzące z adresami zewnętrznymi.** Wymienione pakiety zwykle pochodzą od atakujących bądź są błędne.
  - **Skonfiguruj ruch sieciowy DNS odpowiednio dla zapytań DNS bazujących zarówno na UDP, jak i TCP.** Bez usługi rozpoznawania adresów większość innych funkcji sieci nie będzie działała.

  - Należy zezwalać na ruch sieciowy HTTP i prawdopodobnie na HTTPS przez otworzenie portu numer 80 oraz odpowiednie przekierowanie tego ruchu.
  - Jeżeli używane są serwery poczty, to należy włączyć SMTP i (lub) POP3 przez otworzenie ich portów.
  - Należy odpowiadać na prośby o pomoc kierowane przez otwieranie poszczególnych portów lub tras po sprawdzeniu tych próśb i upewnieniu się, że funkcje sieciowe wymagają tego rodzaju dostępu
- Wymienione reguły są stosowane w kolejności od początku listy.