BEZPIECZEŃSTWO SIECI KOMPUTEROWYCH

PRAKTYCZNE PRZYKŁADY I ĆWICZENIA W SYMULATORZE CISCO PACKET TRACER

JERZY KLUCZEWSKI

iTst@rt

Książka **Packet Tracer – Bezpieczeństwo w sieciach teleinformatycznych**, dedykowana jest wszystkim osobom chcącym nauczyć się projektowania i tworzenia bezpiecznych sieci komputerowych.

Książka jest zbiorem ćwiczeń uzupełniających wiedzę (teoretyczną oraz praktyczną) dotyczącą **bezpieczeństwa sieci teleinformatycznych wg programu kształcenia Cisco Academy** oraz w oparciu o możliwości programu Packet Tracer w wersji **7.1.1**.

Książka zawiera materiał poświęcony klasyfikowaniu zagrożeń w sieciach, zasadom obrony sieci przed atakami, założeniom polityki bezpieczeństwa, protokołom SSH, NTP, SYSLOG, RADIUS, TACACS+, GRE, IPsec, usługom AAA a także problemom związanym z prawem ogólnego rozporządzenia o ochronie danych osobowych RODO (GDRP).

Istotną zaletą książki są załączone gotowe rozwiązania w postaci plików PKT oraz PKA, zawierających prawidłowe rozwiązania przykładów i ćwiczeń.

Zastrzeżonych nazw firm, organizacji i produktów użyto w książce wyłącznie do ich identyfikacji.

Projekt okładki: ***Daniel Pliszka***

Redakcja i skład: ***Marcin Kaim i Marek Smyczek,***

Wydawnictwo informatyczne

http://www.itstart.pl

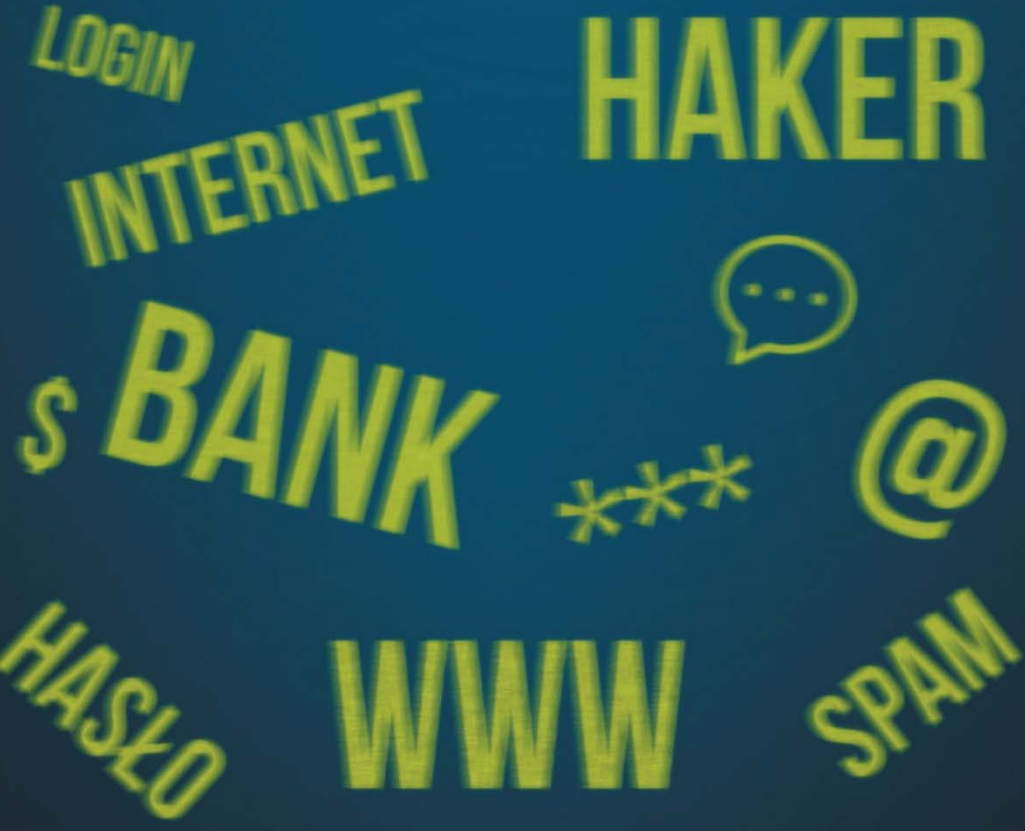
email: itstart@itstart.pl

Niniejszą publikację opracowano w celach promowania programu CISCO w Polsce oraz jako podręcznik ułatwiający przyswajanie treści praktycznych związanych z sieciami komputerowymi.

ISBN 978-83-65645-09-8

Wydanie pierwsze – Piekary Śląskie 2019

SPIS TREŚCI



1 | WSTĘP

1 Wstęp

Autor i Wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Ponadto autorzy nie ponoszą żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Chcąc ułatwić naukę i poznawanie sieci, autor siódmej części książki poświęconej bezpieczeństwu sieci, przygotował liczne przykłady i ćwiczenia, wspomagające proces nauczania. Jednak nie zostały one umieszczone na żadnym nośniku dołączonym do książki, lecz opublikowaliśmy je na specjalnej stronie internetowej naszego wydawnictwa, pod adresem: http://security.itstart.pl. Chcąc uzyskać pełny dostęp do plików, należy się zalogować przy pomocy loginu: **sec** i hasła: **qwAS78&***

Pliki zostały podzielone na trzy kategorie: **Przykłady**, **Ćwiczenia**. Pliki znajdują się podkatalogach:

- przykłady
- ćwiczenia

Uwaga 1: Aby móc je otworzyć i używać, musisz mieć zainstalowaną wersję programu Packet Tracer **7.1.1**.

Uwaga 2: W trakcie edycji niniejszej książki firma Cisco Systems opublikowała wersję programu Packet Tracer **7.2 - Wydawca oraz autor nie odpowiadają za niewłaściwe działanie plików w nowszych wersjach programu Packet Tracer.**

2 | PODSTAWOWE DEFINICJE I ZAGROŻENIA

2 Podstawowe definicje i zagrożenia

W tym rozdziale przedstawiono podstawowe definicje oraz klasyfikacje dotyczące problematyki bezpieczeństwa w sieciach oraz systemach gromadzących dane. Pojęcie systemu rozumiane jest tutaj ogólnie, czyli dotyczy ono serwerów, komputerów stacjonarnych, urządzeń mobilnych oraz typowych urządzeń sieciowych takich jak przełączniki, routery, zapory sieciowe.

Bezpieczeństwo systemu (*ang. system security*) przesyłającego lub gromadzącego dane to taki stan systemu, w którym ryzyko powstania zagrożenia dla jego prawidłowego działania jest ograniczone do pewnego akceptowalnego poziomu. Z tej definicji wynika, że w obecnej cyberprzestrzeni nie istnieją systemy w 100% bezpieczne.

Dlatego zadaniem administratorów jest nieustanne poprawianie polityki i technik zabezpieczeń w celu ochrony systemów i gromadzonych danych przed nieautoryzowanym ich wykorzystaniem, uszkodzeniem lub zniszczeniem.

Identyfikator użytkownika (*ang. user id*) – ciąg znaków literowych, cyfrowych lub innych jednoznacznie określających osobę upoważnioną do przetwarzania danych w systemie (najczęściej nazywany **loginem**).

Hasło (*ang. password*) – ciąg znaków literowych, cyfrowych lub innych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym.

Poufność informacji (*ang. confidentiality*) – informacje ujawniane są wyłącznie uprawnionym podmiotom oraz na potrzeby określonych procedur, w dozwolonych przypadkach i w dozwolony sposób.

Uwierzytelnianie osoby (*ang. authentication of person*) – cecha gwarantująca, że osoba korzystająca z systemu jest rzeczywiście tą, za którą się podaje.

Uwierzytelnianie informacji (*ang. information authentication*) – cecha gwarantująca, że informacja rzeczywiście pochodzi od źródła, które jest w niej zawarte.

Integralność informacji (*ang. integrity*) – cecha danych oznaczająca ich gromadzenie danych dokładnych i kompletnych.

Raportowanie (*ang. reporting*) – cecha systemu informatycznego polegająca na tym, że może on gromadzić operacje aktywności użytkowników oraz operacje wykonywane na danych.

Publiczna sieć telekomunikacyjna (*ang. telecommunications network*)

(definicja 1) Sieć telekomunikacyjna nie będąca siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych (*Prawo telekomunikacyjne – ustawa z dnia 21 lipca 2000 r.*)

(definicja 2) Systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju; wykorzystywane są one głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych (*Prawo telekomunikacyjne - ustawa z dnia 16 lipca 2004 r.*).

Patrz:

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2014 r.
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Dział 1. Rozdział 1. Art. 2. Punkt 29 (strona 8).

Pliki zawierające wspomniane akty prawne:

- p2-1-rozporzadzenie_mswa_dziennik_ustaw_poz_1024.pdf
- p2-1-prawo_telekomunikacyjne_ustawa_16_07_2004.pdf

2.1.1 Podstawowa klasyfikacja zagrożeń

Rodzaje zagrożeń dla bezpieczeństwa współczesnych sieci można sklasyfikować na różne sposoby. W tym podrozdziale pogrupowano rodzaje zagrożeń, wg: przyczyn, miejsca powstawania, czynników socjologicznych (tzw. oszustwa internetowe), oraz zagrożenia fizyczne i logiczne (jako typowe ataki sieciowe).

2.1.2 Zagrożenia wg przyczyn

- świadoma, celowa, destrukcyjna działalność człowieka (np. szpiegostwo, wandalizm, terroryzm, ambicje hakerów, zemsta, szantaż, sabotaż),
- nieświadoma działalność człowieka (np. błędy ludzkie, nieprzestrzeganie procedur),
- wydarzenia losowe (np. awarie sprzętu i wady oprogramowania, pożar, zalanie wodą, awaria zasilania, katastrofy, klęski żywiołowe, wyładowania atmosferyczne).

2.1.3 Zagrożenia wg miejsca powstawania

- wewnętrzne, powstające wewnątrz organizacji będącej właścicielem systemu (np. nieświadomość odpowiedzialności za powierzony obszar bezpieczeństwa, nieodpowiedzialne żarty robione kolegom, zemsta pracownika na przełożonym),
- zewnętrzne, powstające w sieci publicznej (np. próby włamania z sieci Internet za pomocą wirusów, robaków, hacking, oszustwo, sabotaż, piractwo).

2.1.4 Zagrożenia wg czynników socjologicznych (tzw. oszustwa internetowe)

Inżynieria społeczna, ***inżynieria socjalna***, ***socjotechnika*** *– zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę. Hackerzy często wykorzystują niewiedzę bądź łatwowierność użytkowników systemów informatycznych, aby pokonać zabezpieczenia odporne na wszelkie formy ataku. Wyszukują przy tym najsłabszy punkt systemu bezpieczeństwa, którym jest człowiek.*

Źródło: https://pl.wikipedia.org/wiki/Inżynieria_społeczna_(informatyka)

Zagrożenie to polega głównie na uzyskiwaniu informacji bezpośrednio od ludzi nie mających pojęcia, że podali hakerowi istotne dane, czyli osobie wykorzystującej następujące socjotechniki.

Główne rodzaje socjotechnik stosowanych w sieci to:

- **Niechciane informacje** (*ang. spam*) – niepotrzebne wiadomości elektroniczne. Najczęstsze kategorie spamu to: ***Unsolicited Commercial Email*** (UCE) – niezamawiana oferta handlowa, spam komercyjny o charakterze reklamowym, zakazany przez prawo polskie i dyrektywę UE oraz ***Unsolicited Bulk Email*** (UBE) – niezamawiana poczta masowa, maile o charakterze często niekomercyjnym, takie jak apele organizacji społecznych i charytatywnych czy partii politycznych, prośby o pomoc czy masowe rozsyłanie ostrzeżeń, np. o wirusach komputerowych (*Źródło: https://pl.wikipedia.org/wiki/Spam*).
- **Wyłudzanie informacji** (*ang. phishing*) – przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań.

2.1.5 Zagrożenia fizyczne

Zagrożenia fizyczne polegają na fizycznej obecności intruza w obszarze chronionym lub/oraz kradzieży zasobów informacyjnych za pomocą bezpośredniego fizycznego dostępu.

Zagrożenie fizyczne może przybierać następujące formy:

- przebywanie osób nieuprawnionych w obszarze chronionym (np. w serwerowni),
- otwarcie drzwi do chronionego obszaru lub poruszanie się w chronionym obszarze,

2.1.6 Zagrożenia wirusami, robakami oraz typowe ataki sieciowe

Zagrożenia związane z wirusami, robakami oraz typowymi atakami sieciowymi zostały opisane na następnym podrozdziałach.

2.2 Zagrożenia związane z działaniem wirusów i robaków

Co to jest **wirus**?
Wirus to złośliwy kod (program), który dołącza się do innego programu w celu wykonania konkretnych niepożądanych operacji w komputerze (hoście).

Co to jest **robak**?
Robak to złośliwy kod, który instaluje swoje kopie w pamięci zainfekowanego komputera. Zainfekowany komputer rozsyła robaka do innych komputerów (hostów).

Główne różnice między działaniem wirusa i robaka polegają na tym, że:

- wirus wymaga programu użytkownika do uruchomienia,
- robak może działać samodzielnie i rozprzestrzeniać się w sieci,

Robaki to samodzielne programy atakujące system poprzez wykorzystanie luki. Po pomyślnym wejściu do systemu, robak kopiuje się z hosta atakującego do nowego hosta i cykl zaczyna się od nowa.

Wyróżniamy pięć podstawowych faz ataku robaka:

1. **Próbowanie (***ang. Probe phase***)** - Celem jej jest znalezienie komputerów, które mogą być zaatakowane. Przykładowe techniki: użycie protokołu Internet Control Message Protocol (ICMP) w celu tworzenia mapy sieci, skanowanie i identyfikacja systemów operacyjnych, pozyskiwanie haseł przy użyciu socjotechniki, atak słownikowy, brute-force, sniffing.

2. **Penetracja (***ang. Penetrate phase***)** - kod exploit jest transferowany do podatnych na atak hostów. Następnie kod wykonuje się wykorzystując, np. przepełnienia bufor lub uruchamia wirusa.

3. **Instalowanie (***ang. Persist phase***)** - po udanym ataku z, kod próbuje zainstalować się w systemie docelowym tak, aby kod atakujący został uruchomiony po ponownym uruchomieniu systemu (modyfikacja systemu plików, rejestru).

4. **Propagowanie (***ang. Propagate phase***)** - atakujący kod próbuje przenieść atak do innych celów, szukając słabo zabezpieczonych sąsiednich hostów wykorzystując kopie list mailowych, przesyłanie plików do innych systemów wykorzystujących udziały plików lub usługę FTP lub przesyłanie plików przez Internet Relay Chat (IRC), wysłanie wiadomości do przyjaciół z facebooka.

5. **Paraliżowanie (***ang. Paralyze phase***)** - faktyczne szkodliwe działanie w systemie: usunięcie plików, poważne uszkodzeni systemu, kradzież informacji, wykonanie DoS lub DDoS.

2.3 Rodzaje typowych ataków sieciowych

2.3.1 Ataki pasywne i aktywne

2.3.1.1 Pasywne

Ataki pasywne polegają na podsłuchiwaniu, monitorowaniu lub analizowaniu przesyłanych jawnie komunikatów sieciowych. Celem osoby atakującej jest zdobycie treści komunikatu. Ataki pasywne mogą działać na dwa sposoby:

1. Wykrywanie treści komunikatu.
2. Przechwycenie i analiza komunikatu.

Drugi sposób ataku pasywnego polega na analizie przesyłanych komunikatów. wyszukiwaniu danych krytycznych i tożsamości komputerów wymieniających informacje, badaniu długości komunikatów i częstości, z jaką są wysyłane.

2.3.1.2 Aktywne

Ataki aktywne. Polegają one na modyfikowaniu strumienia danych lub tworzeniu danych fałszywych i dzielą się na cztery typy: maskarada, powtórka, modyfikacja komunikatów, blokowanie działania.

2.3.2 Pozostałe typy ataków

2.3.2.1 Ataki typu Rekonesans/Rozpoznanie (ang. Reconnaissance)

Ataki rozpoznawcze obejmują nieuprawnione wykrycie i mapowanie systemów, usług lub luk. Atak ten często wykorzystuje programy typu sniffer pakietów i skaner portów, które są powszechnie dostępne do bezpłatnego pobrania z Internetu np. **Wireshark**.

Atak typu **Reconnaissance** jest również znany jako zbieranie informacji i w większości przypadków, poprzedza dostęp lub ataku DoS. W ataku rozpoznawczym, złośliwy intruz zazwyczaj rozpoczyna się od przeprowadzenia tzw. **sweep ping** sieci docelowej, aby określić, które adresy IP są aktywne. Intruz następnie określa, które usługi lub porty są dostępne aktualnie na danych adresach IP.

Najbardziej popularna aplikacja do wykonywania skanowania portów to **Nmap**. Pozwala na uzyskanie takich informacji jak: nr portu, typ, wersja systemu aplikacji.

Używane narzędzia do ataku to:

- packet sniffers
- ping sweeps (skanowanie adresów IP w sieci)
- port scanning (skanowanie portów)
- internet information queries

Packet Sniffer to aplikacja, która korzysta z karty sieciowej w trybie mieszanym, aby wychwycić wszystkie pakiety sieciowe, które są przesyłane w sieci LAN.

Tryb nasłuchiwania (*ang. promiscuous mode*) – tryb nasłuchiwania, tryb mieszany to tryb pracy interfejsu sieciowego (np. ethernetowej karty sieciowej), polegający na odbieraniu całego ruchu docierającego do karty sieciowej, nie tylko skierowanego na adres MAC karty sieciowej. Aby przestawić kartę sieciową w tryb **nasłuchiwania** w systemie Linux należy wykonać w terminalu polecenie:

```
ifconfig <karta_sieciowa> promisc
```

2.3.2.2 Ataki typu skanowanie za pomocą ping (ang. ping sweep)

Ping sweep jest podstawową techniką skanowania sieciowego, która określa, jaki zakres adresów IP jest aktualnie aktywny w sieci. Składa się ona z poleceń ping (ICMP)

wysyłanych do wielu hostów. Jeśli dany adres jest aktywny, to zwraca odpowiedź **ICMP echo**.

2.3.2.3 Ataki typu skanowanie portów (ang. port scanning)

Każda usługa na komputerze wiąże się z określonym numerem portu. **Skanowanie portów** jest skanowaniem zakresu portów TCP i UDP na komputerze w celu wykrycia **potencjalnych luk w zabezpieczeniach**, **usług, rodzaju systemu operacyjnego**. Jeśli nadawca otrzyma odpowiedź z portu to znaczy, że port jest używany.

Hakerzy mogą sprawdzić charakterystyki aktywnych aplikacji, co daje im konkretne informacje, które są przydatne do złamanie usługi.

2.3.2.4 Ataki dostępowe (ang. access attacks)

Ataki dostępowe wykorzystują znane luki w zabezpieczeniach usługi uwierzytelniania, usługi FTP i usługach internetowych w celu uzyskania dostępu do kont internetowych, poufnych baz danych i innych poufnych informacji. Atak dostępowy może być wykonywany na wiele różnych sposobów. Atak ten często używa ataku słownikowego do odgadnięcia haseł systemowych. Istnieją wyspecjalizowane słowniki dla poszczególnych języków, które mogą być stosowane.

Ataki w celu uzyskania hasła mogą być realizowane przy użyciu kilku metod: ***brute-force, konie trojańskie, spoofing IP i sniffer pakietów***.

Jednak większość ataków na hasła odnosi się do metody brute-force, która obejmuje powtarzające się próby oparte na wbudowanym słowniku, do identyfikacji konta lub hasła.

Atak brute-force jest często wykonywany za pomocą programu, który działa w sieci i próbuje zalogować się do wspólnego zasobu, np. serwera. Po osoba atakująca uzyska dostęp do zasobu, atakujący ma takie same prawa dostępu jak użytkownik, którego konto zostało naruszone. Jeśli konto ma wystarczające uprawnienia, atakujący może utworzyć tzw. tylne drzwi dla przyszłych dostępów.

Typy ataków dostępowych:

- **Password attack** – atakujący próbuje zgadnąć hasło, wykorzystuje atak słownikowy. Ataki na hasła mogą być implementowane jako brute-force, Trojan Horse, lub Packet Sniffer.
- **Trust exploitation** – atakujący wykorzystuje przywileje do systemu w nieautoryzowany sposób, co może prowadzić do pogorszenia bezpieczeństwa systemu.

- **Port redirection** – zainfekowany system jest używany jako miejsce przygotowane do przekierowania ataków na inne cele.
- **Man-in-the-middle attack** – atakujący znajduje się pomiędzy dwoma urządzeniami w sieci tak, aby móc czytać i modyfikować dane przechodzące między tymi urządzeniami. Oczywiście urządzenia nie mogą wiedzieć o jego istnieniu. Na przykład użycie laptopa jako nielegalnego punktu dostępowego, aby przejąć ruch sieciowy kierowanego do użytkownika docelowego.
- **Buffer overflow** – działanie programu, który zapisuje dane buforze pamięci. Przepełnienie bufora zazwyczaj powstaje w wyniku błędu programie napisanym w C lub C ++. Wynikiem przepełnienia jest to, że ważne dane są zastępowane innymi umożliwiającymi wykonanie złośliwego kodu.

2.3.2.5 Ataki typu DoS (ang. Denial of Service)

Ataki typu DoS wysyłają bardzo dużą liczbę żądań przez sieć lub Internet. Te żądania powodują, że serwery usług nie nadążają z odpowiedziami. Powoduje to awarie aplikacji i serwerów.

Atak DoS jest to atak sieciowy, który powoduje przerwę w świadczeniu usług dla użytkowników, urządzeń lub aplikacji. Najprostszą metodą jest generowanie dużych ilości tego, co wydaje się ważnym ruchem w sieci.

Główne objawy ataku DoS to:

- Host lub aplikacja nie obsługuje nieoczekiwanych żądań, złośliwie sformatowanych danych wejściowych, nieoczekiwane interakcje elementów systemu lub wyczerpanie zasobów.
- Sieć, host lub aplikacja nie jest w stanie obsłużyć ogromnej ilości danych, co powoduje awarię systemu lub bardzo wolne jego działanie.

2.3.2.6 Ataki typu DDoS (ang. Distributed Denial of Service)

Atak Distributed Denial of Service (**DDoS**) jest podobny do ataku DoS, z tym, że atak DDoS generowany jest z wielu skoordynowanych źródeł.

Typy ataków DDoS:

- **Ping of Death** – Hacker wysyła żądanie echa większego niż maksymalna wielkość pakietu z 65535 bajtów. Wysłanie polecenia ping o tej wielkości może spowodować zawieszenie komputera docelowego.

- **Smurf Attack** – Atakujący wysyła dużą liczbę żądań ICMP skierowanych do adresów rozgłoszeniowych (*ang. broadcast addresses*) z fałszywych adresów źródłowych w tej samej sieci. Atak ten polega na technice fałszowania zapytań ping (*ICMP Echo Request*), poprzez zamianę adresu źródła tych zapytań na adres atakowanego serwera. Tak spreparowane pakiety ping, wysyłane są na adres rozgłoszeniowy sieci zawierającej wiele komputerów. Pakiety zostają rozesłane do wszystkich aktywnych systemów w sieci, co powoduje przesłanie przez nie pakietów *ICMP Echo Reply* na sfałszowany wcześniej adres źródłowy atakowanej ofiary.

Smurf attack wysyła wiele żądań ICMP na adresy rozgłoszeniowe (broadcast addresses) ze źródłowego adresu sfałszowanego w danej sieci.

- **TCP SYN Flood** – Atak polega na wysyłaniu dużej ilości pakietów z ustawioną w nagłówku flagą synchronizacji (SYN) i najczęściej ze sfałszowanym adresem IP nadawcy (IP spoofing). Pakiety TCP z ustawioną flagą SYN służą do informowania zdalnego komputera o chęci nawiązania z nim połączenia. Podczas takiego ataku serwer, który otrzymał pakiet z flagą SYN na port, który jest otwarty, odpowiada na każdy pakiet zgodnie z zasadami protokołu TCP wysyłając pakiet z ustawionymi flagami synchronizacji (SYN) i potwierdzenia (ACK) do komputera, który w tym wypadku nie istnieje, istnieje, ale nie zamierzał nawiązywać połączenia z atakowanym hostem lub jest to komputer atakującego, który specjalnie nie odpowiada. Powoduje to przesyłanie dużych ilość danych i obciąża łącze sieciowe.

  Oprócz odpowiedzi na pakiety SYN atakowany komputer zapisuje w tablicy stanów połączeń informację, że nastąpiła próba połączenia i wysłano potwierdzenie (pakiet z flagami SYN i ACK). Tablice te są przechowywane w pamięci RAM, a ich wielkość jest ograniczona. Jeżeli taki atak będzie powtarzany a liczba takich pakietów będzie bardzo duża, w pewnym momencie nastąpi przepełnienie tablicy połączeń atakowanej maszyny co spowoduje, że ów komputer nie będzie akceptował następnych przychodzących połączeń. Serwer wówczas będzie cały czas w stanie oczekiwania na pakiety ACK, które nigdy nie nadejdą.

  Ciągły atak SYN flooding powoduje zaprzestanie odpowiadania na nowe zapytania. Jak również spowalnia obsługiwanie otwartych połączeń poprzez znaczny wzrost zapotrzebowania na zasoby komputera (przede wszystkim pamięć). W skrajnym przypadku może spowodować zawieszenie systemu.

Ataki TCP SYN flood, Ping of Death oraz Smurf mogą spowodować następujące uszkodzenia:

- Zużycie zasobów, takich jak przepustowość, miejsce na dysku lub czas procesora.
- Zakłócenie informacji konfiguracyjnych, takich jak informacje o routingu.
- Zakłócenie informacji publicznej, takich jak resetowanie sesji TCP.
- Zakłócenia fizycznych składników sieci.
- Utrudnianie komunikacji między ofiarą i innymi hostami.

Zwykle nie jest trudno ustalić, czy występuje atak DoS. Należy jednak pamiętać, że ataki DoS mogą być elementem większej ofensywy. Ataki DoS mogą prowadzić do problemów w segmentach sieci na atakowanych komputerach.

Przykładowe symptomy ataku DoS:

- Bardzo duże spowolnienie sieci, przy dostępie do stron www lub otwieraniu plików.
- Brak dostępu do poszczególnych stron www.
- Brak dostępu do dowolnej strony www.
- Dramatyczny wzrost liczby spamu w skrzynce pocztowej (mail bomb).

2.4 Ogólne zasady obrony sieci przed atakami

Poniższe porady opierają się na materiałach szkoleniowych firmy Cisco Systems oraz są jedynie punktem wyjścia do prawidłowego zarządzania bezpieczeństwem. Organizacje oraz przedsiębiorstwa muszą zachować czujność w każdej chwili i w każdym miejscu, aby modyfikować swoje zabezpieczenia wobec zmieniających się ciągle zagrożeniach.

1. Instaluj aktualne łatki (patche) co tydzień lub codziennie, jeśli to możliwe, w celu uniknięcia przepełnienia bufora i ataków dot. przekroczenia uprawnień.
2. Wyłącz niepotrzebne usługi i porty.
3. Używaj silnych haseł i zmieniaj je często.
4. Kontroluj fizyczny dostęp do systemów i urządzeń.
5. Ograniczaj zbędny kod Twojej strony. Niektóre strony internetowe pozwalają użytkownikom na wpisanie nazwy użytkownika i hasła. Haker może wpisać zamiast nazwy użytkownika, polecenia wykonania skryptu, co może doprowadzić do usunięcia systemu plików z serwera. Programiści PHP powinni

ograniczyć znaki przyjmowane na wejściu, aby nie przyjmować niedozwolonych znaków takich jak |; <>.
6. Na bieżąco wykonuj kopie zapasowe i testuj kopie zapasowych plików.
7. Kształć pracowników o zagrożeniach związanych z inżynierią społeczną oraz opracuj strategię sprawdzenia tożsamości przez telefon, za pośrednictwem poczty elektronicznej lub osobiście.
8. Używaj szyfrowania oraz haseł do ochrony poufnych danych.
9. Wdrażaj sprzęt bezpieczeństwa i oprogramowanie: zapory sieciowe, IPS, wirtualne sieci prywatne (VPN), oprogramowanie antywirusowe i filtrowanie treści.
10. Opracowuj politykę bezpieczeństwa na piśmie dla Twojej firmy.

2.5 Polityka bezpieczeństwa wg Cisco Systems

Zarządzanie systemem bezpieczeństwa to nie tylko tworzenie haseł, list ACL lub konfigurowanie zapór sieciowych, ale także tworzenie założeń dotyczących. bezpieczeństwa firmy (przede wszystkim ciągła ich modyfikacja) w oparciu o dotychczasowe doświadczenia, testy odpornościowe sieci oraz najnowsze urządzenia i technologie chroniące przed sabotażem oraz intruzami. Takie kompleksowe działania nazywamy polityką bezpieczeństwa.

Definiowanie polityki bezpieczeństwa wg korporacji **Cisco Systems** składa się z następujących etapów:

- Definiowanie reguł bezpieczeństwa,
- Monitorowanie i analiza systemu,
- Testowanie zabezpieczeń,
- Zarządzanie systemem bezpieczeństwa sieciowego.

Etapy należy wykonywać cyklicznie w trakcie zarządzania systemem bezpieczeństwa.

2.6 Techniki testowania bezpieczeństwa

2.6.1 Bezpieczeństwo operacyjne

Bezpieczeństwo operacyjne dotyczy codziennych praktyk wymaganych do wdrożenia i utrzymania bezpiecznego systemu. Wszystkie sieci są podatne na ataki, jeśli planowanie, wdrażanie, operacje i konserwacja sieci nie są zgodne z praktykami bezpieczeństwa operacyjnego.

Bezpieczeństwo operacyjne rozpoczyna się od planowania i wdrażania sieci. Podczas tych faz zespół operacyjny analizuje projekty, identyfikuje zagrożenia i słabe punkty i dokonuje niezbędnych dostosowań. Rzeczywiste zadania operacyjne rozpoczynają się po skonfigurowaniu sieci i obejmują ciągłą konserwację środowiska. Dzięki temu środowisko, systemy i aplikacje mogą działać poprawnie i bezpiecznie.

Niektóre techniki testowania bezpieczeństwa są wykonywane ręcznie, a inne są zautomatyzowane. Niezależnie od rodzaju testów, personel, który tworzy i przeprowadza testy bezpieczeństwa, powinien posiadać bardzo dobrą wiedzę na temat konfiguracji sieci i jej ochrony, w następujących obszarach:

- Zabezpieczania urządzeń
- Zapory sieciowe
- IPSs
- Systemy operacyjne
- Podstawowe programowanie
- Protokoły sieciowe
- Luki w sieciach i ograniczanie ryzyka

2.6.2 Testowanie i ocena bezpieczeństwa sieci

W fazie wdrożenia testy bezpieczeństwa (***ang. Security Test and Evaluation***) są przeprowadzane na określonych częściach sieci. Po całkowitym zintegrowaniu i uruchomieniu sieci przeprowadzany jest test bezpieczeństwa i ocena (STE) STE to badanie środków ochronnych, które są umieszczone w sieci operacyjnej.

Testy należy powtarzać okresowo i zawsze, gdy w systemie wprowadzana jest jakakolwiek zmiana.

W przypadku systemów bezpieczeństwa, które chronią krytyczne informacje lub chronią hosty narażone na ciągłe zagrożenie, testy bezpieczeństwa powinny być przeprowadzane częściej.

2.6.3 Typy testów sieciowych

- **Testy penetracyjne -** Testy penetracyjne sieci symulują ataki ze złośliwych źródeł. Celem jest ustalenie wykonalności ataku i możliwych konsekwencji, które mogłyby wystąpić.

- **Skanowanie sieci -** Obejmuje oprogramowanie, które może pingować komputery, skanować w poszukiwaniu portów TCP i wyświetlać typy zasobów dostępnych w sieci. Niektóre programy skanujące mogą również wykrywać

nazwy użytkowników, grupy i udostępnione zasoby. Administratorzy sieci mogą wykorzystać te informacje do ulepszania zabezpieczeń swoich sieci.

- **Skanowanie podatności na atak -** Obejmuje oprogramowanie, które może wykryć potencjalne słabości w testowanych systemach. Słabe punkty systemów mogą obejmować na przykład błędną konfigurację, puste lub domyślne hasła lub potencjalne cele ataków DoS. Niektóre programy pozwalają administratorom na symulowaną awarię systemu w celu identyfikacji luki w systemie.

- **Łamanie haseł -** Obejmuje oprogramowanie używane do testowania i wykrywania słabych haseł, które powinny zostać zmienione. Po wykryciu słabych haseł, zasady tworzenia haseł powinny zostać zmienione.

- **Przegląd logów -** Administratorzy systemu powinni przejrzeć dzienniki zabezpieczeń, aby zidentyfikować potencjalne zagrożenia bezpieczeństwa. Nieprawidłowe działanie powinno być badane za pomocą oprogramowania filtrującego w celu skanowania długich plików dziennika.

- **Kontrolowanie integralności -** System kontroli integralności wykrywa i raportuje zmiany w systemie. Większość monitoringu koncentruje się na systemie plików. Niektóre systemy kontrolne mogą jednak zgłaszać czynności logowania i wylogowania.

- **Wykrywanie wirusów -** Oprogramowanie do wykrywania wirusów może być używane do identyfikowania i usuwania wirusów komputerowych i innego złośliwego oprogramowania.

2.6.4 Wykorzystanie wyników testu bezpieczeństwa sieci

Wyniki testu bezpieczeństwa sieci można wykorzystać na kilka sposobów:

- Do definiowania działań ograniczających (znalezienie zidentyfikowanych słabych punktów
- Jako punkt odniesienia do śledzenia postępów organizacji w spełnianiu wymagań bezpieczeństwa.
- Ocenianie stanu wdrożenia wymagań bezpieczeństwa systemu.
- Przeprowadzenie analizy kosztów i korzyści w celu poprawy bezpieczeństwa sieci.
- Aby usprawnić inne działania, takie jak ocena ryzyka, certyfikacja i autoryzacja w celu poprawy sprawności organizacji.
- Jako punkt odniesienia dla działań naprawczych.

2.6.5 Narzędzia do testowania sieci

Do testowania sieci można używać różnych narzędzi programowych, m. in.:

- Nmap / Zenmap - wykrywa komputery i usługi w sieci komputerowej, tworząc w ten sposób mapę sieci.
- SuperScan - oprogramowanie do skanowania portów zaprojektowane do wykrywania otwartych portów TCP i UDP, określania usług uruchomionych na tych portach i uruchamiania zapytań takich jak whois, ping, traceroute i wyszukiwanie nazw hostów.
- Zarządzanie zdarzeniami związanymi z bezpieczeństwem (SIEM) - technologia wykorzystywana w organizacjach przedsiębiorstw do zapewniania raportowania w czasie rzeczywistym i długoterminowej analizy zdarzeń związanych z bezpieczeństwem.
- GFI LANguard - skaner sieci i bezpieczeństwa, który wykrywa luki w zabezpieczeniach.
- Tripwire - ocenia i zatwierdza konfiguracje IT zgodnie z wewnętrznymi zasadami, standardami zgodności i najlepszymi praktykami bezpieczeństwa.
- Nessus - oprogramowanie do skanowania luk w zabezpieczeniach, koncentrujące się na zdalnym dostępie, błędnych konfiguracjach i atakom DoS przeciwko stosowi TCP / IP.
- L0phtCrack - aplikacja do kontroli i odzyskiwania hasła.
- Metasploit - dostarcza informacji na temat luk w zabezpieczeniach i pomaga w testach penetracyjnych i tworzeniu sygnatur IDS.

2.6.5.1 Nmap

Podstawowa funkcjonalność Nmap pozwala użytkownikowi wykonać kilka zadań:

- Klasyczne skanowanie portów TCP i UDP - wyszukiwanie różnych usług na jednym hoście.
- Klasyczne systematyczne skanowanie TCP i UDP - wyszukuje tę samą usługę na wielu hostach.
- Stealth TCP i UDP - Podobne do klasycznych skanów, ale trudniejsze do wykrycia przez hosta docelowego lub IPS.
- Zdalna identyfikacja systemu operacyjnego - określana jest również jako "fingerprinting" systemu operacyjnego.

Zaawansowane funkcje Nmap obejmują skanowanie protokołów, znane jako skanowanie w warstwie 3 portu. Funkcja identyfikuje obsługę protokołu warstwy 3 na hoście. Przykładami protokołów, które można zidentyfikować, są **GRE** i **OSPF**.

Nmap może być używany do testowania bezpieczeństwa, ale może być również wykorzystywany do szkodliwych celów. Nmap ma dodatkową funkcję, która pozwala mu używać hostów w tej samej sieci LAN, co host docelowy, co maskuje źródło skanowania.

2.6.5.2 Zenmap

Zenmap to graficzna nakładka na **Nmap**.

SuperScan to narzędzie do skanowania portów systemu Microsoft Windows. Działa na większości wersji systemu Windows i wymaga uprawnień administratora. **SuperScan** wersja 4 ma wiele przydatnych funkcji:

- Regulowana prędkość skanowania.
- Obsługa nieograniczonej liczby adresów IP.
- Wykrywanie hosta za pomocą wielu metod ICMP.
- Skanowanie TCP SYN.
- Skanowanie UDP.
- Proste generowanie raportu HTML.
- Skanowanie portu źródłowego.
- Szybkie rozwiązywanie nazw hostów.
- Rozległe możliwości wychwytania banerów.
- Ogromna wbudowana baza danych opisów portów.
- Kolejność losowania skanowania IP i portu.
- Wybór przydatnych narzędzi, takich jak ping, traceroute i whois.

2.6.5.3 SIEM

Security Information Event Management (SIEM) to technologia wykorzystywana w organizacjach korporacyjnych, zapewniająca raportowanie w czasie rzeczywistym i długoterminową analizę zdarzeń związanych z bezpieczeństwem. SIEM ewoluował z dwóch wcześniej oddzielnych produktów: Security Information Management (SEM) i Security Event Management (SEM). SIEM może być wdrożony jako oprogramowanie zintegrowane z Cisco Identity Services Engine (ISE) lub jako usługa zarządzana.

SIEM zawiera następujące podstawowe funkcje:

- Analiza sądowa - Możliwość wyszukiwania dzienników i rekordów zdarzeń ze źródeł w całej organizacji zapewnia pełniejszą informację do analizy sądowej.
- Korelacja - analizuje logi i zdarzenia z różnych systemów lub aplikacji, przyspieszając wykrywanie i reagowanie na zagrożenia bezpieczeństwa.
- Agregacja - zmniejsza objętość danych zdarzeń poprzez konsolidację zduplikowanych rekordów zdarzeń.

- Retencja - raportowanie przedstawia skorelowane i zagregowane dane o zdarzeniach w monitorowaniu w czasie rzeczywistym i podsumowaniach długoterminowych.

SIEM dostarcza szczegółowych informacji na temat źródła podejrzanej aktywności, m.in.:

- Informacje o użytkowniku (nazwa, status uwierzytelnienia, lokalizacja, grupa autoryzacji, status kwarantanny)
- Informacje o urządzeniu (producent, model, wersja systemu operacyjnego, adres MAC, metoda połączenia sieciowego, lokalizacja)
- Informacje o postawie (polityka zgodności z polityką bezpieczeństwa firmy, wersja programu antywirusowego, zgodność z zasadami zarządzania urządzeniami mobilnymi)

Dzięki tym informacjom inżynierowie bezpieczeństwa sieci mogą szybko i dokładnie ocenić znaczenie każdego zdarzenia związanego z bezpieczeństwem i odpowiedzieć na najważniejsze pytania:

- Kto jest związany z tym wydarzeniem?
- Czy jest to ważny użytkownik mający dostęp do własności intelektualnej lub poufnych informacji?
- Czy użytkownik jest uprawniony do dostępu do tego zasobu?
- Czy użytkownik ma dostęp do innych poufnych zasobów?
- Jakiego rodzaju urządzenie jest używane?
- Czy to wydarzenie reprezentuje potencjalny problem ze zgodnością?

2.6.6 Podsumowanie

Narzędzie	Opis
L0phtCrack	Aplikacja do audytu i odzyskiwania hasła
Tripwire	Uzyskiwanie dostępu i sprawdzanie konfiguracji IT pod kątem wewnętrznych zasad, standardów zgodności i najlepszych praktyk bezpieczeństwa
Nmap/Zenmap	Narzędzie do skanowania portów TCP i UDP w celu tworzenia mapy sieci
SIEM	Zapewnia raportowanie w czasie rzeczywistym i długoterminową analizę zdarzeń związanych z bezpieczeństwem

Nessus	Oprogramowanie do skanowania luk w zabezpieczeniach, koncentrujące się na zdalnym dostępie, błędnych konfiguracjach i DoS przeciwko stosowi TCP/IP
SuperScan	Narzędzie do skanowania portów systemu Microsoft Windows

Tabela 2.1 Podsumowanie narzędzi do testowania sieci

2.7 Cykl projektowania bezpieczeństwa sieci

Cykl projektowania bezpiecznej sieci to ciągły proces oceny i ponownej oceny wyposażenia i potrzeb w zakresie bezpieczeństwa w miarę zmian sieci. Ważnym aspektem tej ciągłej oceny jest zrozumienie, które zasoby musi chronić organizacja, nawet gdy te zasoby zmieniają się.

Określ, jakie są zasoby organizacji, zadając pytania:

- Co organizacja ma, czego inni chcą?
- Jakie procesy, dane lub systemy informacyjne mają kluczowe znaczenie dla organizacji?
- Jaki czynnik spowodowałby, że organizacja nie mogłaby prowadzić działalności gospodarczej lub wypełniać swojej misji?

Odpowiedzi na powyższe pytania mogą wskazywać takie zasoby, jak krytyczne bazy danych, ważne aplikacje, ważne informacje o klientach i pracownikach, sklasyfikowane informacje handlowe, udostępnione dyski, serwery poczty e-mail i serwery WWW.

Sieciowe systemy zabezpieczeń pomagają chronić te zasoby, ale sam system zabezpieczeń nie może zapobiec narażeniu zasobów na zagrożenia. Techniczne, administracyjne i fizyczne systemy bezpieczeństwa mogą zostać pokonane, jeśli społeczność użytkowników końcowych nie przestrzega zasad i procedur bezpieczeństwa.

Polityka zasad bezpieczeństwa obejmuje następujące zagadnienia:

- Zasady identyfikacji i uwierzytelniania.
- Zasady haseł.
- Dopuszczalne zasady użytkowania.
- Zasady dostępu zdalnego.
- Zasady utrzymania sieci.
- Zasady postępowania z incydentami.

Zasady identyfikacji i uwierzytelniania określają upoważnione osoby, które mogą mieć dostęp do zasobów sieciowych i przedstawia procedury weryfikacji.

Zasady haseł zapewniają, że hasła spełniają minimalne wymagania i są regularnie zmieniane.

Dopuszczalne zasady użytkowania identyfikują zasoby sieciowe i zastosowania, które są akceptowane przez organizację. Może również zidentyfikować konsekwencje, jeżeli ta polityka zostanie naruszona.

Zasady dostępu zdalnego określają, w jaki sposób zdalni użytkownicy mogą uzyskać dostęp do sieci i co jest dostępne za pośrednictwem zdalnego połączenia.

Zasady konserwacji sieci określają systemy operacyjne urządzeń sieciowych i procedury aktualizacji aplikacji użytkownika końcowego.

Zasady postępowania z incydentami opisują sposób postępowania z incydentami bezpieczeństwa.

Jednym z najczęstszych składników polityki bezpieczeństwa jest tzw. **Polityka Dopuszczalnego Użytkowania - PDU** (***ang. Acceptable Use Policy - AUP***). Można to również nazwać polityką odpowiedniego użytkowania.

Ten komponent określa, co użytkownicy mogą i czego nie mogą wykonywać na różnych komponentach systemu. Obejmuje to typ ruchu dozwolonego w sieci. AUP powinna być tak wyraźnie i jasno określona, jak to tylko możliwe, aby uniknąć nieporozumień. Na przykład AUP może wymieniać określone witryny, grupy dyskusyjne lub aplikacje wymagające dużej przepustowości, do których nie mają dostępu komputery firmowe lub sieć firmowa.

2.8 Projektowanie zasad polityki bezpieczeństwa

Projektowanie zasad polityki bezpieczeństwa to proces bardzo skomplikowany, składający się z następujących elementów:

- Określanie obiorców polityki bezpieczeństwa.
- Definiowanie polityki bezpieczeństwa na poziomie kadry zarządzającej.
- Definiowanie polityki bezpieczeństwa na poziomie kadry technicznej.
- Definiowanie polityki bezpieczeństwa na poziomie użytkownika końcowego.
- Tworzenie dokumentów ogólnych dotyczących polityki zabezpieczeń.
- Tworzenie dokumentów szczegółowych (procedur dotyczących polityki zabezpieczeń).
- Tworzenie hierarchii osób zarządzających bezpieczeństwem sieci.
- Przygotowanie kursów uświadamiających zagrożenia (motywacja pracowników).
- Testowanie sieci (sprawdzanie możliwych ataków).
- Zbieranie danych (po wystąpieniu naruszenia bezpieczeństwa).

- Modyfikowanie zasad polityki bezpieczeństwa (w oparciu o wyniki testowania sieci).

2.8.1 Odbiorcy polityki bezpieczeństwa

Odbiorca polityki bezpieczeństwa to każdy, kto ma dostęp do sieci. Wewnętrzni odbiorcy to kadry organizacji, tacy jak menedżerowie i dyrektorzy, działy i jednostki biznesowe, personel techniczny i pracownicy. Zewnętrzni odbiorcy to zróżnicowana grupa, która obejmuje partnerów, klientów, dostawców, konsultantów i wykonawców. Prawdopodobnie jeden dokument nie obejmie potrzeb wszystkich odbiorców w dużej organizacji. Dlatego należy tworzyć różne dokumenty dotyczące polityki bezpieczeństwa informacji zgodnie z potrzebami docelowej grupy odbiorców.

Odbiorcy określają zawartość polityki zabezpieczeń. Na przykład nie ma potrzeby dodawania opisu, dlaczego coś jest wymagane w polityce przeznaczonej dla personelu technicznego. Można założyć, że personel techniczny już wie, dlaczego uwzględniono określone wymaganie.

Menedżerowie prawdopodobnie nie będą zainteresowani technicznymi aspektami tego, dlaczego dany wymóg jest potrzebny. Zamiast tego chcą przeglądu na wysokim poziomie lub zasad wspierających ten wymóg.

Pracownicy często potrzebują więcej informacji o tym, dlaczego potrzebne są określone zasady bezpieczeństwa. Jeśli zrozumieją powody, dla których reguły te są bardziej prawdopodobne, są bardziej skłonne do ich przestrzegania.

2.8.2 Polityka zabezpieczeń na poziomie kadry zarządzającej

Polityka zabezpieczeń na poziomie zarządzania określa ogólne cele firmy w zakresie bezpieczeństwa dla menedżerów i personelu technicznego. Obejmuje wszystkie interakcje związane z bezpieczeństwem między jednostkami biznesowymi i działami wspierającymi w firmie.

Polityka zabezpieczeń na poziomie zarządzania obejmuje następujące obszary:

- Oświadczenie o problemie, do którego odnosi się polityka
- Jak polityka ma zastosowanie w środowisku
- Role i obowiązki osób których dotyczy ta polityką
- Działania, czynności i procesy, które są dozwolone (i niedozwolone)
- Konsekwencje niezgodności z zasadami polityki

2.8.3 Polityka zabezpieczeń na poziomie kadry technicznej

Polityka na poziomie kadry technicznej to szczegółowe dokumenty, które są wykorzystywane przez personel techniczny podczas wykonywania codziennych obowiązków związanych z ochroną. Są to głównie podręczniki dotyczące bezpieczeństwa, które opisują, co robi personel techniczny, ale nie w jaki sposób wykonuje swoje funkcje.

- **Zasady ogólne** - Obejmują **PDU**, zasady żądania dostępu do konta, politykę oceny nabycia, politykę audytu, politykę wrażliwości na informacje, politykę oceny ryzyka oraz globalne zasady serwera internetowego.
- **Zasady dot. telefonii** – definiuje zasady używania linii telefonicznych.
- **Zasady dot. poczty elektronicznej** – zawiera ogólne zasady używania poczty oraz zasady poczty przekierowywanej automatycznie.
- **Zasady dostępu zdalnego** – zawiera zasady używania VPN oraz logowania zdalnego.
- **Zasady sieciowe** – zawiera zasady dot. extranetu, minimalne wymagania dostępu do sieci, standardy dostępu do sieci, zabezpieczeń routerów, przełączników oraz serwerów.
- **Zasady dot. aplikacji** – obejmuje akceptowalną politykę szyfrowania, politykę dostawcy aplikacji (ASP), zasady kodowania poświadczeń bazy danych, zasady komunikacji między procesami, strategię bezpieczeństwa projektu i zasady ochrony kodu źródłowego.

2.8.4 Polityka zabezpieczeń na poziomie użytkownika końcowego

Zasady polityki zabezpieczeń dotyczące użytkowników końcowych obejmują wszystkie zasady dotyczące bezpieczeństwa informacji, które użytkownicy końcowi powinni znać oraz przestrzegać. Te zasady są zazwyczaj zgrupowane w jednym dokumencie w celu ułatwienia jego użycia.

Zasady dla użytkowników końcowych mogą pokrywać się z zasadami technicznymi, ale mogą również obejmować następujące zasady:

- **Zasady tożsamości** - Definiują zasady i praktyki ochrony sieci organizacji przed nieautoryzowanym dostępem. Praktyki te pomagają zmniejszyć ryzyko, że informacje o tożsamości trafią w niepowołane ręce.
- **Zasady dotyczące haseł** - hasła są ważnym aspektem bezpieczeństwa komputera. Polityka haseł definiuje reguły, które wszyscy użytkownicy muszą przestrzegać podczas tworzenia i zabezpieczania swoich haseł.

- **Zasady ochrony antywirusowej** - określają standardy ochrony sieci organizacji przed wszelkimi zagrożeniami związanymi z wirusami, robakami lub końmi trojańskimi.

2.8.5 Dokumenty dotyczące polityki zabezpieczeń

Najważniejszy dokument to lista sugestii, ogólnych czynności, standardów dla danej organizacji. Jest to zbiór bardziej elastyczny i zazwyczaj nie jest obowiązkowy. Zalecenia zawarte w nim można stosować w celu zdefiniowania sposobu opracowywania standardów i zagwarantowania przestrzegania ogólnych zasad bezpieczeństwa.

Niektóre z najbardziej pomocnych wskazówek (zwanych jako **Best Practices**) można znaleźć w repozytoriach następujących organizacji:

- National Institute of Standards and Technology (NIST) Computer Security Resource Center
- National Security Agency (NSA) Security Configuration Guides
- The Common Criteria standard

2.8.6 Dokumenty dotyczące procedur

Dokumenty zawierające procedury to zazwyczaj dokumenty które są obszerniejsze oraz bardziej szczegółowe niż normy i wytyczne. Procedury zawierają szczegóły implementacji, które są prezentowane w formie instrukcji krok po kroku oraz mogą zawierać grafikę (rysunki, zdjęcia).

2.8.7 Kadra zarządzająca polityką zabezpieczeń wg CISCO

Przykładowa hierarchia kadry zarządzającej polityką zabezpieczeń:

- **Chief Executive Officer (CEO)** - Ostatecznie odpowiedzialny za sukces organizacji. Wszystkie stanowiska kierownicze podlegają dyrektorowi generalnemu.
- **Chief Technology Officer (CTO)** - Identyfikuje i ocenia nowe technologie. Kieruje każdym nowym rozwojem technologii. Odpowiedzialny za utrzymanie i usprawnianie istniejących systemów. Zapewnia przywództwo w zakresie wszystkich zagadnień związanych z technologią, które wspierają operacje. CTO odpowiada za infrastrukturę technologiczną.
- **Chief Information Officer (CIO)** - Odpowiedzialny za wszystkie systemy informatyczne i komputerowe, które wspierają cele przedsiębiorstwa. Kieruje

udanym wdrażaniem nowych technologii i procesów roboczych. W małych i średnich organizacjach rolę tę często łączy się z CTO. CIO zapewnia przywództwo, gdy opracowywane są procesy i praktyki wspierające przepływ informacji.

- **Chief Security Officer (CSO)** - opracowuje, wdraża i zarządza strategią i programami bezpieczeństwa organizacji. Zapewnia przywództwo w zakresie rozwoju wszelkich procesów związanych z działalnością biznesową, w tym ochrony własności intelektualnej. GUS musi ograniczyć narażenie na odpowiedzialność we wszystkich obszarach ryzyka finansowego, fizycznego i osobistego.
- **Chief Information Security Officer (CISO)** - CISO koncentruje się na bezpieczeństwie IT. CISO odpowiada za opracowanie i wdrożenie polityki bezpieczeństwa. CISO może być głównym autorem polityki bezpieczeństwa lub zapewniać przywództwo innym autorom. W każdym razie CISO jest odpowiedzialny i odpowiedzialny za treść polityki bezpieczeństwa.

2.8.8 Szkolenia uświadamiające zagrożenia

Szkolenia uświadamiające są zwykle skierowane do odbiorców na wszystkich poziomach organizacji, w tym stanowisk kierowniczych. W ramach szkolenia należy wykonać działania mające na celu podnoszenie świadomości bezpieczeństwa oraz zmianę zachowania lub wdrożenie właściwych praktyk bezpieczeństwa.

Przykładem tematu szkolenia uświadamiającego lub materiału do rozpowszechniania jest ochrona przed wirusami. Temat można krótko omówić, opisując, czym jest wirus, co może się stać, gdy wirus zainfekuje system użytkownika, co użytkownik musi zrobić, aby chronić system i co użytkownicy robią, gdy odkryją wirusa.

Przykładowe metody zwiększania świadomości bezpieczeństwa to:

- wykłady, filmy wideo
- plakaty, artykuły, biuletyny
- nagrody za dobre praktyki bezpieczeństwa
- przypomnienia, takie jak banery do logowania, podkładki pod mysz, filiżanki do kawy i notatniki

2.8.9 Szkolenia dotyczące bezpieczeństwa

Przykładem szkolenia dla personelu spoza działu IT może być kurs dotyczący odpowiednich praktyk bezpieczeństwa specyficznych dla aplikacji, z których użytkownik końcowy musi korzystać, takich jak aplikacje bazodanowe.

Przykładem szkolenia dla personelu IT może być kurs bezpieczeństwa informatycznego, który szczegółowo omawia mechanizmy zarządzania: operacyjne i techniczne, które należy wdrożyć.

Skuteczny kurs szkoleniowy dotyczący bezpieczeństwa wymaga odpowiedniego planowania, wdrażania, utrzymania i okresowej oceny. Kurs szkoleniowy dotyczący bezpieczeństwa sieci może obejmować następujące etapy:

Etap 1. Zidentyfikuj zakres, cele i cele szkolenia - Zakres szkolenia zapewnia szkolenia dla wszystkich typów osób, które wchodzą w interakcje z systemami IT. Ponieważ użytkownicy potrzebują szkoleń związanych bezpośrednio z korzystaniem z konkretnych systemów, konieczne jest uzupełnienie dużego programu dla całej organizacji o więcej kursów specyficznych dla systemu.

Etap 2. Identyfikacja i kształcenie kadry szkoleniowej - Ważne jest, aby trenerzy mieli wystarczającą wiedzę na temat zagadnień bezpieczeństwa komputerowego, zasad i technik. Ważne jest również, aby wiedzieli, jak skutecznie przekazywać informacje i pomysły.

Etap 3. Identyfikacja odbiorców docelowych - Nie każdy potrzebuje tego samego stopnia lub rodzaju informacji bezpieczeństwa komputerowego, aby wykonać przypisane zadanie. Kursy szkoleniowe dotyczące bezpieczeństwa, które przedstawiają jedynie informacje potrzebne poszczególnym odbiorcom oraz pomijają nieistotne informacje, mają najlepsze wyniki.

Etap 4. Motywuj zarządzanie i pracowników - Rozważ wykorzystanie technik motywacyjnych, aby pokazać kierownictwu i pracownikom, w jaki sposób ich udział w szkoleniu przynosi korzyści organizacji.

Etap 5. Administruj kursami - Ważne uwagi dotyczące administrowania kursem obejmują wybór odpowiednich metod szkoleniowych, tematów, materiałów oraz technik prezentacji.

Etap 6. Utrzymanie kursów - Bądź informowany o zmianach w technologii komputerowej i wymaganiach bezpieczeństwa. Kursy szkoleniowe, które obecnie odpowiadają potrzebom organizacji, mogą stać się nieskuteczne, gdy organizacja zacznie korzystać z nowej aplikacji lub zmieni swoje otoczenie, na przykład wdrażanie VoIP.

Etap 7. Ocena skuteczności kursu - Ocena ma na celu ustalenie, ile informacji jest przechowywanych, w jakim stopniu przestrzegane są procedury bezpieczeństwa komputerowego oraz jak będą wdrażane w przyszłości.

2.8.10 Proces zbierania danych

Proces zbierania danych musi odbywać się precyzyjnie i szybko. Po wystąpieniu naruszenia bezpieczeństwa konieczne jest natychmiastowe odizolowanie zainfekowanego systemu. Systemy nie powinny być wyłączane lub restartowane, zanim pamięć zostanie zrzucona do pliku, ponieważ system opróżnia pamięć za każdym razem, gdy urządzenie jest wyłączone. Ponadto przed rozpoczęciem pracy z danymi na twardym dysku należy wykonać obraz dysku. Wiele kopii dysku twardego jest zwykle wykonywanych po wyłączeniu urządzenia w celu ustanowienia kopii wzorcowych.

Kopie wzorcowe są zwykle zamykane w sejfie, a badacze używają kopii roboczych zarówno dla oskarżenia, jak i dla obrony. Badacze mogą ustalić, czy doszło do sabotażu danych, porównując kopie robocze z wzorcową kopią, która została zabezpieczona i nienaruszona od początku dochodzenia.

Po zebraniu danych, ale przed odłączeniem sprzętu, konieczne jest sfotografowanie sprzętu w miejscu. Wszystkie dowody muszą być rozpatrywane przy zachowaniu właściwej sekwencji dostaw, co oznacza, że tylko osoby posiadające zezwolenie mają dostęp do dowodów, a dostęp do nich jest udokumentowany.

2.8.11 RODO - Rozporządzenie o ochronie danych osobowych

UWAGA:

Opisywane ogólne założenia RODO zawierają dane z okresu lutego 2018 roku.

RODO to ogólne rozporządzenie Parlamentu Europejskiego i Rady Unii z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

Przewidywana data zastosowania rozporządzenia: **25.05.2018**

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Źródło:

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.POL&toc=OJ:L:2016:119:TOC

GDPR (ang. General Data Protection Regulation) – Ogólne Rozporządzenie o Ochronie Danych to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Rozporządzenie weszło w życie 17 maja 2016 r. Zacznie ono obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r. Rozporządzenie wiązać będzie wszystkich, którzy przetwarzają dane osobowe w związku z prowadzoną działalnością gospodarczą.

Rozporządzenie wprowadza szereg zmian oraz rozszerza zakres obowiązków administratorów oraz podmiotów przetwarzających dane. Celem nowych przepisów jest również wyposażenie osób fizycznych oraz organów nadzorujących w skuteczne narzędzia reagowania na naruszenia Rozporządzenia. Bardzo istotną dla przedsiębiorców kwestią jest też **określenie maksymalnego poziomu kar za naruszenia przepisów, które to kary mogą sięgnąć nawet 20 000 000 euro lub 4% całkowitego rocznego światowego obrotu przedsiębiorcy** z roku obrotowego poprzedzającego naruszenie.

Źródło:

https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/topics/RODO-ochrona-danych-osobowych.html

2.8.11.1 RODO – Zakres rozporządzenia

Zakres rozporządzenia obejmuje kraje Unii Europejskiej, ale nie wymaga implementacji stosownie do prawa poszczególnych państw.

Każdy podmiot gromadzący i przetwarzający dane osobowe będzie miał obowiązek aktywnego zabiegania o ochronę prywatności na każdym etapie przetwarzania oraz na każdym etapie projektowania procesów przetwarzania

2.8.11.2 RODO – Obowiązki przedsiębiorstw (organizacji)

RODO przewiduje szereg obowiązków, które podmioty przetwarzające i administratorzy powinni spełnić w celu zgodnego z prawem przetwarzania danych osobowych.

Obowiązki te obejmują m.in. opracowanie i prowadzenie dokumentacji przetwarzania danych, w tym rejestru czynności przetwarzania i rejestru naruszeń, monitorowanie naruszeń ochrony danych, a w określonych sytuacjach notyfikowanie organu nadzorczego lub podmiotu danych o naruszeniu, np. wycieku danych.

RODO wymaga, aby administratorzy danych osobowych i podmioty przetwarzające analizowały poziom ryzyka i na podstawie jego oceny decydowali o rodzaju i zakresie środków technicznych i organizacyjnych ochrony danych.

Istotnym czynnikiem jest w tym przypadku adekwatność środków do zagrożeń -odpowiedź na pytanie, czy zidentyfikowane ryzyka wystarczająco odpowiadają do przyjętych rozwiązań.

RODO nie będzie regulowało precyzyjnie wytycznych organizacyjnych ani technologicznych zabezpieczenia danych. Administratorzy muszą ocenić i zdecydować co i jak zrobić, żeby sieć oraz serwery były bezpiecznie.

2.8.11.3 RODO – Procedura oceny oddziaływania na ochronę danych osobowych

Czemu służyć ma procedura oceny oddziaływania na ochronę danych osobowych oraz konsultacje z organem ochrony danych osobowych?

Ocena skutków przetwarzania ma na celu sprawdzenie czy przetwarzanie danych w konkretnym przypadku jest odpowiednio zabezpieczone. Na podstawie analizy ryzyka naruszenia praw i wolności osób fizycznych uzupełnionej o cel, charakter, zakres i kontekst przetwarzania powinniśmy być w stanie ocenić, jakie środki organizacyjne i techniczne pozwolą odpowiednio zabezpieczyć przetwarzanie.

2.8.11.4 RODO – Wpływ na procesy pozyskiwania danych od klientów

RODO (GDPR) wprowadza katalog obowiązków informacyjnych, jakie musimy wykonać zbierając dane. Dane można zbierać, pamiętając o tym, że musimy rzetelnie informować, a tam, gdzie jest to konieczne – prosić o zgodę na przetwarzanie danych osobowych. Fakt odebrania zgody trzeba będzie odpowiednio udokumentować. Na potrzeby wykazania zgodności przetwarzania z prawem będziemy zobligowani do przechowywania informacji o tym kto wyraził zgodę, kiedy to zrobił, w jakim zakresie oraz jakie informacje zostały mu przekazane przy okazji odbierania zgody.

2.8.11.5 RODO – Zgoda na przetwarzanie danych

RODO (GDPR) wprowadza następujące obowiązki:

- Zgoda na przetwarzanie danych osobowych musi być wyrażona konkretnemu podmiotowi (Oświadczenie o wyrażeniu zgody powinno zostać wyodrębnione, musi także mieć także zrozumiałą formę, tj. zostać sformułowane w jasny i prosty sposób)
- Udostępnianie danych innemu podmiotowi stanowi czynność przetwarzania – jej przeprowadzenie wymaga odpowiedniej podstawy prawnej. Jeśli nie mamy takiej podstawy, nie możemy udostępnić danych osobowych – w przeciwnym wypadku ryzykujemy odpowiedzialność prawną.

2.8.11.6 RODO – Obowiązek powiadamiania i kary

RODO (GDPR) wprowadza następujące obowiązki i kary:

Należy zgłosić do organu nadzorczego incydent naruszenia bezpieczeństwa w ciągu 72 godzin od jego zajścia. Należy powiadomić które dane osobowe zostały – bądź mogły zostać – poważnie naruszone.

Uwaga: Powyższy warunek może spowodować poważne problemy, zarówno techniczne oraz organizacyjne i finansowe, w szczególności przy wyciekach danych na dużą skalę. Należy pamiętać, że niedopełnienie obowiązku notyfikacyjnego będzie mogło skutkować nałożeniem kary finansowej do 10 mln euro.

3 | MINIMALNE ZABEZPIECZENIA DOSTĘPU DO ROUTERÓW