Wykład 1

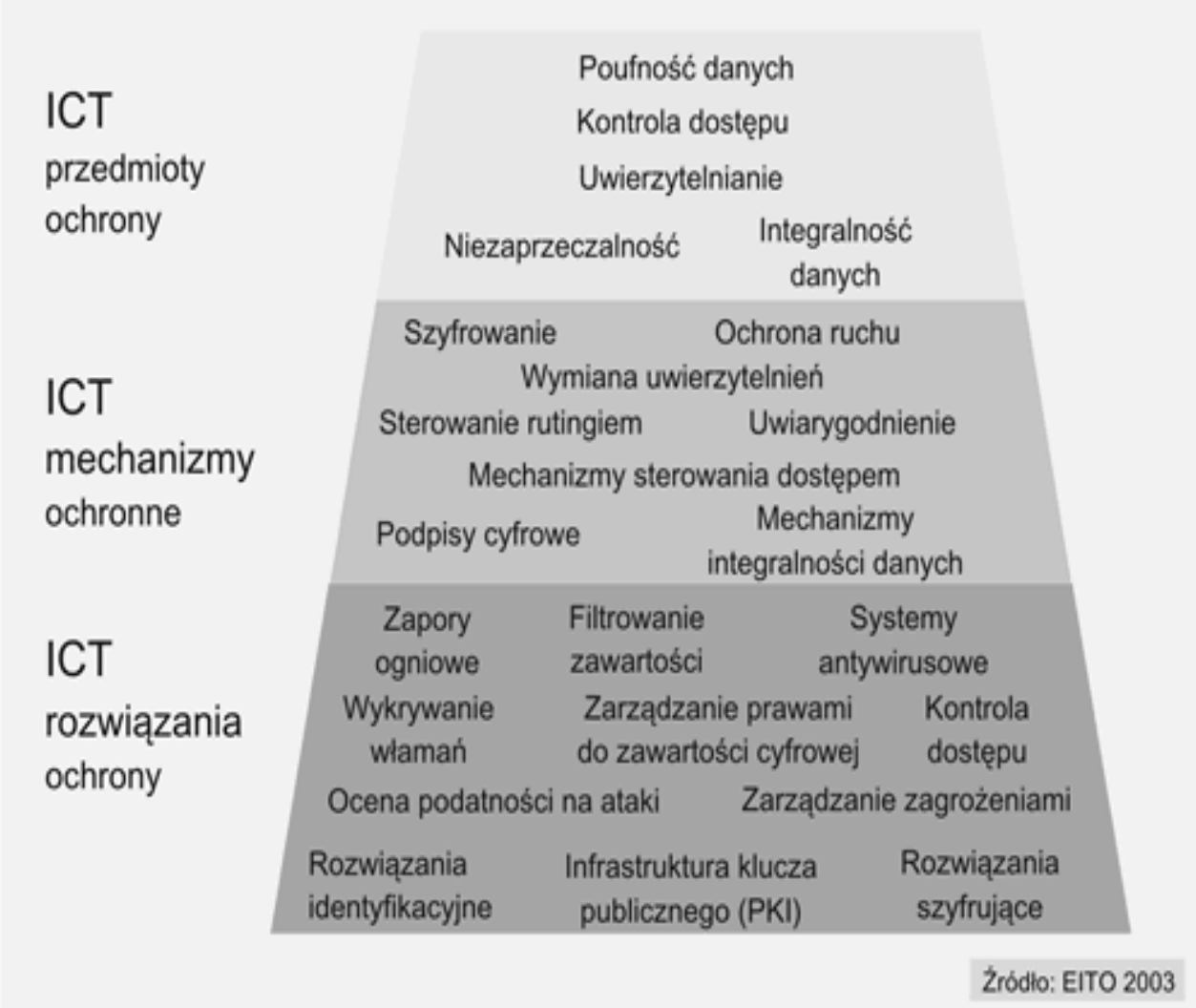
TEMAT: PODSTAWY BEZPIECZEŃSTWA SIECI KOMPUTEROWO-TELEINFORMATYCZNYCH (SKI)

1.1. Ogólne pojęcie bezpieczeństwa

Próba określenia bezpieczeństwa za pomocą jednej definicji może okazać się nie wystarczająca. Dlaczego? Dlatego, że bezpieczeństwo to zagadnienie bardzo obszerne. Dla administratora sieci może to oznaczać pewność, że system nie zostanie zhakowany; dla twórców stron internetowych – gwarancję, że numer karty kredytowej klienta dokonującego zakupów przez Internet nie będzie przechwycony. Jeszcze inną interpretację przedstawi zarząd firmy. Dla nich oznacza to stan, w którym przedsiębiorstwo jest odpowiednio chronione przed stratami.

Wieloznaczność interpretacji tego tematu nasuwa wnioski: aby stworzyć bezpieczny system ochrony informacji, nie można skupić się na rozwiązaniach punktowych, takich jak np. zapory ogniowe (firewall), czy skanery antywirusowe. Przy tworzeniu możliwie najbezpieczniejszej infrastruktury sieciowej koniecznym jest postrzeganie bezpieczeństwa jako całości. Jeśli jeden element w systemie jest słaby, to automatycznie cały system jest zagrożony. Dla przykładu: użycie zapory ogniowej ogranicza możliwość ataku intruzów z zewnątrz, ale nie wyklucza nieuczciwych działań pracowników wewnątrz firmy. Trzeba także pamiętać, że czynności zabezpieczania sieci nie można uznać za jednorazowe. Zapewnienie bezpieczeństwa to proces ciągły. Jeśli pracownik SKI nie dba o aktualizowanie oprogramowania, usunięcie błędów systemowych czy chociażby monitorowanie ruchu sieciowego, to pewnego dnia może się okazać, że sieć stanie się łatwym celem ataku. Aby uniknąć niepotrzebnego ryzyka należy stosować się do pewnych reguł.

Zarządzanie systemem informatycznym w kontekście bezpieczeństwa polega na zapewnieniu usług ochrony (niezaprzeczalności, kontroli dostępu, integralności danych, uwierzytelniania, poufności danych), niezależnie od tego, czy pod tym pojęciem kryje się jednostkowy komputer, czy tez cała sieć komputerowa.



Rys. 1.1. Hierarchiczny model bezpieczeństwa SKI

1.2. Usługi ochrony – użyteczna klasyfikacja usług ochrony:

- **integralność danych** [1] – potwierdzenie w przekazach telekomunikacyjnych, że przesyłana informacja nie została podmieniona, zniekształcona lub zmieniona bez wiedzy adresata. W praktyce funkcję integralności realizuje się przez dołączenie do wiadomości tzw. podpisu cyfrowego i prywatnego (tajnego) klucza znanego tylko odbiorcy. Niejawny klucz nadawcy jest zaszyfrowany wspolnym dla nadawcy i odbiorcy kluczem kodu integralności lub kodu uwierzytelnienia wiadomości;
- **uwierzytelnianie** [2] – proces potwierdzenia tożsamości osoby lub obiektu implementowany w systemach ochrony sieci komputerowych; stosowany głównie w celu zabezpieczenia sieci przed niepożądaną penetracją osób lub obiektów (programów, plików, serwerów itd.), także zabezpiecza przed podpisywaniem się przed fałszerzy. Technika uwierzytelniania obejmuje 3 podstawowe rozwiązania, każde o innym stopniu ufności uwierzytelniania: zwykle karty identyfikacyjne (*token*) [3], inteligentne karty identyfikacyjne oraz urządzenia biometryczne (obraz twarzy, linie papilarne, siatkówka oka, identyfikacja głosowa) o największej pewności identyfikacji użytkownika;
- **poufność** – informacje przesyłane i składowane w sieci nie mogą być czytane przez nieuprawnione podmioty;
- **integralność** – informacje nie są zniszczone, zmodyfikowane lub skradzione przez niepowołane osoby z zewnątrz lub wewnątrz;
- **dostępność** – elementy sieci, dane i usługi są zawsze dostępne, kiedy są potrzebne.

---

[1] **Leksykon teleinformatyka**

[2] **Leksykon teleinformatyka**

[3] **karta identyfikacyjna [wg Leksykonu teleinformatyka] – o znormalizowanych rozmiarach i funkcjach karta (zwykła, magnetyczna*, elektroniczna**, inteligentna), zawierająca zapis informacji niezbędnych do identyfikacji jej właściciela po uprzednim wprowadzeniu odpowiedniego i właściwego kodu hasłowego. Inteligentne karty identyfikacyjne generują zmienny kod hasłowy, co dobrze je chroni przez niepowołanym podsłuchem;**

*** karta magnetyczna [wg Leksykonu teleinformatyka] – typ bankomatowej karty identyfikacyjnej z laminowanego PCV o standardowych wymiarach 86x54x0,76 [mm]. Karty tego typu mają naniesiony pasek magnetyczny (koercja 300 Oerstedów) i kilka zabezpieczeń: hologram, nadruk UV, mikrodruk oraz unikatowe cechy związane z kartą, kontem i klientem systemu – kodowane na pasku magnetycznym. Często wymaganymi etapami personalizacji są: przetłoczenie karty przy jej wydawaniu oraz złożenie nieścieralnego wzoru podpisu użytkownika na sylikonowej warstwie karty;**

**** karta elektroniczna [wg Leksykonu teleinformatyka] – typ płatniczej lub identyfikacyjnej karty plastikowej o ustalonych wymiarach (86x54x0,76 [mm]), z wmontowanymi jednym lub więcej układami scalonymi. Ze względu na sposób komunikacji z otoczeniem zewnętrznym karty elektroniczne dzielą się na stykowe (metalizowane styki) i bezstykowe ze specjalnymi układami komunikacji. Wyróżnia się dwa rodzaje kart:**

- **pamięciowe (*memory card*) – z zapisem jednokrotnym EPROM lub wielokrotnym EEPROM oraz**
- **mikroprocesorowe (*smard card*), inaczej zwane inteligentnymi (CPU, RAM, ROM, EPROM, WE/WU) – zarządzające dostępem do poszczególnych jej fragmentów oraz układów WE/WU. Inteligentne karty mikroprocesorowe przechowują informacje, wykonują operacje na danych (zapis, odczyt, uaktualnianie), umożliwiają dwukierunkową komunikację, a oprócz identyfikacji wykonują także procedury kryptograficzne (szyfrowanie za pomocą wymiennych kluczy).**

1.3. Ataki na bezpieczeństwo

1.3.1. Rodzaje ataków

SKI może być zaatakowany na wiele różnych sposobów. Osoby niepowołane wykorzystują luki programowe, wyszukują nowe błędy w oprogramowaniu, co prowadzi do powstawania coraz bardziej wyrafinowanych technik ataków. Zgodnie z klasyfikacją zaproponowaną przez Stephena T. Kenta wyróżnia się dwa typy ataków: **pasywne** i **aktywne**.

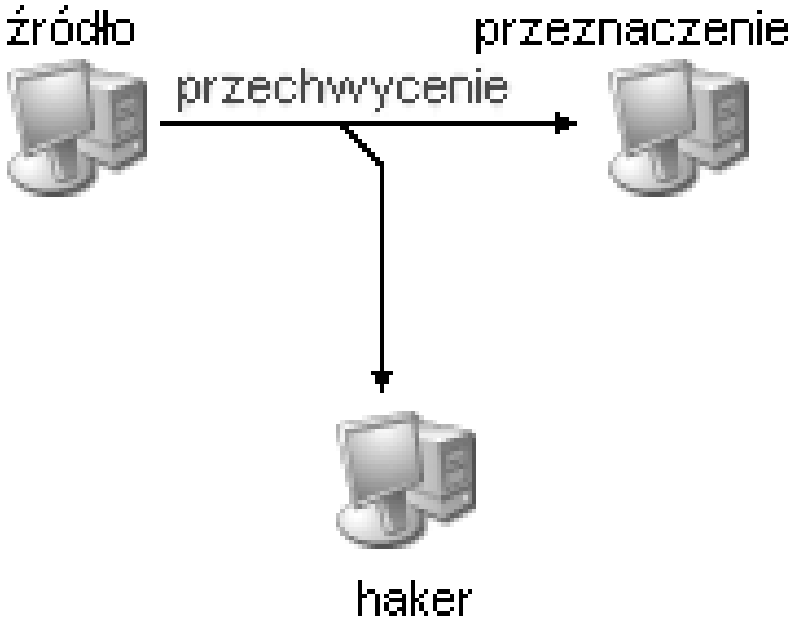
Ataki pasywne – polegają na przechwyceniu, podsłuchiwaniu lub monitorowaniu przesyłanych danych. Osoba niepowolana ogranicza się do odkrycia treści komunikatu-strumienia danych lub jego analizy, ale nie ingeruje w samą strukturę przechwyconej informacji. W związku z tym są to działania bardzo trudne do wykrycia. W postępowaniu z tego rodzaju zagrożeniami skuteczniejsze są metody zapobiegawcze.

Ataki aktywne – w przeciwieństwie do pasywnych, ich celem jest modyfikacja lub fałszowanie danych, oddziaływanie na SKI powodując przerwanie transmisji, modyfikacje strumienia danych lub podszywania się pod kogoś innego. Wyróżnia się kilka ich typów:

- ***maskarada (masquerade)*** – działanie polegające na podszywaniu się pod komputer uprzywilejowany; zwykle towarzyszą jej inne ataki aktywne,
- ***powtórka (replay)*** – polega na przechwyceniu danych i ich retransmisji do osiągnięcia własnych niedozwolonych celów,
- ***modyfikacja (modification)*** – sprowadza się do zmiany oryginalnego fragmentu komunikatu i podstawienia własnego zazwyczaj w celu osiągnięcia niedozwolonych skutków, np.: dostęp do zasobów,
- ***blokada usług (denial of service)*** – przeszkadzanie w normalnym funkcjonowaniu urządzeń komunikacyjnych w celu uniemożliwienia lub całkowitego zablokowania dostępu do łącza fizycznego; ciągły napływ pakietów danych, który w rezultacie może prowadzić do tzw. programowego przepełnienia bufora i zawieszenia urządzenia.

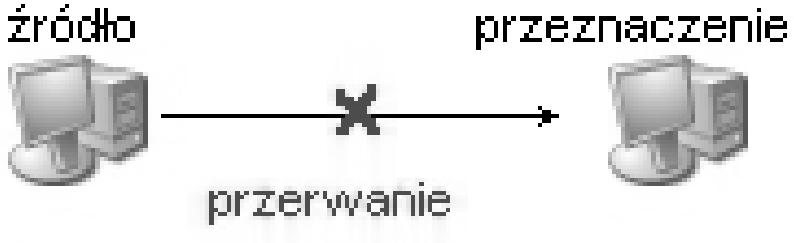
Ze względu na charakter ataku rozróżnia się:

- ***przechwycenie (interception)*** – jest to atak (pasywny) na poufność; występuje, gdy osoba nieupoważniona uzyskuje dostęp do zasobów, np.: podsłuchiwanie pakietów transmisijnych celem przechwycenia danych w sieci i nielegalne kopiowanie plików lub programów;



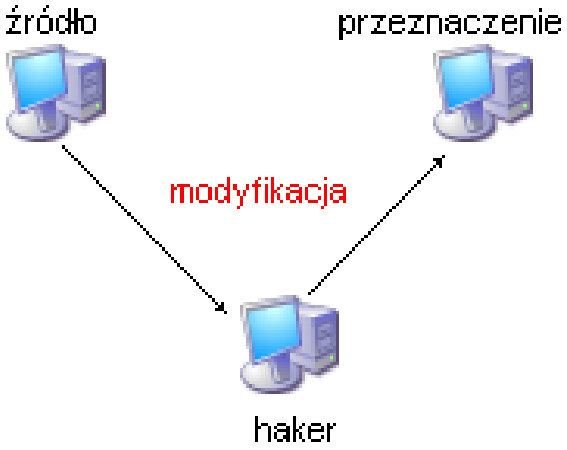
Rys. 1.2. Schemat ataku przechwycenia

- ***przerwanie (interruption)*** – jest to atak (aktywny) na dyspozycyjność; polega na na zniszczeniu części informacji lub spowodowaniu jej niedostępności albo niemożności użycia niektórych elementów systemu; Przykładem może być fizyczne zniszczenie fragmentu komputera lub sieci, np. uszkodzenia dysku twardego, przecięcie medium transmisyjnego, lub uniemożliwienie działania systemu zarządzania plikami;



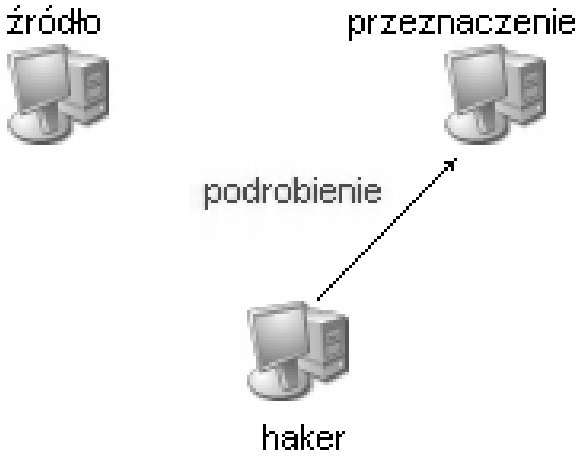
Rys. 1.3. Schemat ataku przerwania

- ***modyfikacja (modification)*** – jest atakiem (aktywnym) na nienaruszalność; polega nie tylko na zdobyciu przez napastnika dostępu do zasobów ale również modyfikacji ich, np.: zmiana zawartości w pliku z danymi albo skryptów startowych lub modyfikacja komunikatów przesyłanych w sieci, wprowadzenie zmiany w programie w celu wywołania innego sposobu jego działania;



Rys. 1.4. Schemat ataku modyfikacji

- ***podrabianie (fabrication)*** – jest atakiem (aktywnym) na autentyczność; napastnik wprowadza do systemu fałszywe obiekty, np.: wprowadzenie nieautentycznych komunikatów do sieci lub dodanie danych do pliku.



Rys. 1.5. Schemat ataku podrobienia

1.3.2. Ataki pasywne

1.3.2.1. Sniffing, czyli podsłuchiwanie

Sniffing jest techniką polegającą na przechwytywaniu pakietów przepływających w SKI. Każdy komputer podłączony do lokalnej sieci komputerowej ma swój własny unikalny adres sprzętowy (MAC). W sieci, w której występuje rozgłaszanie (broadcasting), dane są rozsyłane do wszystkich komputerów, ale odbierają je tylko te, do których są zaadresowne. Wykorzystując fakt, że karty sieciowe w trybie mieszanym pozwalają na odczytywanie pakietów przesyłanych do innych komputerów w sieci, osoba niepowołana może przechwycić poufne informacje przesyłane przez sieć. Programy służące w tym celu nazywa się snifferami. Pierwotnie sniffery stanowiły narządzie administracyjne do analizowania ruchu sieciowego i wykrywania problemów sprzętowych konfiguracyjnych. Z czasem zostały przyswojone przez osoby nieupoważnione. Dziś są poważnym zagrożeniem dla poufności danych w sieci przedsiębiorstwa. Praktyka pokazuje, że większość ataków tego typu polega na kradzieży istotnych danych lub przechwyceniu sekwencji bajtów zawierających informacje autoryzacji (login i hasło). W infrastrukturze każdej SKI istnieje kilka newralgicznych punktów, w których mogą zostać zainstalowane sniffery. Są to między innymi: rutery, węzły komunikacyjne pomiędzy dwoma sieciami LAN, serwery korporacyjne, komputery użytkowników. Zainstalowanie sniffera w newralgicznym miejscu w sieci, np. na routerze, może doprowadzić do pokonania zabezpieczeń wszystkich innych stacji roboczych z nim połączonych. Programy tego typu na ogół przechwytują wszystkie pakiety z danymi. Jeśli osoba nieupoważniona nie kradnie danych, to z punktu jej widzenia większość pakietów nie ma dla niej znaczenia, dlatego ogranicza się przechwytywanie do kilkuset bajtów z każdego pakietu. Zazwyczaj wystarczy to do poznania nazwy użytkownika i jego hasła. Sniffery można zainstalować na każdej maszynie w SKI, ale najbardziej interesujące dla osoby nieupoważnionej są miejsca, gdzie dokonuje się procedur autoryzacji. Na szczególne niebezpieczeństwo narażone są komputery bedące bramkami miedzy sieciami.

Ze względu na umiejscowienie sniffera w sieci wyróżnić można trzy sytuacje:

- sniffer znajduje się na routerze między siecią lokalną a Internetem, bądź też miedzy różnymi sieciami lokalnymi lub rozległymi; ten rodzaj sniffingu jest najbardziej niebezpieczny;
- sniffer znajduje się na komputerze, z którego inicjowane jest połączenie;

- sniffer działa na komputerze, na który następuje próba logowania użytkownika.

Wyróżnia się dwa sposoby prowadzenia sniffingu:

1. Pierwszy z nich to podsłuch za pomocą urządzeń włączonych na pewnym odcinku medium transmisyjnego. Trudne do zlokalizowania zwłaszcza, że takie urządzenie może znajdować się w dowolnym miejscu w sieci. Niedawno wydawało się, że zastosowanie światłowodów ograniczy swobodę podsłuchiwaczy. Dziś wiadomo już, że bariera ta została pokonana. W zlokalizowaniu snifferów pomocne okazują się reflektometry dziedziny czasu TDR (Time Domain Reflectometr) wykorzystujące zjawisko odbicia części energii fali elektromagnetycznej.

2. Sniffery występują także w formie oprogramowania dedykowanego. Jedne to rozwiązania komercyjne oferujące duże możliwości co do ilości analizowanych protokołów oraz wsparcia technicznego. Drugie to darmowe, nieco uboższe programy dostępne na wielu witrynach internetowych (niekoniecznie do legalnego wykorzystania).

Są również mieszane, sprzętowo-programowe metody podsłuchiwania ruchu sieciowego. Istnieje jeszcze jedna metoda ograniczania sniffingu – podział sieci na mniejsze podsieci za pomocą urządzeń typu most, przełącznik lub ruter (ograniczają przepływ informacji w danej podsieci, co zmniejsza prawdopodobieństwo przechwycenia ich przez sniffer). Niestety jest to rozwiązanie mało praktyczne ze względu na wydatki jakie niesie ze sobą zakup owych urządzeń.

W ostatnim czasie znacznie udoskonalono technologie w zakresie bezpieczeństwa systemów komputerowych. Większość systemów operacyjnych stosuje kryptografię już na poziomie pakietu, tak więc jeżeli osoba niepowołana przechwyci już jakieś pakiety będą one w postaci zaszyfrowanej. Sniffery mogą także przyczynić się do naruszenia bezpieczeństwa sąsiednich sieci komputerowych bądź stopniowego dostępu do nich. Wymogiem uruchomienia sniffera na danej maszynie jest posiadanie uprawnień administratora, ponieważ możliwość przestawinia karty sieciowej w tryb mieszany dozwolone jest tylko administratorom. Wykrywanie snifferów jest zadaniem trudnym, bowiem programy tego typu działają pasywnie i nie zostawiają żadnych śladów w logach systemowych.

1.3.2.2. Kradzieże haseł

Kolejną warstwą ochrony jest procedura uwierzytelniania użytkownika rozpoczynającego pracę w systemie. Procedura ta ma na celu ochronę przed nielegalnym dostępem do systemu. Najczęściej procedura taka wykonywana jest z wykorzystaniem haseł. Aby procedura ta zapewniała odpowiednio wysoki poziom bezpieczeństwa, hasło powinno być kontrolowane na etapie tworzenia. Hasło powinno wykazywać odpowiedni stopień zawiłości (nie powinno być oczywiste). Istnieje szereg narzędzi, zarówno dostarczanych z systemami operacyjnymi, jak i dodatkowych, służących do kontroli zawiłości haseł. Niektóre z tych narzędzi tworzą słowniki najpopularniejszych wyrażeń i stosując pewien zbiór reguł próbują wygenerować niebezpieczne hasła, które później nie są dopuszczane do użytkowania. Prawdopodobnie największym zagrożeniem bezpieczeństwa w Internecie jest wielokrotne używanie tych samych haseł i przesyłanie ich w postaci zwykłego, niezaszyfrowanego tekstu. Problem ten dotyczy zarówno sieci zewnętrznych, jak i wewnętrznych. Jedyną metodą obrony przed podsłuchiwaniem haseł jest eliminacja przekazywania ich w postaci niezaszyfrowanego tekstu oraz częsta zmiana.

Tworzenie silnych haseł

Dobre zabezpieczenia komputera obejmują stosowanie silnych haseł logowania do sieci oraz do konta administratora na danym komputerze. Aby hasło było silne i trudne do złamania, powinno:

- liczyć co najmniej siedem znaków;
- zawierać znaki z trzech następujących grup (tab. 1.1):

Tabela 1.1

Spis znaków używanych do tworzenia silnych znaków

Opis	Przykłady
Litery (wielkie i małe)	A, B, C,...; a, b, c,...
Cyfry	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbole (wszystkie znaki nie będące literami ani cyframi)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

- mieć przynajmniej jeden znak symbolu między pozycjami drugą a szóstą;
- być zdecydowanie inne od poprzednich haseł;
- nie zawierać imienia, nazwiska ani nazwy użytkownika;
- różnić się od wszelkich wyrazów i nazw własnych.

Hasła mogą być najsłabszym ogniwem w łańcuchu zabezpieczeń komputera. Oprogramowanie do łamania haseł stosuje jedną z trzech następujących metod: inteligentne odgadywanie, ataki ze słownika i automatyzację polegającą na wypróbowywaniu wszystkich możliwych kombinacji znaków. Dysponując odpowiednią ilością czasu, metoda zautomatyzowana jest w stanie złamać każde hasło.

Należy też uważać, gdzie się zapisuje hasło na komputerze. Niektóre okna dialogowe, np. te służące do dostępu zdalnego i innych połączeń telefonicznych, oferują opcję zapisania lub zapamiętania hasła, zalecane jest nie zaznaczanie tej opcji.

1.3.2.3. Skanowanie

Jedną z pierwszych czynności, jakie wykonuje osoba nieupoważniona, jest test penetracyjny atakowanego komputera w celu zdobycia informacji dotyczących:

- oferowanych usług TCP, UDP, RPC;
- rodzaju i wersji oprogramowania udostępnianych usług jak i samego systemu operacyjnego;
- struktury SKI.

W pierwszej kolejności wykonuje skanowanie zdalnej maszyny pod kątem otwartych portów, a następnie próbuje uzyskać informacje o rodzaju i wersji oprogramowania odpowiedzialnego za obsługę tych portów, a także informacje o architekturze i systemie operacyjnym. Posiadając już wszelkie informacje, osoba nieupoważniona może ściągając odpowiedni program z Internetu „exploit", przeprowadzić atak słabiej części SKI. Skanowanie przeprowadza się techniką siłową poprzez wysyłanie pakietów na różne porty w zależności od otrzymanej odpowiedzi lub jej braku, poprzez dedukcję otrzymuje się porty, które są otwarte.

1.3.2.4. Social engineering

Terminem social engineering określa się zestaw sposobów na wyłudzenie informacji o kontach i hasłach dostępu oraz innych elementów wpływających na bezpieczeństwo SKI. Pod tym pojęciem kryje się niebezpieczny mechanizm nadużywania ludzkiego zaufania w celach kryminalnych. Uświadomienie użytkownikowi problemów występujących podczas pracy z komputerem może zapobiec niebezpiecznym incydentom. Zazwyczaj człowiek jest najsłabszym elementem systemu bezpieczeństwa w firmie. Niekoniecznie musi to być efekt świadomego działania. Błędy mogą wynikać z braku odpowiedniej świadomości istniejących zagrożeń. Istnieją dwa sposoby oszukania użytkownika. Pierwszy to użycie środków programowo-sprzętowych, np. rozmieszczenie stron zawierających odpowiednio umotywowaną prośbę o podanie identyfikatora użytkownika oraz hasła. Natomiast drugi bazuje na bezpośrednim kontakcie telefonicznym lub osobistym z celem ataku - użytkownikiem, lub pracownikiem działu helpdesk.

Jeśli firma nie posiada opracowanej polityki bezpieczeństwa to prędzej czy później dojdzie do incydentu przekazania tajnych informacji osobom nieuprawnionym. By zabezpieczyć się przed taką ewentualnością konieczne jest wdrożenie dobrych zasad ochrony informacji poufnych. Stosowanie zabezpieczeń technicznych w postaci zapór ogniowych, programów antywirusowych nie wystarczy. Ważne jest także odpowiednie szkolenie użytkowników. Niebezpiecznym zwyczajem jest przesyłanie znajomym różnych żartobliwych obrazków lub animacji. Potencjalnie w każdym z nich może znajdować się wirus

lub trojan. Większości niebezpiecznych sytuacji da się uniknąć dzięki odpowiedniemu uświadomieniu użytkownikom istniejących zagrożeń.

1.3.3. Ataki aktywne

1.3.3.1. Spoofing

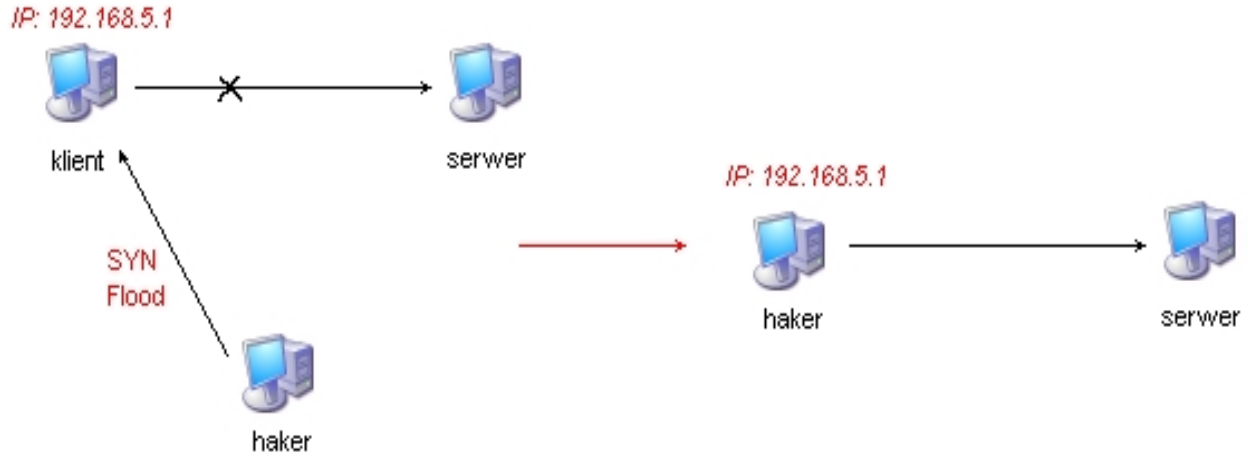
Atak polegający na oszukiwaniu systemów zabezpieczeń SKI poprzez podszywanie się jednego komputera pod inny, upoważniony do nawiązywania połączenia. Wśród wielu odmian tego ataku najpopularniejsze to IP-Spoofing oraz DNS-Spoofing. Rzadziej spotykane to ARP-Spoofing czy RIP-Spoofing.

IP-Spoofing

Metoda została opisana po raz pierwszy w roku 1985, a pierwszy atak z wykorzystaniem tej techniki odnotowano w Boże Narodzenie 1994 r. Jej działanie polega na podsłuchiwaniu przez sniffer połączenia pomiędzy klientem a serwerem i wyłapywaniu wysyłanych numerów sekwencji. Po znalezieniu algorytmu, jakim są one tworzone, haker doprowadza do niestabilności połączenia, np. poprzez atak SYN Flood na stacje klienta, zmienia numer IP na numer klienta i przewidując numer sekwencji korzysta z istniejącego połączenia jako autoryzowany użytkownik: tzn. sprowadza się do przesyłania pakietów ze sfałszowanym adresem źródłowym. W efekcie komputer odbierający pakiety błędnie identyfikuje nadawcę. Najczęściej atak IP-Spoofing przeprowadzany jest z sieci publicznej po to, aby przejąć kontrolę nad jakimś ważnym komputerem z sieci prywatnej. Składa się z kolejnych faz:

1) atak na klienta w sieci prywatnej; powoduje niestabilność pracy systemu – cel osiągany z wykorzystaniem jednej ze skutecznych technik, np. SYN Flood;

2) przejęcie adresu komputera uprzywilejowanego i podszycie się pod zablokowanego klienta – napastnik kontynuuje nawiązane wcześniej połączenie z serwerem jako autoryzowany użytkownik.



Rys. 1.6. Zasada dzialania IP-Spoofingu

DNS-Spoofing

Rys. 2.8.

Jest atakiem na nienaruszalność serwera DNS (Domain Name System): polega na włamaniu się do serwera DNS, który przechowuje bazę danych (odpowiedzialną za proces przekształcania adresów-nazw na odpowiednie adresy IP). Sprowadza się do zmiany tablic mapowania nazw hostów na adresy IP poprzez modyfikację wpisów w tablicy DNS w taki sposób, że żądania klientów są kierowane do komputera krakera, zamiast do prawdziwego miejsca docelowego.

Kiedy klient wysyła żądanie podania adresu IP jakiegoś hosta, to w odpowiedzi otrzymuje adres podrobiony: może to być adres IP komputera znajdującego się pod całkowitą kontrolą krakera. Podszywanie DNS jest dość łatwo wykryć. Jeśli podejrzewamy któryś z serwerów DNS, należy wysłać żądania do innych serwerów DNS w sieci. Po porównaniu odpowiedzi łatwo można zauważyć wystąpienie ew. anomalii. Jedyną przeszkodę napotkamy, gdy ataku na dany serwer DNS dokonano stosunkowo dawno i tablica mapowania została przesłana do innych serwerów.

Ryzyko zagrożenia atakiem typu Spoofing można zminimalizować poprzez odpowiednio skonfigurowany filtr pakietów – blokowanie tych pakietów nadchodzących z sieci publicznej, które posiadają adres źródłowy z zakresu sieci prywatnej. Bardziej zaawansowane przeciwdziałanie obejmuje zainstalowanie zapory ogniowej dysponującej funkcją *antispoofing*. Funkcja ta umożliwia wykrycie, czy pakiet został sfałszowany, czy nie. Decyzję tą podejmuje na podstawie prostej zasady. Otóż zapora ogniowa identyfikuje sieci znajdujące się poza jej fizycznymi interfejsami. Zatem jeśli pakiet przychodzący (z prywatnym adresem nadawcy) pojawi się na interfejsie sieci wewnętrznej, zostanie potraktowany jako prawdziwy. W innym przypadku będzie uznany za sfałszowany.

1.3.3.2. Ataki typu DoS

Jest to jeden z najczęściej stosowanych atak na sieciowe systemy komputerowe, mający na celu zakłócenie funkcjonowania systemu lub całkowite sparaliżowanie jego pracy. Być może dlatego, że jest dość łatwy do przeprowadzenia i efektywny, a w konsekwencji niebezpieczny. Ataki przeprowadzane zdalnie wykorzystują wady protokołu TCP/IP. Niebezpieczeństwo polega na tym, że z założenia protokół ten miał spełniać zadania wyznaczone w specyfikacji. Nikt nie spodziewał się, iż będzie wykorzystywany do innych celów. Pocieszającą wiadomością może być fakt, że w momencie zlokalizowania błędów w aplikacjach, ich producenci wypuszczają na rynek oprogramowanie korygujące, co w przyszłości zapobiega podobnym przypadkom. Niestety, szerokie zastosowanie TCP/IP sprawia, że w zasadzie każdy element sieci z zaimplementowaną obsługą tego standardu, jest podatny na ataki typu DoS.

Charakterystyczne są efekty ataków typu DoS:

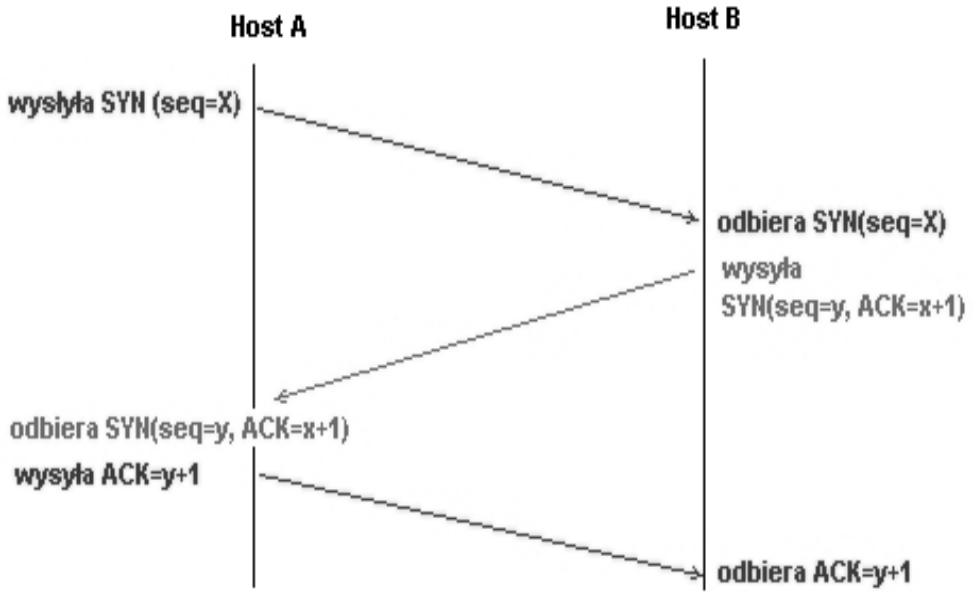
a) ***wyczerpanie zasobów*** – polega na przeciążeniu elementów krytycznych systemu, tj. procesora, pamięci, pamięci dyskowej, itp. Procesy żądające ponadprzeciętnej dostępu do tych zasobów mogą zostać zablokowane;

b) ***zniszczenie zasobów*** – spowodowanie niestabilności pracy programów skutkuje błędami, które mogą doprowadzić do zniszczenia, np.: wprowadzanie pakietów o nieprawidłowych rozmiarach lub z błędnymi opcjami prowadzi zawieszenia gniazda w aplikacji;

c) ***wstrzymanie usług*** – wykorzystuje zjawisko odtwarzania procesów; ma miejsce, gdy system w celu zachowania niezawodności, zamyka i odrzuca przez pewien czas połączenia TCP dla danej pary adresu i portu źródłowego i docelowego.

Odmiany DoS:

SYN flood - najpopularniejszy atak typu DoS, polega na wysłaniu do serwera ofiary bardzo dużej liczby zapytań, np. tysięcy odwołań do tej samej strony internetowej.



Rys. 1.7. Schemat nawiązania połączenia

Kraker przeprowadza atak SYN flood w sposób automatyczny, korzystając z gotowych programów, jakie bez trudu można znaleźć w Internecie. Wykonywany przez taki program atak polega na wykorzystaniu protokołu Three-way-Handshaking czyli trójfazowe porozumienie: do serwera wysyłany jest początkowo pakiet służący do synchronizacji transmisji (tzw. pakiet SYN), żądając nawiązania połączenia poprzez wymaganie od serwera wysłania potwierdzenia. Ponieważ system musi odpowiedzieć na zapytanie (zgodnie ze specyfikacją), odsyła pakiet SYN/ACK, czyli informuje, że może nawiązać połączenie. Po jego otrzymaniu program potwierdza swoją gotowość, połączenie zostaje nawiązane, natomiast jednocześnie serwer rezerwuje na ten cel jeden z wolnych portów, część pamięci i deskryptor pliku nowego połączenia. Oczekuje na trzecią fazę procesu – powrotny ACK. Kraker nie poprzestaje jednak na odsyłaniu takiej informacji (co powoduje, że serwer ponownie zażąda potwierdzenia nawiązania łączności, ale z dwukrotnie większym czasem oczekiwania na odpowiedź; taka próba ma miejsce zwykle ok. 6 razy – potem serwer odrzuca połączenie), zalewając serwer kolejnymi żądaniami połączenia, tym razem nie wysyłając potwierdzeń. Pełna komunikacja sieciowa nie zostaje więc do końca nawiązana, a serwer przebywa w stanie ciągłego oczekiwania na otwarcie połączeń. Odpowiednio duża liczba żądań powoduje, że w krótkim czasie zablokowane zostają wszystkie wolne porty. Ponieważ po pewnym czasie serwer zwalnia zajęte porty, skuteczny atak wymaga ciągłego utrzymywania pracy programu-agresora. Takie działanie skutecznie blokuje ruch przychodzący i wychodzący maszyny atakowanej. Poważna utrata mocy obliczeniowej maszyny w wielu przypadkach prowadzi do zawieszenia danej usługi sieciowej lub całego serwera, przez co odwołania rzeczywistych jego użytkowników nie mogą już zostać zrealizowane.. Rzutuje to także na inne systemy wspomagające bezpieczeństwo w sieci, np.: zaporę ogniową lub proxy serwer. Dla każdego przychodzącego połączenia firewall tworzy nowy wpis do tablicy stanów, a proxy nowy punkt końcowy proxy dla pośrednictwa między maszyną klienta i serwera. Wynikiem wyczerpania zasobów jest bezużyteczność obu urządzeń (na czas ich odblokowania).

W celu przywrócenia działania systemu konieczna staje się wówczas interwencja administratora. Zlokalizowanie sprawcy ataku DoS jest stosunkowo łatwym zadaniem i sprowadza się do określenie adresu IP komputera, z którego wysyłane są pakiety. Dla wyspecjalizowanych służb wyśledzenie sprawcy nie stanowi problemu, nawet w przypadku, gdy stosuje on technikę fałszowania adresów IP (tzw. IP spoofing).

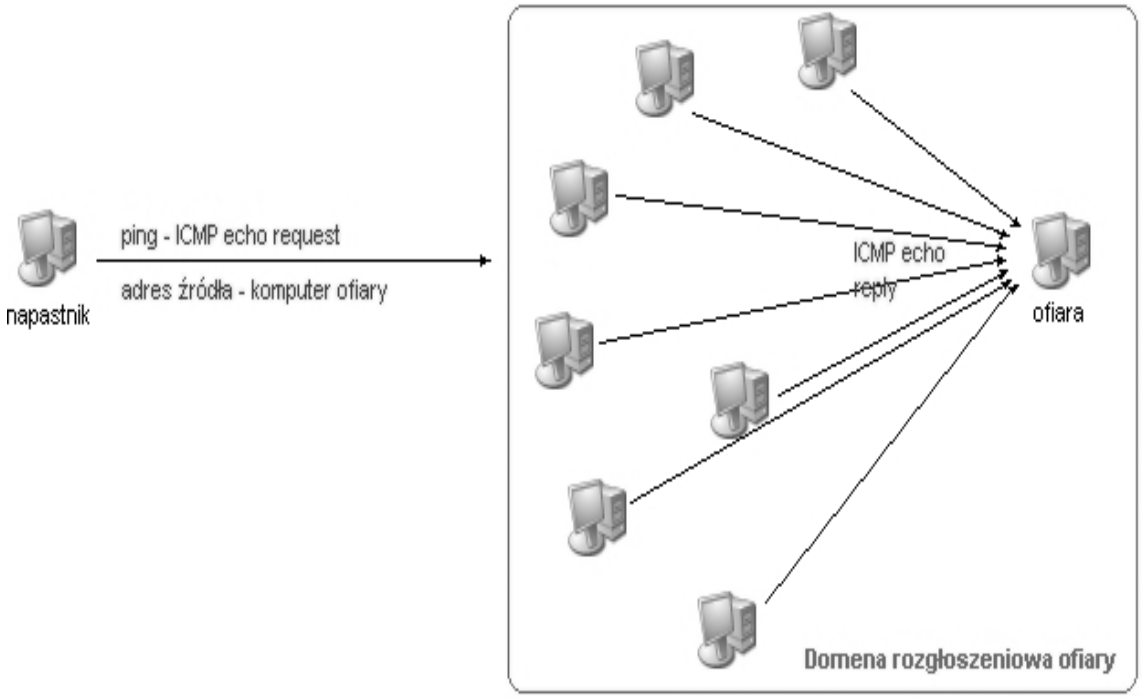
Czasami SYN flood nie jest skierowany bezpośrednio na konkretne urządzenie komunikacyjne w sieci, które może być jedynie pretekstem do rzeczywistego celu, jakim jest zapchanie łączy, co w dalszym ciągu uniemożliwia komunikację wewnątrzsieciową. Rozwiązaniem mogą być access listy, które filtrują ruch na maszynach trasujących. Jednak w dalszym ciągu atak będzie dochodził do rutera brzegowego. W poważnych sytuacjach koniecznym może się okazać współpraca z dostawcą łącza internetowego. Niezależnie od tego zaleca się stosowanie asekuracyjnych zabiegów, które zmniejszają podatność systemu na ataki SYN flood, a są to między innymi:

- **rozsądne ustawienie liczby powtórzeń wysyłanych pakietów ACK – wówczas serwer szybciej zwalnia gniazda po nieudanej próbie połączenia;**
- **zwiększenie ilości możliwych połączeń – utrudnia w krótkim czasie zablokowanie wszystkich dostępnych gniazdek;**
- **obarczenie dostawcy Internetu (ISP) odpowiedzialnością za ochronę przed atakami,**
- **aktualizowanie oprogramowania.**

Amplification attack

Atak stosowany w sytuacjach, gdy sieć ofiary ma znacznie większą przepustowość niż łącze napastnika. Załóżmy, że haker może wysyłać dane z prędkością 2 Mbit/s, a sieć docelowa ma 155 Mbit/s. Niemożliwym jest zapchanie, aby atakujący wysłał tyle pakietów, żeby zapchać całe dostępne pasmo. W 1998 roku po raz pierwszy pojawiła się technika zwana ***amplification attack***, której przedstawicielem jest atak typu ***Smurf***.

Koncepcja działania ***Smurfa*** polega na wysyłaniu do domeny rozgłoszeniowej komputera-ofiary dużej ilości pakietów ICMP echo request (ping) tak, aby w polu adresu źródłowego znajdował się adres maszyny atakowanej, a w polu adresu docelowego – adres rozgłoszeniowy. Wówczas każdy komputer w domenie odpowie pakietem ICMP echo reply i pojedynczy komputer zostanie zalany zwielokrotnioną ilością informacji, co prowadzi do zawieszenia jego usług. Nie wiadomo też kto dokonał ataku, bo podmieniony adres źródłowy wskazuje na komputer ofiary.



Rys. 1.8. Schemat ataku typu Smurf

Aby bronić się przed ***Smurfem*** należy ustawić odpowiednie reguły sterujące pakietami na ruterze – uniemożliwienie przepływu pakietom wychodzącym na adres rozgłoszeniowy.

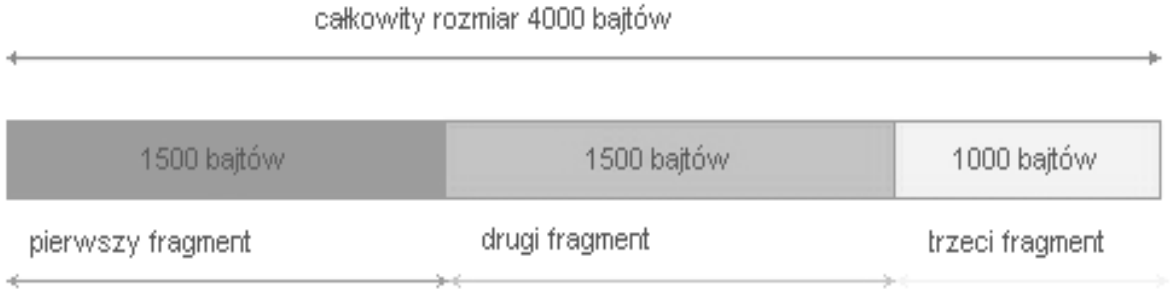
Fragmentation attack

Stanowi zagrożenie dla urządzeń sieciowych (rutery, zapory ogniowe, systemy wykrywania włamań). Podstawą ataków z tej grupy jest proces fragmentacji, jaki zachodzi w warstwie sieciowej IP lub transportowej TCP. Proces polega na dzieleniu pakietu na mniejsze części i wysyłaniu go do odbiorcy, gdzie z powrotem zostaje poskładany do formy pierwotnej. Celem ataków jest zajęcie czasu systemom ochronnym tak, żeby jak najbardziej ograniczyć dostępność zasobów maszyny. Aby to osiągnąć napastnik wysyła pakiety o jak najmniejszym rozmiarze i z możliwie dużym współczynnikiem fragmentacji. Efekt obciążenia systemu końcowego potęgują: celowe opóźnienia pakietów, ich wzajemne nachodzenie na siebie, nieuporządkowanie oraz wielokrotne powtarzanie tych samych informacji i tworzenie wielu połączeń na raz. W wyniku tych zabiegów obiekt ataku spędza sporo czasu, zanim poskłada wszystkie dane w jedną całość i pozamyka otwarte sesje TCP.

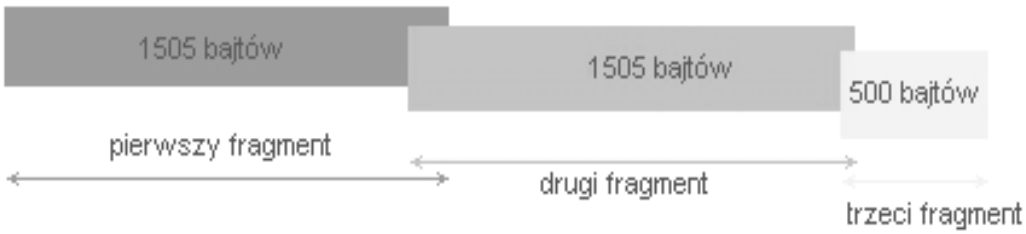
Dla przykładu:

- ***TearDrop***

Wykorzystuje błąd fragmentacji IP. Atak Teardrop ustawia w nagłówkach IP znaczniki przesunięcia, które wraz z numerem sekwencyjnym stanowią informację dla systemu końcowego jak odtworzyć pierwotną postać datagramu.



Prawidłowo sfragmentowany datagram



Przykładowy efekt zmiany znacznika przesunięcia nagłówka IP

Rys. 1.9. Błędna rekonstrukcja pakietu

Jeśli mamy do przesłania pakiet długości 4000 bajtów, to pola znacznika przesunięcia w kolejnych fragmentach powinny zawierać wartości: np. 1 do 1500, 1501 do 3000, 3001 do 4000. Działanie ataku sprowadza się do ustawienia tych wartości w taki sposób, aby zachodziły na siebie, czyli np. 1 do 1500, 1500 do 3000, 3000 do 3500. Na dodatek ostatni pakiet ma długość mniejszą od oczekiwanej. Host odbierający nie jest w stanie poprawnie złożyć pakietów w jedną całość i generuje błędy rekonstrukcji. Skutek – zawieszenie lub restart urządzenia.

- ***Ping of Death***

Atak ten polega na wysłaniu do maszyny zdalnej pofragmentowanych datagramów, których łączna długość przekracza maksymalną dopuszczalną w specyfikacji – 65 535 bajtów. Protokół TCP/IP wykorzystuje dzielenie datagramów na mniejsze części po to, aby wysyłaną informację można było umieścić w fizycznej ramce łącza danych. Jeśli urządzenie docelowe będzie próbowało odtworzyć datagram sprzed fragmentacji, zwykle powoduje to zawieszenie systemu lub nawet restart maszyny. Realizację ataku najczęściej przeprowadza się przy użyciu ICMP echo request, czyli popularnego narzędzia „ping” do sprawdzania dostępności hosta zdalnego. Spotyka się także wykorzystanie protokołów TCP, UDP oraz IPX. Atak stanowi spore zagrożenie, ponieważ jest niezależny od platformy sprzętowej. Są na niego podatne niektóre systemy UNIX, Mac OS, NetWare, również urządzenie typu zapora ogniowa czy ruter.

Aby chronić się przed tym atakiem należy instalować „łaty” uaktualniające systemy obrony, które dostarcza producent. Skuteczne zabezpieczenie stanowi implementacja filtru pakietów lub odpowiedniego systemu zaporowego, który blokuje datagramy IP o wielkości przekraczającej dopuszczalny rozmiar.

DDoS *(Distributed Denial of Service)*, czyli rozproszony atak typu DoS

Jest ulepszoną i znacznie bardziej niebezpieczną wersją ataku DoS wykorzystującym tzw. rozproszone środowisko komputerowe.Taktyka ataku DDoS polega na zdobyciu przewagi liczebnej i na skoncentrowanym ataku zdalnym. Ściślej mówiąc, napastnik wykorzystuje do swoich celów systemy komputerowe osób, które nawet nie zdają sobie sprawy, że w tym uczestniczą. Pierwsza faza ataku polega na podporządkowaniu sobie komputerów pośredniczących, tzw. *zombie*. Po zainstalowaniu odpowiednich wtyczek (dostępnych na stronach hakerskich) na wybranych komputerach, napastnik jest zdolny do przesyłania prostych komend sterujących potajemnie przejętym systemem. Zwykle pomiędzy *zombie* a napastnikiem są jeszcze *agenci*, czyli 3 albo 4 komputery kontrolujące „armię zombie".

Druga faza to przypuszczenie ataku. Rozkaz wysłany z kwatery głównej wyzwala serię działań z wykorzystaniem znanych scenariuszy ataków. Przy takim oblężeniu ofiara nie jest w stanie się obronić. Praktyka pokazuje, że nie można lekceważyć ataków DDoS. W 1999 roku spustoszenie w sieci siał Tribal Network Flood, który wykorzystywał źle skonfigurowane zapory ogniowe i rutery z „dziurawymi" filtrami ruchu sieciowego. Podstawą działania było szyfrowanie treści komunikatów ICMP echo reply. Parę miesięcy później pojawił się na tyle dopracowany atak o nazwie Stacheldraht („drut kolczasty"), że umożliwiał uwierzytelnianie własnych technik szyfrujących w systemie ofiary i dokonywał nawet automatycznej aktualizacji. Trzeba zaznaczyć, że rozproszony DoS ciągle ewoluuje i pojawiają się coraz bardziej wyrafinowany jego odmiany.

Sposobem na zminimalizowanie podatności sieci na ataki DoS są działania profilaktyczne, czyli:

- konfigurowanie list dostępu na zaporach ogniowych i ruterach;
- korzystanie jedynie z niezbędnych usług;
- ustalanie ograniczeń na zasoby systemowe (przestrzeń dyskowa, przepustowość łączy, itp.) - QUOTA;
- monitorowanie wykorzystania zasobów systemowych;
- instalowanie łat na systemy w jak najkrótszym czasie po wykryciu luk;
- czytanie list dyskusyjnych i innych materiałów poświęconych bezpieczeństwu w SKI;
- używanie systemów wykrywania włamań IDS;
- przygotowania narzędzi umożliwiających obronę i lokalizowanie źródła ataku.

1.3.3.3. Konie trojańskie

"Koń trojański" - program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. fałszywy program *login* kradnie hasło użytkownika).

Konie trojańskie stanowią poważne zagrożenie z kilku powodów:

- działają skrycie, nie rezerwują żadnych nowych identyfikatorów procesów PID;
- wykorzystują nazwy istniejących programów - nie zdziwi na przykład fakt, że na liście procesów zobaczymy ten właśnie program, np. kilkakrotnie uruchomiony httpd;
- konie trojańskie trudno jest wykryć i rozróżnić od prawdziwych, autoryzowanych programów.

Wykrywanie koni trojańskich zazwyczaj polega na wyszukaniu podejrzanych zmian w plikach dyskowych. Inną metodą może być próba zdebugowania programu, albo nawet oglądniecie jego kodu maszynowego w najprostszym edytorze w celu wyszukania nietypowych komunikatów. Jeśli np. w programie jak w/w login znaleźlibyśmy string postaci: "Segmentation Fault", który jest komunikatem normalnie tworzonym przez mechanizmy systemu, od razu moglibyśmy stwierdzić, ze coś jest nie tak.

1.3.3.4. Ataki typu Buffer Overflow

Atak ma na celu przepełnienie bufora w wybranym programie, co prowadzi do zawieszenia usługi albo do przejęcia praw administratora. Najpopularniejszą formą ataku wykorzystującą przepełnienie bufora jest atakowanie buforów na stosie. Ataki są tak przeprowadzane, aby uzyskać następujące cele:

- wprowadzić swój wykonywalny kod, jest to przeważnie zestaw instrukcji maszynowych wykonujących shella, co w efekcie daję powłokę z prawami administratora;
- zmienić adres powrotu, dla aktualnie wykonywanej funkcji system ma przeznaczony pewien obszar stosu, przepełnieni bufora nadpisuje adres powrotu z aktualnej funkcji w taki sposób, aby został wykonany kod ataku. Kiedy funkcja zostanie wykonana, zamiast wrócić do miejsca z którego została wywołana, przenosi się w miejsce, gdzie znajduje się kod włamywacza.

1.3.3.5. Tylne drzwi

Pojęciem tym określa się nieudokumentowane „tylne wejścia” do programów lub systemów. Stanowią awaryjny dostęp do danych zasobów na prawach superużytkownika. Są to często tajne skróty klawiszowe w aplikacjach albo uniwersalne hasła do systemu czy specjalne programy pozostawione w systemie po udanym włamaniu hakera. Nieraz stanowią poważną lukę w systemie ochrony i pomimo zainstalowanych zabezpieczeń, umożliwiają nieuprawnionym użytkownikom dostęp do zasobów SKI.

Jednym ze sposobów wprowadzenia tylnego wejścia jest stworzenie konta lub procesu z uprawnieniami superużytkownia. Takie zdarzenia mają miejsce najczęściej przy instalacji lub konserwacji systemu. Nieusunięte pozostałości po tych zabiegach mogą być łatwo wychwycone przez włamywacza. Dla administratora istotnym jest wykrycie niepożądanych dziur w systemie powstałych w wyniku wyżej wymienionych działań. Łatwo je także zlikwidować, na przykład przy użyciu polecenia finger, które jest w stanie pokazać rzadko używane konta z prawami administratora. W praktyce zdarza się również, że konta superużytkowników są tylko zablokowane. Włamywacze posługują się na tyle wyrafinowanymi metodami, że są w stanie odblokować owe konto bez pozostawienia śladu jakichkolwiek działań – stają się przecież normalnymi użytkownikami. Dodatkowo modyfikują logi systemowe.

Możliwe jest zainstalowanie tylnego wejścia w kompilatorze. Rozwiązanie takie, niezależnie od kompilowanego kodu źródłowego programu, umożliwia generowanie kodu wynikowego zawierającego tylne wejście. Przeglądanie programu źródłowego nie uwidoczni niedociągnięć, ponieważ zagrożenie ukryte jest w kodzie kompilatora.

Innym przykładem tworzenia tylnego wejścia jest posługiwanie się specjalnymi programami, których zadaniem jest podmiana plików z hasłami w taki sposób, aby umożliwić intruzowi logowanie do systemu o określonej porze z prawami administratora.

Do zaawansowanych tylnych wejść należą także tzw. *konie trojańskie*, które potrafią całkowicie przejąć kontrolę na zdalnym komputerem., a nawet doprowadzić do całkowitego zniszczenia zaatakowanego systemu. Cały problem w tym, że w większości przypadków konie trojańskie są dołączone do kodu binarnego programów i są tym samym trudne do wykrycia. Nieraz korzystają z wewnętrznych funkcji systemu. Jeśli nawet zostały przedsięwzięte odpowiednie kroki i sieć korporacyjna zabezpieczona jest przez zaporę ogniową, to prawdopodobnie ruch protokołu HTTP nie zostanie ograniczony. Okazuje się, że można napisać konia trojańskiego, który po przesłaniu pocztą e-mail do ofiary będzie zdolny do przejęcia kontroli nad owym komputerem. Do takiego zdarzenia może dojść w następujący sposób – użytkownik dostaje wiadomość przez e-mail:

Gratulacje!!! Wygrałeś telefon komórkowy, kliknij poniższy adres, aby dowiedzieć się szczegółów

WWW.SZCZESLIWA.WYGRANA.COM

Ciekawość i naiwność użytkownika nie doprowadzi go na żadną stronę internetową, za to uruchomi w tle działalność konia trojańskiego, który wymusi komunikację z komputerem napastnika na porcie 80 (uruchomi u niego serwer oczekujący połączenia z komputera ofiary). Przy tym należy powiedzieć, że zapora ogniowa nie będzie protestować, bo przecież komputer atakującego będzie jedynie „odpowiadał” na zapytania ofiary. W ten prosty sposób można doprowadzić do przejęcia kontroli nad zdalnym komputerem. Nawet po wykryciu i usunięciu *trojana* można się spodziewać, że pozostawił w systemie inne ukryte furtki, z których w przyszłości skorzystają hakerzy.

Liczba możliwych tylnych wejść dla każdej platformy jest praktycznie nieograniczona. Przykładowo, dla systemu Unix można wykorzystać ogólnie dostępny katalog /tmp do umieszczenia w nim shella z uprawnieniami superużytkownika. Innym sposobem jest ingerencja w plik konfiguracyjny inetd.conf zawierający demony różnych programów, które są uruchamiane przez demon inetd.

Aby ustrzec się przez końmi trojańskimi należy stosować się do podstawowych zasad, takich jak:

- dokładne czytanie ze zrozumieniem skryptów uruchomieniowych;
- używanie programów ze znanego i wiarygodnego źródła;
- ignorowanie wiadomości poczty elektronicznej z podejrzanymi treściami i załącznikami;
- nie należy uruchamiać nowych (szczególnie nieznanych aplikacji) na koncie z pełnymi uprawnieniami.

1.4. Główne obszary związane z bezpieczeństwem IT

Własności sieci można rozciągnąć na poszczególne obszary SKI:

- ***obszar fizyczny*** (sprzęt komputerowy, urządzenia komunikacyjne, media transmisyjne, budynki, nośniki danych, itp.);
- ***obszar osobowy*** – pracownicy powiązani ze sobą i z osobami spoza firmy tworzą tak zwane interfejsy personalne organizacji, kreują także jej wizerunek i reputację; w rozwijaniu kontaktów pomagają im zasoby, takie jak: faksy, telefony, poczta elektroniczna;
- ***obszar logiczny (sieciowy)*** – obejmuje dane i informacje, które są przechowywane na komputerach i osiągalne za pośrednictwem sieci przedsiębiorstwa; często użytkownik nie zna rzeczywistej lokalizacji tych zasobów; dostęp do informacji gwarantują interfejsy sieciowe, np. systemy telefoniczne i poczty głosowej, modemy.

1.5. Proces zapewniania bezpieczeństwa

W obrębie działań mających na celu zachowania bezpieczeństwa znajdują się cztery główne fazy:

- ocena i polityka;
- ochrona zasobów;
- monitorowanie i wykrywanie;
- reakcja i odzyskiwanie.

Na poziomie ***oceny i polityki*** określa się wymagania względem bezpieczeństwa, odpowiedzialności i rozdziału funkcji organizacyjnych.

Po ocenie sieci i stworzeniu zasad polityki bezpieczeństwa można przejść do kolejnego etapu, jakim jest ***ochrona zasobów***. Głównym celem jest wdrażanie polityki w życie przy pomocy wybranych środków technicznych. Ważnym elementem przy wprowadzaniu zabezpieczeń jest implementacja całości systemu ochrony. Wzajemne uzupełnianie się rozwiązań ochrony stanowczo polepszy bezpieczeństwo w SKI, np.: zastosowanie samej zapory ogniowej nie daje wystarczającej ochrony, ale w połączeniu z systemem wykrywania włamań IDS daje narzędzie przeciwdziałające atakom włamywaczy i wykrywające ewentualne udane próby przebicia się przez firewall'a. Chodzi o to, że pojedynczy element powinien wykonywać zadania, które dopełniają i uzupełniają funkcje i role pozostałych komponentów sieci.

Jeśli wszystkie działania związane z wdrażaniem środków ochrony zostaną zastosowane, można przejść do ***monitorowania i wykrywania***, czyli innymi słowy weryfikacji działania nowej topologii. Ten etap zobowiązuje do przeglądania konfiguracji urządzeń sieciowych i poszukiwania luk w ustawieniach, a także do monitorowania dzienników zdarzeń systemowych. Urządzenia (firewalle, rutery, serwery) posiadają usługi raportowania o błędach, logowaniach, nieudanych próbach połączeń. Informacje te są przydatne do określenia stanu bieżącego bezpieczeństwa SKI, ale zwykle są w takich ilościach, że nie starcza czasu na ich analizowanie. Oczywiście istnieje oprogramowanie, którego zadaniem jest poszukiwanie przypadków, które mogą oznaczać naruszenie zasad bezpieczeństwa. Zwracają one uwagę na takie aspekty, jak: ilość nieudanych prób logowania, próby odgadnięcia topologii sieciowej z zewnątrz, próby nieautoryzowanego dostępu. Zauważenie takich działań może w szczególnym przypadku doprowadzić do napastnika, ponieważ działa on na zasadzie testowania zabezpieczeń SKI – udany atak zawsze poprzedza kilka, czy kilkanaście nieudanych prób.

Po tak żmudnym przygotowywaniu zabezpieczeń sieciowych zdawać by się mogło, że nic już nie jest w stanie zagrozić takiej infrastrukturze. Istnieją jednak ludzie tak zdeterminowani, że znajdą każdą słabość systemu, nawet nie zdajemy sobie z tego sprawy. Są to sytuacje bardzo rzadkie, ale i na taką możliwość trzeba być odpowiednio przygotowanym. ***Reakcja i odzyskiwanie*** danych powinny być wcześniej przygotowane w dokumentach i procedurach polityki bezpieczeństwa. Jest to swoistą gwarancją, że w

skrajnym przypadku utraty danych łatwo będzie można przywrócić system do poprawnego funkcjonowania.

1.6. Metody bezpieczeństwa SKI i protokołów sieciowych

1.6.1. Organizacyjne

Metody ochrony informacji w SKI przedstawiono na podstawie sieci komputerowej, w której wykorzystano koncepcje domeny Windows 2000 Server. Proponowana sieć może składać się z dwustu urządzeń końcowych lub więcej, ponieważ proponowane rozwiązania zapewniają skalowalność sieci.

Jedna z podstawowych strategii bezpieczeństwa polega na zapewnianiu bezpieczeństwa przez stosowanie wielowarstwowych mechanizmów ochrony. Podstawą każdej bezpiecznej sieci komputerowej są zastosowane środki organizacyjne**:** (*podział kompetencji personelu, kontrola dostępu i rozliczanie czasu pracy; w głównej mierze to właśnie techniki administracyjne zabezpieczają systemy komputerowe; wprowadzenie programu ochrony informacji powinna poprzedzać analiza zagrożeń informacji oraz określenie środków im przeciwdziałających; podczas wprowadzania programów ochrony należy zarówno uwzględnić nowe procedury i metody organizacyjne, szkolenie i orientowanie się pracowników w zakresie bezpieczeństwa, jak i zapewnić możliwość kontroli*).

Niech w firmie istnieje odział informatyczny, do którego należą administratorzy systemu odpowiedzialni za całą SKI. Ponieważ osobisty kontakt i pomoc użytkownikom w tak scentralizowanej formie jest utrudniony, w każdym z oddziałów znajduje się partner, do którego zadań należy:

- bieżąca pomoc użytkownikom;
- składanie zleceń instalacji systemu i oprogramowania, zakupu nowego oraz składowania starego sprzętu;
- informowanie i szkolenie użytkowników w zakresie koncepcji realizowanej w firmie.

W systemie jest hierarchia użytkowników w związku z uprawnieniami, jakie posiadają, zrealizowana za pomocą mechanizmu grup Windows 2000. Dla zapewnienia skalowalności wprowadzono dwie domeny. Domena USER jest domeną, w której są założone konta użytkowników, a domena RESOURCES jest domeną, w której założone są konta komputerów pracujących w sieci lokalnej. Domena RESOURCES ufa domenie USER. W ten sposób administrator domeny RESOURCES, której zasoby znajdują się tylko z sieci z lokalizacji oddziału FIRMY1, nie ma dostępu do zasobów oddziału FIRMY2. Jednocześnie administrator domeny USER może znajdować się tylko w jednej lokalizacji, z której zarządza kontami wszystkich użytkowników FIRMY1 i FIRMY2. Pracownicy przedsiębiorstwa mogą zmieniać lokalizacje i mieć dostęp do tego samego konta, możliwa jest też łatwa rozbudowa. Użytkownik otrzymując konto w domenie USER nie ma uprawnień do instalacji nowego

oprogramowania na komputerze. Istnieje tylko jedno konto lokalne administratora na komputerze, do którego hasło znają administratorzy, a przechowywane jest na serwerze zdalnej instalacji. Wyjątkiem mogą być Laptopy, które używane są poza przedsiębiorstwem i ze względu na potrzebę zmiany konfiguracji wymagane jest ujawnienie lokalnego hasła administratora.

W SKI obowiązuje zasada przyznawania minimum uprawnień. Dzięki temu w przypadku zagrożenia na niebezpieczeństwo narażony jest tylko fragment systemu. Każdy użytkownik ma swoją przestrzeń na dysku, do której tylko on ma dostęp. Dodatkowo każdy oddział ma swój katalog, do którego dostęp zostaje przyznany tylko pracownikom danej jednostki. Dla przeprowadzanych projektów, w których uczestniczą osoby z różnych oddziałów, także tworzony jest Katalog z odpowiednimi uprawnieniami. Do wszystkich powyższych zastosowań wykorzystane zostaną Access Control List.

Ponieważ, zmiany personelu oraz ilość przeprowadzanych projektów jest duża, potrzebny jest sposób dokumentacji zmian wprowadzanych w systemie. Dokumentacja użytkowników, zasobów sprzętowych oraz udostępnianych katalogów prowadzona jest przy pomocy bazy danych, gdzie zawarte są informacje:

Tabela 1.2. Użytkownik

Imię	Nazwisko	Identyfikator w systemie	Zakres dostępnych usług np. www, ftp, VPN

Tabela 1.3. Zasoby sprzętowe

Nazwa komputera	Adres IP	MAC	Nazwisko pracownika	Partner IT	Zainstalowane pakiety

Tabela 1.4. Udostępniane katalogi

Nazwa katalogu	Nazwa udziału	Grupy z prawami dostępu	Odp. partner IT

Prowadzenie bazy danych należy do grupy administratorów, do nich należy także obowiązek dokumentowania wszystkich zmian i zdarzeń w systemie. Instalacje systemu i oprogramowania przeprowadzane są zdalnie na żądanie partnera.

Mechanizmy, które wspomagają wyżej wymienione metody zabezpieczeń w systemie Windows 2000 Server, obejmują:

- *Uwierzytelnianie Kerberosem v5* — jest to domyślna metoda uwierzytelniania w Windows 2000, pozwalająca na o wiele łatwiejsze zarządzanie relacjami zaufania oraz bezpieczniejszą uwierzytelniania niż metoda używana przez Windows NT 4 (NTLM). Kerberos dzieli klucze tajne z urządzeniami w sieci poprzez serwer centralny, wobec czego gra rolę zewnętrznego certyfikatora i arbitra.
- *Zaszyfrowany system plików* (EFS – *Encrypted File System*) — pozwala na szyfrowanie danych na partycjach NTFS, chroniąc je przed niepowołanym dostępem osób mogących mieć dostęp fizyczny do komputera lub dysku twardego.
- *IPSec* — pozwala na tworzenie bezpiecznych dwustronnych połączeń w sieciach IP.
- *Infrastruktura klucza publicznego* — kryptografia klucza publicznego pozwala na bezpieczną wymianę danych z innymi osobami przez nie zabezpieczone łącza, np. Internet.
- *Obsługa kart inteligentnych (Smart Card)* — karty inteligentne pozwalają na przenoszenie poświadczeń zabezpieczeń i innych prywatnych danych w sposób bezpieczny. Użytkownicy mogą korzystać z kart inteligentnych do bardziej bezpiecznego uwierzytelniania niż za pomocą nazwy użytkownika i hasła.

Każda infrastruktura zabezpieczeń jest z definicji budowana na dwóch kamieniach węgielnych:

- *Protokół (protokoły) zabezpieczeń* — definiują, jak dokładnie użytkownik jest w stanie udowodnić systemowi, że jest tym, za kogo się podaje (uwierzytelnianie) i zapewniają bezpieczeństwo komunikacji pomiędzy użytkownikiem i systemem.
- *Algorytm(y) szyfrowania* — pozwalają protokołom zabezpieczeń na ochronę przed podglądaniem danych wymienianych pomiędzy użytkownikiem a systemem.

Dla systemu Windows 2000 Server, Microsoft wykorzystał najlepsze możliwe standardy dla każdego obszaru zabezpieczeń i dodał je do arkusza specyfikacji produktu, aby zwiększyć jego możliwości współpracy. W konsekwencji Windows 2000 Server zawiera oprócz starego zbioru własnych protokołów (NTLM, Secure RPC i PPTP) również obsługę takich protokołów, jak Lightweight Directory Access Protocol (LDAP), Kerberos, Public Key Cryptography Standard (PKCS) i IP Security (IPSec). To samo można powiedzieć o szyfrowaniu, które obejmuje obecnie DES, 3DES, RSA, RC4, które zostaną przedstawione w dalszej częsci.

Reakcje na próby ataku na system

W przypadku ataku na system ważną sprawą jest prawidłowa reakcja na wykrycie faktu udanego bądź nie udanego ataku na bezpieczeństwo systemu. W razie wykrycia na przykład działania dziwnych procesów w SKI, wielokrotnych prób zalogowania się na konto administratora czy modyfikacji pliku lub katalogu, należy natychmiast podjąć zaplanowane uprzednio środki bezpieczeństwa. Należą do nich:

- szczegółowa analiza zaistniałej sytuacji;
- zatrzymanie pracy całego lub części systemu w celu zapobieżenia powstaniu nowych szkód, poinformowanie użytkowników o zaistniałym zagrożeniu.

Istotnym jest zapisanie stanu zaatakowanego systemu w celu późniejszej dokładnej analizy zaistniałej sytuacji.

Odtworzenie ostatnio zachowanego stanu systemu z archiwów

W celu wyeliminowania efektów działań intruza należy odtworzyć poprzedni stan systemu. Należy przy tym pamiętać, iż:

- poprzedni stan systemu może również zawierać modyfikacje wprowadzone przez napastnika, o ile zagrożenie nastąpiło po jego zapisie;
- zostaną utracone modyfikacje systemu, jakie wykonano przed sporządzeniem ostatniej kopii zapasowej.

Konieczność wcześniejszego opracowania planu działania w przypadku awarii

Bardzo ważną sprawą jest odpowiednio wczesne przygotowanie planu działania w przypadku odkrycia zagrożenia. W szczególności należy przygotować plan wstrzymywania pracy SKI zawierający opis sposobu sprawnego informowania użytkowników. Działanie zgodnie z opracowanym wcześniej planem znacząco ułatwia likwidację skutków zagrożenia.

1.6.2. Techniczne

- środki fizyczne oraz identyfikacja, uwierzytelnienie i upoważnienie personelu; zabezpieczenia fizyczne takie jak bramy, kraty itp. umożliwiają odgrodzenie obszarów o ograniczonym dostępie oraz kontrole użytkowników wchodzących lub wychodzących z nich; jednak żaden system bezpieczeństwa nie będzie skuteczny, jeśli osoba zawiedzie zaufanie;
- są podstawą, dzięki której możliwa jest realizacja założeń polityki bezpieczeństwa.

Pierwszą warstwą zabezpieczeń, którą należy wziąć pod uwagę, jest bezpieczeństwo fizyczne stacji roboczych. Ważna jest kontrola dostępu i zabezpieczenia przed kradzieżą. Kontrola dostępu jest realizowana na poziomie systemu operacyjnego. Wspomagane tej metody poprzez uaktywnienie hasła BIOS'u nie jest uzasadnione na komputerach stacjonarnych, ponieważ atakujący może łatwo ominąć to zabezpieczenie np. wyjąć baterię lub zresetować pamięć CMOS. Natomiast w Laptopach jest wymagane, ze względu na charakter korzystania z nich, w miejscach gdzie dostęp fizyczny do Laptopa mają osoby całkowicie postronne (poza terenem firmy). Takie zabezpieczenie uniemożliwia szybką zmianę ustawień BIOS'u lub uruchomienie systemu z dyskietki przez atakującego. Na teren przedsiębiorstwa mają dostęp osoby tylko do tego upoważnione, dlatego takie niebezpieczeństwo jest zminimalizowane. Pomieszczenia w których znajdują się komputery powinny jednak posiadać dodatkowe zabezpieczenie np. monitoring. Należy także podjąć działania pozwalające zidentyfikować sprzęt po jego kradzieży. Oprócz dokładnej inwentaryzacji sprzętu warto posłużyć się dodatkowo technikami pozwalającymi zidentyfikować sprzęt bez rozkręcania obudowy, np. poprzez oznaczenia niezmywalną farbą, farbą fluoroscencyjną czy reagującą na ultrafiolet.

Sieć zbudowana w topologii gwiazdy jest scentralizowana, stacje robocze jednego segmentu sieci są podłączone do jednego urządzenia switcha. Zaletą takiego rozwiązania jest bezpośrednie uniezależnienie się od innych stacji roboczych, izolacja transmisji, możliwość zarządzania każdym komputerem z osobna. Centralizacja wymusza istnienie krytycznego punktu, którego awaria ma bardzo złe skutki. Jeśli atakujący wyłączy na przykład switch, może odciąć od reszty sieci cały segment. Dlatego też wszelkie urządzenia sieciowe, jak routery, switche muszą być odpowiednio zabezpieczone. Ataki na sprzęt są dużo groźniejsze niż na oprogramowanie. O ile awaria pojedynczego komputera może nie być zauważona przez resztę sieci, awaria rutera może w całości ją unieruchomić. Zazwyczaj udane ataki na sprzęt sieciowy wynikają z prostych błędów wynikających z zaniedbania administratorów. Wielu z nich zapomina o włączenia kodowania podczas konfiguracji zdalnej albo o zmianie domyślnych

haseł. Duża część z nich pozwala na ominięcie hasła w przypadku dostępu fizycznego (choćby przycisk resetujący NVRAM).

Dostęp do serwerowni jak i szaf z osprzętem sieciowym musi być ograniczony i być dostępnym tylko dla administratorów. Dostęp do urządzeń, pomieszczeń, a także możliwość naliczania czasu pracy umożliwiają karty magnetyczne, współpracujące z odpowiednim oprogramowaniem. Należy zwrócić uwagę, że do każdego z tych pomieszczeń możliwy jest dostęp tradycyjny, ponieważ w wyniku awarii lub braku zasilania uniemożliwiony by został dostęp do ważnych pomieszczeń. Klucze jednak powinny być w normalnych warunkach nie udostępniane.

Backup

Plan archiwizowania danych musi być tak opracowany, by umożliwiał przywrócenie stanu systemu z przed awarii z możliwie dużą wiernością. Z użytkownikami należy uzgodnić jakie dane i w jakich odstępach czasowych należy archiwizować. W większości przypadków odpowiednim jest zastosowanie opcji „Full Backup" zaplanowanej na weekend oraz Differential Backup w każdy dzień tygodnia. Dla zapewnienia możliwości odzyskiwania danych potrzebne jest zaplanowanie jak długo przechowywane będą dane na taśmach. Dla zminimalizowania ilości nośnika plan przechowywanych taśm będzie wyglądać następująco:

- kopie różnicowe: 4 tygodnie;
- kopie pełnej archiwizacji wykonywane na koniec miesiąca: 4-6 miesięcy;
- pozostałe kopie pełnej archiwizacji: 4 tygodnie.

Wszystkie nośniki z danymi składowane są w oddzielnym ognioodpornym pomieszczeniu, do którego dostęp został ograniczony w taki sposób jak do serwerowni.

1.6.3. Kryptograficzne

Dobre rozwiązanie problemów bezpieczeństwa sieci komputerowych wymaga zwykle połączenia środków organizacyjnych, technicznych i kryptograficznych. Udział poszczególnych elementów zależy od znaczenia chronionych informacji, rodzaju zagrożenia i dostępnych środków.

Kryptografia – dziedzina wiedzy zajmująca się zasadami, narzędziami i metodami przekształcania danych w celu ukrycia zawartych w nich onformacji, zapobiegania mozliwości tajnego ich modyfikowania lub eliminacji dostępu do nich osobom niepowołanym.

Podstawowym zadaniem kryptografii jest utrzymanie w tajemnicy tekstu jawnego (bądź klucza, bądź obu elementów jednocześnie) przed wścibskimi (zwanymi również przeciwnikami, atakującymi, podsłuchującymi, intruzami lub po prostu wrogami) [4]. Chcą oni uzyskać pełen dostęp do komunikacji między nadającym i odbiorcą.

Działaniami stojącymi w opozycji do krytpografii zajmuje się **kryptoanaliza –** nauką o odtwarzaniu tekstu jawnego bez znajomości klucza [5]. Skuteczna kryptoanaliza umożliwia odtworzenia tekstu jawnego lub klucza. Zajmuje się również wyszukiwaniem słabych punktów systemów kryptograficznych, punktów, które mogłyby otworzyć drogę do poznania tekstu jawnego lub klucza. (Utrata tajności klucza wskutek działań niekryptoanalitycznych jest nazywana kompromitacją).

Stosowanie kryptoanalizy nazywa się łamaniem szyfru (*atak*) [6]. Podstawowym założeniem kryptoanalizy, po raz pierwszy sformułowanym w dziewiętnastym wieku przez holendra A. Kerckhoffs'a, jest założenie (ang. *Kerckhoffs' assumption*), że bezpieczeństwo algorytmu kryptograficznego jest oparte wyłącznie na kluczu [7]. Kerckhoffs założył, że kryptoanalityk zna wszystkie szczegóły algorytmu szyfrowania i jego implementacji, nie zna natomiast zastosowanych kluczy. Nie jest to co prawda założenie prawdziwe w wielu realnych sytuacjach, lecz jest to założenie, które warto przyjąć. Jeśli nie można złamać szyfrogramu wiedząc, jak działa algorytm szyfrujący, to na pewno nie uda się go złamać nie wiedząc, jak ten algorytm działa.

Połączenie kryptografii i kryptoanalizy stanowi dziedzina wiedzy **kryptologia**.

---

[4] **Schneier B. „Kryptografia dla praktyków", WNT, 2002.**

[5] **Grzywak A. Bezpieczeństwo systemów komputerowych, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.**

[6] **Schneier B. „Kryptografia dla praktyków", WNT, 2002.**

[7] **Kerckhoffs A. „La cryptographie militaire";**
Shannon C. Communication Theory if Secrecy Systems" Bell System Technical *Jurnal,* 1948;
Bauer F. L. „Sekrety kryptografii", Helion, 2002.