Wykl 2 i 3

2.1. Podstawowe założenia bezpieczeństwa sieci komputerowej

Bezpieczeństwo sieci jest nieodłącznie związane z trzema zagadnieniami: poufnością, integralnością i dostępnością (ang. *Confidentiality, Integrity* oraz *Availability,* C-I-A). W zależności od kontekstu i konkretnego zastosowania, niektóre z tych zagadnień mogą być bardziej kluczowe od pozostałych. Przykładowo, w agencji rządowej w sieci mogą być przesyłane elektronicznie zaszyfrowane dokumenty, co chroni je przed dostępem niepowołanych osób. W tym przypadku poufność informacji jest zagadnieniem kluczowym. Jeśli nieupoważniona osoba uzyska możliwość złamania szyfru i przesłania do odbiorców zmodyfikowanej postaci dokumentu, zostanie naruszona integralność przekazu. Z drugiej strony organizacje zajmujące się handlem w Internecie odniosą znaczne straty finansowe w przypadku niedostępności usług przez dłuższy czas. W takich przypadkach kluczowym zagadnieniem jest dostępność.

• **Poufność informacji** polega na jej zabezpieczeniu przed dostępem osób niepowołanych. Złamanie poufności może być celowe, na przykład w razie złamania zabezpieczeń i odczytania informacji, lub przypadkowe, wskutek nieuwagi lub braku kompetencji użytkowników biorących udział w przekazywaniu informacji.

• **Dostępność** informacji zapewnia autoryzowanym użytkownikom bieżący i nieprzerwany dostęp do danych w systemie i sieci.

• **Integralność** – nienaruszenie oryginalnej postaci danych.

Integralność informacji realizuje dwie funkcje.

1. Zapobiega nieautoryzowanym lub przypadkowym modyfikacjom informacji przez osoby upoważnione.
2. Zapewnia spójność wewnętrzną i zewnętrzną:
   - *spójność wewnętrzna* dotyczy wewnętrznych zależności pomiędzy danymi, na przykład w bazie danych suma elementów w całej organizacji musi równać się sumie elementów przypisanych poszczególnym jednostkom organizacji;
   - *spójność zewnętrzna* zapewnia zgodność informacji zapisanych w bazie danych ze stanem rzeczywistym, na przykład całkowita liczba elementów na półkach w magazynie musi odpowiadać całkowitej liczbie elementów uwzględnionych w bazie.

Do zagrożeń poufności należą:

• *przeglądanie,* polegające na przeszukiwaniu pamięci głównej (operacyjnej) i zewnętrznej komputerów w celu uzyskania określonych informacji,

• *przenikanie,* związane z dostępem do chronionych danych w czasie legalnych operacji wykonywanych na tych danych przez upoważnionych użytkowników (chociażby przeglądanie danych w czasie ich transmisji niedostatecznie zabezpieczonym kanałem, np. „podglądanie" przesyłanych haseł użytkowników rozpoczynających pracę w systemie),

• *wnioskowanie,* polegające na wydobywaniu tajnych, szczegółowych informacji ze zbioru ogólnych i jawnych informacji statystycznych na dany temat. Na przykład: zakładamy, że znamy liczbę pracowników pewnej firmy, średnie wynagrodzenie w tej firmie i średnie wynagrodzenie pracowników firmy posiadających wykształcenie wyższe. Zakładając, że X jest jedynym pracownikiem ,firmy nie posiadającym wykształcenia wyższego, możemy na podstawie powyższych informacji statystycznych ustalić jego wynagrodzenie.

Do zagrożeń autentyczności zaliczamy:
• *zniekształcanie danych,* będące ich modyfikacją nie zmieniającą sensowności z merytorycznego punktu widzenia. Np. zmieniamy wartość wynagrodzenia pracownika z 800 złotych na 1000.
• *powtarzanie danych,* np. ponawianie komunikatu w systemie komputerowym banku, zgodnie z którym na pewne konto ma być przelana określona suma.
• *wstawianie danych,* np. wstawianie pomiędzy już istniejące nowych zleceń wydania towaru z magazynu w komputerowym systemie zarządzania magazynem,
• *niszczenie danych,* jako akt wandalizmu lub świadomego działania na szkodę organizacji.

2.2. Ochrona dogłębna

Metodologia ochrony dogłębnej opiera się na wielowarstwowym schemacie zabezpieczeń poszczególnych elementów systemu informatycznego. Strategia ochrony dogłębnej obejmuje następujące obszary:
- ochrona sieci i infrastruktury;
- ochrona granicy enklawy;
- ochrona środowiska komputerowego;
- infrastruktury pomocnicze.

Termin **enklawa** w kontekście definicji ochrony dogłębnej oznacza „*zbiór środowisk komputerowych, połączonych jedną lub większą liczbą sieci lokalnych pod wspólną kontrolą z zastosowaniem jednolitej polityki bezpieczeństwa*''. Kontrola ta obejmuje również bezpieczeństwo związane z personelem oraz fizyczne bezpieczeństwo systemów. Enklawy stanowią zawsze najwyższą kategorię zabezpieczeń, zarówno w przypadku zastosowania zautomatyzowanego systemu informatycznego jak i procesów informatycznych świadczonych przez firmy trzecie (ang. *outsourcing).* Ich wymogi bezpieczeństwa są uzależnione od tych systemów. Enklawy zapewniają podstawową właściwość zabezpieczenia informacji które są realizowane jako zabezpieczenia granicy enklawy, mechanizmy wykrywania incydentów i odpowiadania na nie oraz zarządzanie kluczami. Enklawy mają również znaczenie funkcjonalne, na przykład automatyzacja zadań biurowych czy obsługa poczty elektronicznej. Szczegóły implementacji enklaw są uzależnione od organizacji lub misji i środowiska. Ich działania mogą być zdefiniowane na podstawie fizycznie zbliżonego położenia lub realizowanych funkcji, niezależnie od lokalizacji. Przykładami enklaw mogą być sieci lokalne (LAN) oraz obsługiwane przez nie konfiguracje, sieci szkieletowe i centra przetwarzania danych.
Enklawy dzielą się na publiczne, prywatne oraz tajne.

Strategia ochrony dogłębnej opiera się na trzech elementach: ludziach, technologii i działaniach.

• Ludzie
W celu implementacji efektywnych mechanizmów zabezpieczenia informacji w organizacji, jej zarząd musi mieć bezpośredni, wysokopoziomowy wpływ na ten proces. Ten wpływ można podzielić na następujące zagadnienia:
- rozwój polityki i procedur zabezpieczania informacji;
- przydzielanie ról i odpowiedzialności;
- szkolenia kluczowego personelu;
- egzekwowanie odpowiedzialności personelu;
- przydzielanie zasobów;
- organizacja kontroli bezpieczeństwa fizycznego;

- organizacja kontroli bezpieczeństwa personelu;
- wyciąganie konsekwencji z zachowania niezgodnego z ustalonymi zasadami.

• Technologia
Organizacja musi zapewnić, aby do realizacji usług zabezpieczenia informacji były stosowane właściwe technologie. Ten cel można osiągnąć biorąc pod uwagę następujące zagadnienia podczas doboru technologii:
- polityka bezpieczeństwa;
- standardy zabezpieczenia informacji na poziomie systemu;
- podstawowe zasady zabezpieczenia informacji;
- kryteria specyfikacji dla odpowiednich produktów związanych z zabezpieczaniem informacji;
- uzyskanie dostępu do wiarygodnych, zweryfikowanych produktów oferowanych przez firmy trzecie;
- wymagania konfiguracyjne;
- procesy określające ryzyko systemów zintegrowanych.

• Działania
Działania skupiają się na operacjach i elementach niezbędnych do codziennej realizacji strategii bezpieczeństwa organizacji. Te operacje i elementy obejmują:
- przejrzystą i dostosowaną do realiów politykę bezpieczeństwa;
- egzekwowanie polityki bezpieczeństwa informacji;
- certyfikację i akredytację;
- zarządzanie odpowiednimi postawami związanymi z bezpieczeństwem informacji;
- usługi zarządzania kluczami;
- oszacowanie gotowości;
- zabezpieczenie infrastruktury;
- oszacowanie bezpieczeństwa systemów;
- monitorowanie i reagowanie na zagrożenia;
- wykrywanie ataków, generowanie ostrzeżeń i odpowiedzi;
- odtwarzanie systemu po uszkodzeniu.

2.3. Typy ataków
Strategia ochrony dogłębnej jest zdefiniowana w taki sposób, aby chronić przed następującymi typami ataków.

• Atak pasywny. Ataki tego typu obejmują analizę ruchu, monitorowanie niezabezpieczonej komunikacji, odszyfrowanie ruchu sieciowego zaszyfrowanego słabymi algorytmami kryptograficznymi i przechwytywanie informacji uwierzytelniających (na przykład haseł). Pasywne przejmowanie informacji w sieci może posłużyć włamywaczom jako źródło informacji oraz jako ostrzeżenie na temat podjętych przeciwdziałań. Ataki pasywne mogą ujawnić napastnikowi pewne dane i pliki bez potrzeby uzyskania zgody i wiedzy użytkowników. Przykładem danych przejętych w ten sposób mogą być dane osobiste, takie jak numery kart kredytowych.

• Atak aktywny. Ataki tego typu polegają na próbach obejścia lub złamania zabezpieczeń, między innymi z wykorzystaniem szkodliwego kodu lub na kradzieży lub modyfikowaniu informacji. Te ataki mogą być przeprowadzane na sieci szkieletowej organizacji, mogą polegać na wykorzystaniu transmitowanej informacji, elektronicznej penetracji granicy enklawy lub ataku na autoryzowanego użytkownika podczas próby zdalnego zalogowania się

w enklawie. Ataki aktywne mogą posłużyć do ujawnienia lub rozpowszechnienia danych, blokady usług lub modyfikacji danych.

• **Zbliżenie.** Ataki tego typu polegają na uzyskaniu fizycznego dostępu do sieci, systemów lub pomieszczeń w celu dokonania modyfikacji, uzyskania dostępu lub zablokowania dostępu do informacji. Zbliżenie może być dokonane przez działania potajemne lub jawne, może też być wynikiem połączenia tych dwóch metod działania.

• **Ataki od wewnątrz.** Takie ataki mogą mieć charakter złośliwy lub niezłośliwy. *Ataki złośliwe* polegają na celowym podsłuchiwaniu, kradzieży lub uszkadzaniu informacji i wykorzystywaniu ich do celów majątkowych. Mogą również polegać na blokowaniu dostępu do informacji autoryzowanym użytkownikom. *Ataki niezłośliwe* z reguły wiążą się z lekkomyślnością, brakiem kompetencji lub celowym sprzeniewierzeniem się zasadom dla uproszczenia sobie realizacji legalnego zadania.
Należy pamiętać, że ponad 80% ataków na systemy pochodzi z wnętrza sieci. Z tego względu nie należy ufać własnym pracownikom, bardzo częstym przypadkiem jest pracownik podczas okresu wymówienia, który postanawia „odegrać się na firmie". Dlatego też użytkownicy w sieci nie powinni mieć większych możliwości niż bezwzględnie jest im to potrzebne.

• **Dystrybucja.** Takie ataki polegają na modyfikacji sprzętu i oprogramowania na etapie wytwarzania lub dystrybucji. Ataki tego typu polegają na włączeniu do produktu złośliwego kodu, na przykład „tylnych drzwi'' (ang. *back door),* dzięki czemu włamywacz będzie miał w przyszłości dostęp do systemów korzystających z tych produktów.

2.4. Techniki wykorzystywane w metodologii ochrony dogłębnej

• **Obrona w wielu miejscach** — mechanizmy zabezpieczające są instalowane w wielu różnych miejscach, aby zabezpieczyć przed zagrożeniami z zewnątrz i z wewnątrz.
• **Obrona warstwowa** — mechanizmy bezpieczeństwa i detekcji są implementowane w taki sposób, że włamywacz lub zagrożenie musi pokonać kilka różnych barier przed uzyskaniem dostępu do krytycznej informacji.
• **Jakość zabezpieczeń** — szacowanie trwałości i jakości zabezpieczeń z uwzględnieniem wartości zabezpieczanego elementu systemu i każdego elementu mechanizmów zabezpieczania informacji. Jakość zabezpieczeń jest mierzona poziomem zabezpieczania i siłą poszczególnych elementów zabezpieczających.
• **Wykorzystanie zarządzania kluczami** — zastosowanie skutecznych infrastruktur zarządzania kluczami oraz infrastruktur kluczy publicznych.
• **Zastosowanie systemów detekcji włamań** — systemy detekcji włamań służą do analizy informacji, oceny wyników i w miarę potrzeby do podejmowania odpowiednich działań w wyniku próby włamania.

Wskazówki mające zapewnić efektywność implementacji metodologii ochrony dogłębnej :

• Decyzje dotyczące zabezpieczenia informacji powinny być oparte na analizie ryzyka i podstawowych celach operacyjnych organizacji.
• Należy wykorzystywać wszystkie trzy elementy metodologii ochrony dogłębnej: ludzi, działania i technologię. Najlepsze środki technologiczne nie będą dawały dobrych rezultatów bez odpowiednio wyszkolonych pracowników oraz procedur działania definiujących ich wykorzystanie.

• Należy opracować odpowiedni program edukacji, szkoleń, nabywania doświadczenia i świadomości. Zwiększanie fachowości, potwierdzane odpowiednimi certyfikatami, pozwala na pozyskiwanie kadry ekspertów bazując na administratorach systemów.
• Należy przeanalizować możliwość zastosowania dostępnych produktów gotowych, ograniczając własne wytwarzanie elementów systemu do tych, które nie są dostępne w inny sposób.
• Okresowo należy szacować stan infrastruktury zabezpieczenia informacji. Narzędzia specjalizowane, takie jak zautomatyzowane skanery sieci mogą służyć do oceny podatności na ataki.
• Należy wziąć pod uwagę nie tylko działania o wrogich intencjach, lecz również działania związane z nieuwagą lub brakiem odpowiedzialności użytkowników.
• Należy zastosować kilka różnych sposobów ograniczania zagrożeń i uwzględnić zasadę nakładania się zabezpieczeń, aby zapobiec przewidywalnym zdarzeniom. Dzięki temu utrata jednego z zabezpieczeń nie będzie groziła natychmiastową kompromitacją infrastruktury informatycznej.
• Należy się upewnić, że fizyczny dostęp do systemów mają tylko zaufani pracownicy. Istnieje wiele środków służących do implementacji tej zasady, takich jak odpowiednia analiza przeszłości pracowników, kontrola dostępu, szczelny system uprawnień czy wykorzystanie identyfikatorów przez pracowników.
• Do zgłaszania incydentów wykrytych przez systemy detekcji włamań należy stosować ustalone procedury, aby uprościć odpowiednim służbom analizę i podjęcie odpowiednich działań.

2.5. Zarządzanie ryzykiem

Etapy zarządzania ryzykiem

- Oszacowanie ryzyka
- Minimalizacja ryzyka
- Analizy i oceny

2.5.1.Oszacowanie ryzyka składa się z etapów:

- Identyfikacja i ocena ryzyka;
- Identyfikacja i ocena skutków potencjalnego incydentu;
- Rekomendacja działań redukujących ryzyko.

Oszacowanie ryzyka obejmuje:

- Scharakteryzowanie systemu.
- Identyfikacja zagrożeń.
- Identyfikacja słabych punktów.
- Analiza mechanizmów kontrolnych.
- Określenie prawdopodobieństwa.
- Analiza skutków.
- Określenie ryzyka.
- Zalecenia kontrolne.
- Dokumentacja wynikowa.

Należy również rozważyć metody ochrony stacji roboczych ze specjalnym uwzględnieniem komputerów administratorów, z uwagi na ich uprzywilejowanie w dostępie, znajdującą się na nich dokumentację itp.
Projektując politykę bezpieczeństwa, należy pamiętać, że ponad 80% ataków na systemy pochodzi z wnętrza sieci. Z tego względu nie należy ufać własnym pracownikom, dlatego też użytkownicy w sieci nie powinni mieć większych możliwości niż bezwzględnie jest im to potrzebne.
Ograniczenia nakładane na użytkowników powinny tworzyć czytelne reguły dostępu do różnych zasobów i umożliwiać szybką lokalizację nielojalnego lub nieostrożnego pracownika.
Użytkownik powinien również ponosić odpowiedzialność za zachowanie w tajemnicy haseł, dokumentacji, informacji o systemach używanych w firmie, o topologii sieci komputerowej, metodach jej zabezpieczeń i szczegółach polityki bezpieczeństwa.
Każdy użytkownik powinien zostać przeszkolony w dotyczących go zagadnieniach bezpieczeństwa.
Należy także uczulić użytkowników na sytuacje niestandardowe, przykładowo administratora dzwoniącego z prośbą o podanie hasła. Zmniejszymy tym samym niebezpieczeństwo ataków typu „inżynieria społeczna".
Socjotechnika często pozwala na uzyskanie wielu informacji, których zdobycie w przypadku zastosowania środków technicznych wymagałoby znacznych nakładów czasowych i finansowych.

2.5.2. Minimalizacja ryzyka

- Ustalenie priorytetów odpowiednich działań zidentyfikowanych w procesie oszacowania ryzyka;
- Implementacja działań zmniejszających ryzyko;
- Utrzymanie działań zmniejszających ryzyko.

Ograniczenie ryzyka
Proces ograniczania ryzyka służy do ustalenia priorytetów, oceny i implementacji mechanizmów kontrolnych, opracowanych w wyniku procesu oszacowania ryzyka. Ryzyka nie można wyeliminować w sposób kompletny, natomiast implementacja musi być uzasadniona z punktu widzenia kosztowego. Z reguły należy przyjąć zasadę minimalizacji kosztów z jednoczesnym zachowaniem minimalnych skutków negatywnych na systemie informatycznym.
Mechanizmy kontrolne
Mechanizmy kontrolne dzieli się na zapobiegawcze i wykrywające.
♦ **Mechanizmy zapobiegawcze** — do tego typu mechanizmów zalicza się kontrolę dostępu do nośników oraz ich właściwe wycofywanie z użytku, ograniczanie zewnętrznej dystrybucji danych, kontrola wirusów oprogramowania, zabezpieczanie szaf dystrybucyjnych, mechanizmy kopii zapasowych, zabezpieczanie komputerów przenośnych i osobistych, zabezpieczanie infrastruktury informatycznej przed pożarem, zapewnienie awaryjnych źródeł zasilania oraz kontrolę wilgotności i temperatury.
♦ **Mechanizmy wykrywające** — do tych mechanizmów zalicza się zapewnienie fizycznego bezpieczeństwa z użyciem kamer, wykrywaczy ruchu i zapewnienie bezpieczeństwa środowiskowego z użyciem detektorów dymu, czujników i alarmów.

2.5.3. Ocena i analiza

Ryzyko, które istnieje mimo zaimplementowania mechanizmów kontrolnych nazywa się **ryzykiem pozostałym** bądź **szczątkowym**. Wszystkie systemy w pewnym stopniu mu

podlegają, ponieważ pełne wyeliminowanie ryzyka systemów informatycznych jest praktycznie niemożliwe.
Proces analizy i oceny jest procesem ciągłym. Na przykład wyznaczona instytucja bądź osoba akceptująca (ang. *designated approving authority,* DAA) ma obowiązek badania pozostałego ryzyka systemu i decydowania, czy jego poziom jest nadal akceptowalny lub czy jest konieczne zastosowanie dodatkowych środków zmniejszających ryzyko w celu akredytacji systemu informatycznego.
DAA odpowiada za utrzymanie bezpieczeństwa systemu. Jest to z reguły członek zarządu z odpowiednimi uprawnieniami i kompetencjami do oceny równowagi pomiędzy potrzebami systemu a ryzykiem bezpieczeństwa. Ta osoba określa akceptowalny poziom ryzyka systemu. Zarząd oraz DAA jest odpowiedzialny za autoryzację i akredytację systemu informatycznego. DAA oddając system informatyczny do użytku (akredytując system) podpisuje oświadczenie akceptacji pozostałego ryzyka.

2.6. Zarządzanie bezpieczeństwem systemu informatycznego

Na zarządzanie bezpieczeństwem systemu informatycznego składa się kilka technik pozwalających w znacznym stopniu na zminimalizowanie ryzyka naruszenia poufności, integralności oraz dostępności informacji. Narzędzia i techniki zarządcze, choć nie tak spektakularne jak zaawansowane rozwiązania techniczne, mogą być bardzo skuteczne w implementacji i utrzymaniu bezpieczeństwa systemu przy rozsądnych kosztach. Do tego typu narzędzi zalicza się politykę bezpieczeństwa, planowanie urlopów, sprawdzanie historii kariery pracowników, szkolenia kształtujące świadomość bezpieczeństwa oraz planowanie zdarzeń.

2.6.1.Plan ochrony

Plan ochrony opracowywany jest głównie przez osoby opiekujące się systemem komputerowym. Jego realizacja ciąży zarówno na administratorach, jak i na pozostałych użytkownikach systemu.
W planie bezpieczeństwa powinny być zawarte następujące elementy:

- Opis realizacji metod kontroli dostępu do systemu.
- Opis realizacji metod kontroli dostępu do zasobów systemu.
- Opis metod okresowego lub stałego monitorowania systemu.
- Dokładny (na poziomie technicznym) opis metod reagowania na wykrycie zagrożenia.
- Opis metod likwidacji skutków zagrożeń (np. tworzenia kopii zapasowych).

2.6.2.Rola użytkowników systemu komputerowego w zapewnieniu bezpieczeństwa

Należy podkreślić niezwykle istotną rolę użytkowników systemu komputerowego organizacji w zapewnieniu jego bezpieczeństwa. Nawet najlepiej zaprojektowany i wdrożony system zabezpieczeń nie zda się na nic, jeśli użytkownicy nie będą korzystali z niego w sposób poprawny. Jeżeli nie będą podporządkowywać się wymogom *polityki bezpieczeństwa,* w systemie powstaną wyłomy, przez które będą mogli wedrzeć się intruzi.
Pierwszy z problemów wiąże się z ignorancją. Użytkownicy systemu nie zdają sobie sprawy z zagrożeń ani z konsekwencji, jakie mogą wynikać z ich działań. Dlatego zadaniem osób opiekujących się systemem jest ukazywanie istniejących niebezpieczeństw i przyzwyczajanie użytkowników do wypełniania procedur bezpieczeństwa.
Drugi problem wynika z lenistwa zarówno „zwykłych" użytkowników systemu, jak i jego administratorów. Niedopełnianie wymogów bezpieczeństwa, zwłaszcza przez osoby opiekujące się systemem, może powodować bardzo poważne zagrożenia.
Hierarchizacja uprawnień użytkowników systemu

W systemie wprowadzona zostaje hierarchia użytkowników w związku z uprawnieniami, jakie posiadają. Użytkownicy pełniący funkcje administracyjne mają większe prawa niż użytkownicy tych funkcji nie pełniący. Administratorzy poszczególnych podsystemów (np. podsystemu drukowania czy podsystemu poczty elektronicznej) posiadają mniejsze prawa niż administratorzy główni itd. Obowiązuje zasada przyznawania minimum uprawnień. Dzięki temu w przypadku zagrożenia na niebezpieczeństwo narażony jest tylko fragment systemu.

Wielowarstwowy mechanizm ochrony

Pierwszą linię obrony stanowi ograniczanie fizycznego dostępu do systemu komputerowego. Realizowane jest to przez zamykanie komputerów w pomieszczeniach, do których dostęp odbywa się przy uwierzytelnieniu np. za pomocą karty magnetyczne, lub wstukania kodu dostępu na klawiaturze przy drzwiach. Dodatkowo dostęp do drzwi takiego pomieszczenia może być chroniony przez punkty wartownicze z pracownikami ochrony. W powyższy sposób chronione są systemy wymagające największego poziomu bezpieczeństwa, np. w organizacjach rządowych lub w wojsku. Zwykle systemy takie nie są podłączone do globalnej sieci komputerowej, lecz korzystają z własnych sieci telekomunikacyjnych. Zaistnienie zagrożenia w takim systemie automatycznie kieruje podejrzenia na wąskie grono osób mających do nich dostęp.

Kolejną warstwą ochrony może być 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), np. powinno się nie dopuszczać haseł, które wywodzą się z nazwy lub opisu użytkownika, są zbyt krótkie, zawierają zbyt ubogi wachlarz znaków, były już stosowane, wynikają z kodu klawiatury itp. Istnieje szereg narzędzi, zarówno dostarczanych z systemami operacyjnymi, jak i dodatkowych, służących do kontroli zawiłości haseł (np. npasswd, passwd+, goodpw, crack). Niektóre z tych narzędzi tworzą słowniki najpopularniejszych wyrażeń (wśród których są nazwy użytkowników systemu) i stosując pewien zbiór reguł próbują wygenerować niebezpieczne hasła, które później nie są dopuszczane do użytkowania.

Kolejny mechanizm kontroli jakości haseł związany jest z faktem, że użytkownicy nie lubią zmiany haseł (jest to niewygodne) i w związku z tym starają się posługiwać małą liczbą haseł (np. dwoma) na zmianę. Aby utrudnić takie działanie, w systemie tworzona jest lista historii haseł. Oczywiście rozwiązanie takie sprawdzi się, jeżeli jest dostatecznie silne ograniczenie na czas używania haseł.

Jako dodatkowe metody uwierzytelniania stosowane są metody wykorzystujące inteligentne karty. Karty takie mogą mieć różnorakie postacie; mogą przypominać karty telefoniczne czy kalkulatory. Aby karta rozpoczęła działanie, konieczne jest podanie przez użytkownika osobistego numeru identyfikacyjnego PIN, (ang. *Personal Identification Number*). Karty te mogą działać na różnorakie sposoby. Jeden z najpopularniejszych to protokół typu wezwanie-odpowiedź. System generuje pewną losową liczbę i podaje ją użytkownikowi. Ten wprowadza ją do karty, która szyfruje liczbę i rezultat szyfrowania zwracany jest do systemu. System sprawdza, czy liczba została zaszyfrowana poprawnie (metoda ta oparta jest na tzw. kryptograficznym protokole uwierzytelniania ze współdzielonym kluczem). Inna metoda wykorzystania karty polega na tym, że liczba, którą należy podać systemowi, generowana jest przez kartę po wprowadzeniu numeru identyfikacyjnego (ta metoda z kolei wykorzystuje

protokół Lamporta). Karta musi być uprzednio zainicjowana w systemie, z którym będzie współdziałać.

Bardziej wyrafinowaną metodą uwierzytelniania jest ta, w której system po zaakceptowaniu hasła żąda podania od użytkownika informacji typu „Wolisz brunetki, blondynki czy szatynki?'', „Jaki jest twój ulubiony kolor?''. Poprawne odpowiedzi użytkownik wcześniej zadeklarował systemowi. Metoda ta oparta jest na założeniu, że jeśli nawet intruz złamie hasło użytkownika, to nie będzie znał jego preferencji dotyczących kobiet czy kolorów.

2.6.3.Mechanizmy zapobiegawcze i środki techniczne

Mechanizmy zapobiegawcze wykorzystujące środki techniczne polegają na stosowaniu zdobyczy technologicznych do zapobiegania pogwałceniom polityki bezpieczeństwa organizacji. Środki techniczne są znane również pod nazwą środków logicznych i mogą być wbudowane w system operacyjny, występować w postaci aplikacji lub dodatkowego sprzętu bądź oprogramowania.

Przykłady zapobiegawczych środków technicznych obejmują:
• protokoły;
• techniki biometryczne;
• kryptografię;
• karty procesorowe;
• menu;
• ograniczenia interfejsów użytkownika;
• hasła;
• ograniczenia klawiatur.
Ograniczenia interfejsów użytkownika polegają na przykład na dezaktywowaniu („wyszarzeniu") niedostępnych dla użytkownika opcji w menu aplikacji. Ograniczenia klawiatur są związane z zablokowaniem funkcji dostępnych przez naciśnięcie odpowiednich klawiszy na klawiaturach.

2.6.4.Wydzielanie i monitorowanie punktów wymiany informacji systemu z otoczeniem

Przykładem realizacji tej strategii jest architektura firewall, w której wszelka wymiana informacji pomiędzy systemem informatycznym organizacji a siecią globalną odbywa się przez wydzielony fragment systemu (np. komputer łączący sieć organizacji z siecią globalną czy podsieć spełniająca taką funkcję) pod kontrolą odpowiedniego oprogramowania. Oprogramowanie to ma za zadanie monitorować przesyłane informacje i sygnalizować wszelkie nieprawidłowości bądź fakty mogące zagrozić bezpieczeństwu systemu organizacji.

2.6.5.Reakcje na próby ataku na system

Automatyczne blokowanie się systemu w przypadku wykrycia włamania
W strategii tej w przypadku wykrycia zagrożenia system sam blokuje w mniejszym lub większym stopniu swoje działanie uniemożliwiając intruzowi wyrządzanie szkód. Oczywiście ogranicza to (bądź blokuje) możliwości pracy legalnych użytkowników. Jednocześnie system zapewnia zapis swojego stanu w momencie wykrycia zagrożenia, co później ułatwia likwidację ewentualnych szkód lub lokalizację wyłomu w systemie bezpieczeństwa.

Analiza sytuacji, zatrzymanie pracy.
Bardzo 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 systemie, wielokrotnych prób zalogowania się na pewne konto 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.

Zapis stanu systemu
Bardzo istotne jest zapisanie stanu zaatakowanego systemu w celu późniejszej dokładnej analizy.

Odtworzenie ostatnio zachowanego stanu systemu z archiwów
W celu wyeliminowania efektów działań intruza należy odtworzyć poprzedni stan systemu. Należy przy tym pamiętać, iż:

1. Poprzedni stan systemu może również zawierać modyfikacje wprowadzone przez napastnika, o ile zagrożenie nastąpiło po jego zapisie.
2. Zostaną utracone modyfikacje systemu, jakie wykonano przed sporządzeniem ostatniej kopii zapasowej.

Świadome kreowanie i eksponowanie „słabych punktów"
Na zakończenie warto wspomnieć o zastosowaniu pewnego triku polegającego na świadomym wyborze i eksponowaniu fragmentów systemu, które w opinii włamywacza mają uchodzić za „słabe punkty". Odwraca to wówczas uwagę intruza od pozostałych części systemu. Należy oczywiście zadbać o to, aby poziom ochrony w tych „słabych punktach" był dostatecznie wysoki dla uniemożliwienia przeprowadzenia udanego ataku.

2.7. Praktyczna realizacja polityki bezpieczeństwa.

- kontrola dostępu
- ochrona systemu operacyjnego i aplikacji
- narzędzia ochrony systemu plików
- separacja systemu lub jego fragmentu

2.7.1. Kontrola dostępu

Ważne terminy
•**Identyfikacja** (ang. *identification)* — operacja zgłaszania się użytkownika w systemie, polegająca najczęściej na podaniu nazwy użytkownika (ang. *login).*
•**Uwierzytelnianie** (ang. *authentification)* — weryfikacja wiarygodności identyfikacji, na przykład na podstawie podanego hasła.
•**Odpowiedzialność** (ang. *accountability)* — możliwość identyfikacji użytkownika odpowiedzialnego za określone działania w systemie.
•**Autoryzacja** (ang. *authorization)* — nadawanie uprawnień użytkownikowi (lub procesowi) do korzystania z określonych zasobów systemu.

Kontrola dostępu do sieci i związanych z nią zasobów jest kluczowym zagadnieniem bezpieczeństwa sieciowego. W przypadku obecnie spotykanych rozproszonych środowisk informatycznych, gdy na dyskach twardych poszczególnych komputerów spoczywa krytyczna dla istnienia organizacji własność intelektualna, kontrola dostępu staje się jeszcze ważniejszym problemem.

Kontrola dostępu ma na celu zmniejszenie zagrożenia wynikającego ze słabych punktów zabezpieczeń, co jest związane z zagrożeniami sieci wskutek możliwości uzyskania dostępu do systemów przez różnych użytkowników. **Zagrożenie** definiuje się jako zdarzenie lub działanie, które potencjalnie może powodować szkody w systemie sieciowym. W tym przypadku zagrożenie jest związane z możliwością pokonania lub oszukania mechanizmów kontroli dostępu, co pozwala napastnikowi na uzyskanie nieautoryzowanego dostępu do sieci. Prawdopodobieństwo, że zagrożenie spowoduje rzeczywiste straty, jest określane mianem ryzyka. Ponadto przy omawianiu zagadnień kontroli dostępu są wykorzystywane pojęcia obiektu i podmiotu. **Podmiotem** jest aktywna jednostka (na przykład osoba lub proces), natomiast **obiektem** nazywa się jednostkę pasywną (taką jak plik).
Mechanizmy kontroli dostępu są stosowane do zapobiegania atakom lub detekcji przeprowadzonych ataków bądź ich prób oraz w celu przywrócenia sieci do stanu sprzed ataku w przypadku, gdy atak był skuteczny
Należy pamiętać, że ponad 80% ataków na systemy pochodzi z wnętrza sieci. Z tego względu nie należy ufać własnym pracownikom, dlatego też użytkownicy w sieci nie powinni mieć większych możliwości niż bezwzględnie jest im to potrzebne.

Ograniczenia nakładane na użytkowników powinny tworzyć czytelne reguły dostępu do różnych zasobów i umożliwiać szybką lokalizację nielojalnego lub nieostrożnego pracownika. Użytkownik powinien również ponosić odpowiedzialność za zachowanie w tajemnicy haseł, dokumentacji, informacji o systemach używanych w firmie, o topologii sieci komputerowej, metodach jej zabezpieczeń i szczegółach polityki bezpieczeństwa.
Każdy użytkownik powinien zostać przeszkolony w dotyczących go zagadnieniach bezpieczeństwa.

Fizyczne zabezpieczenia komputerów
Z powodu znacznego upowszechnienia technik rozproszonego przetwarzania informacji, w szczególności komputerów przenośnych, fizyczne zabezpieczenie komputerów stało się bardzo ważne.
Mechanizmy kontrolne przeznaczone do tego celu obejmują:
Linki zabezpieczające — są to stalowe linki pokryte tworzywem sztucznym, które służą do mocowania komputera przenośnego lub urządzenia peryferyjnego do biurka.
Blokady portów — są to urządzenia zabezpieczające porty danych (jak napęd dyskietek, port szeregowy lub równoległy itp.) i zapobiegające ich nieautoryzowanemu wykorzystaniu.
Zabezpieczenia wyłączników — blokują dostęp do wyłącznika zasilania komputera, dzięki czemu nieautoryzowany użytkownik nie ma możliwości uzyskania dostępu do systemu przez wyłączenie i włączenie zasilania.
Zabezpieczenia urządzeń peryferyjnych — występują w postaci zabezpieczonych wyłączników, za pomocą których można na przykład zablokować użycie klawiatury.

Techniczne mechanizmy kontrolne
Techniczne mechanizmy kontrolne uzupełniają fizyczne zabezpieczenia oraz środki administracyjne stosowane z reguły w instalacjach o podwyższonym poziomie bezpieczeństwa. Przykładami takich mechanizmów są karty procesorowe oraz urządzenia biometryczne.
Karty dostępu
Kartę (ang. *smart card),* używaną do kontroli dostępu, określa się często po prostu jako **kartę dostępu.** Karty tego typu występują w następujących odmianach:
♦ **Karty ze zdjęciem** — są po prostu kartami identyfikacyjnymi z nadrukowanym zdjęciem jej użytkownika.

♦ **Karty kodowane cyfrowo** — zawierają procesor lub pasek magnetyczny(mogą również zawierać zdjęcie użytkownika). Czytnik kart tego typu może być zaprogramowany w taki sposób, aby kontrolował dostęp do komputera z jednoczesnym zapisem informacji o czasie uzyskania dostępu i wylogowania się z systemu przez użytkownika. Karty tego typu mogą również służyć do wielopoziomowej kontroli dostępu.
♦ **Bezprzewodowe zbliżeniowe czytniki kart** — czytniki tego typu nie wymagają fizycznego włożenia karty do czytnika. Takie karty są również określane jako bezprzewodowe karty dostępu. Czytnik karty wykrywa jej obecność w określonej odległości i na tej podstawie przyznaje dostęp do systemu.

Uznaniowa kontrola dostępu
Jednostka uwierzytelniająca lub podmiot uwierzytelniania w pewnym zakresie ma możliwość określania obiektów kontroli dostępu. Jednym ze sposobów opisywania indywidualnej kontroli dostępu jest *tablica.* Tablica uwzględnia podmioty, obiekty i uprawnienia dostępu, przydzielane podmiotom do poszczególnych obiektów. Tabelę taką czasem określa się mianem **listy kontroli dostępu**

Obligatoryjna kontrola dostępu
Obowiązkowa kontrola dostępu wymaga formalnego dopasowania uprawnień podmiotów z poziomem znaczenia obiektów, które stanowią cel kontroli dostępu. Jednym z takich rozwiązań jest wykorzystanie **etykiety.** Uwierzytelnienie obiektu może odbywać się z wykorzystaniem formy **przepustki,** porównywanej z **wzorcem** zabezpieczenia obiektu. Dana osoba może otrzymać przepustkę o uprawnieniach poufnych, tajnych i ściśle tajnych i na podstawie tej przepustki uzyskać dostęp do dokumentów na określonym lub niższym poziomie poufności. W ten sposób osoba z przepustką na poziomie „tajne" może mieć dostęp do dokumentów zaklasyfikowanych jako poufne, lecz z ograniczeniem określanym jako **potrzeba zapoznania.** Ograniczenie to oznacza, że podmiot może uzyskać dostęp do dokumentu, jeśli jest to niezbędne w celu realizacji jego obowiązków.

Typy implementacji mechanizmów kontroli dostępu
Wyróżnia się trzy typy mechanizmów kontrolnych: **zapobiegawcze, wykrywające** oraz **korekcyjne.** Do implementacji tych mechanizmów są stosowane środki administracyjne, techniczne (logiczne) oraz fizyczne. **Środki administracyjne** obejmują działania formalne, takie jak definicja polityki, procedur, szkolenia kształtujące świadomość bezpieczeństwa oraz kontrola historii pracowników. **Środki techniczne (logiczne)** uwzględniają wykorzystanie mechanizmów kryptograficznych, kart procesorowych i protokołów transmisyjnych. **Środki fizyczne** są najpowszechniej znane, obejmują zatrudnienie strażników czy zabezpieczenie budynków. Połączenie tych środków bezpieczeństwa w zastosowanej implementacji pozwala na realizację różnych kombinacji mechanizmów kontrolnych.

Identyfikacja i uwierzytelnianie
Identyfikacja jest procedurą zgłoszenia systemowi tożsamości użytkownika, z reguły w postaci identyfikatora logowania. Proces ten uruchamia również procedurę zapisu w pliku dziennika informacji o działaniach użytkownika w systemie. **Uwierzytelnianie** polega na weryfikacji tożsamości użytkownika i z reguły jest implementowane w postaci konieczności podania hasła podczas logowania w systemie. Uwierzytelnianie może być również realizowane przez inne mechanizmy, od różnych form haseł po analizę charakterystyki biometrycznej.
Ogólnie ujmując, uwierzytelnianie jest realizowane przez sprawdzenie jednej lub kilku z poniższych cech:

• informacji, która powinna być znana wyłącznie autoryzowanemu użytkownikowi, jak osobisty numer PIN (ang. *personal identification number).* Ten element jest znany jako uwierzytelnianie typu 1. (ang. *Type 1 authentication);*
• urządzenia, które powinno być w posiadaniu wyłącznie autoryzowanego użytkownika, jak karta magnetyczna (z mikroprocesorem i z pamięcią). Ten element jest znany jako uwierzytelnianie typu 2. (ang. *Type 2 authentication);*
• unikalnych cech biometrycznych autoryzowanego użytkownika, jak odcisk palca lub wzór siatkówki. Ten element jest znany jako uwierzytelnianie typu 3.(ang. *Type 3 authentication).*

Hasła

Hasła są najpopularniejszym sposobem uwierzytelniania użytkowników. Z tego powodu skuteczne zabezpieczanie haseł przed niepowołanym dostępem jest kluczowym aspektem polityki bezpieczeństwa.
Najwyższy poziom bezpieczeństwa zapewniają **hasła jednorazowe.** W takim modelu przy każdym logowaniu jest wymagane inne hasło, dzięki czemu napastnik nie może wykorzystać zdobytego w nielegalny sposób hasła, które było wykorzystane przy poprzednim logowaniu. Często zmieniane hasło nazywa się **hasłem dynamicznym.** Hasło, które pozostaje identyczne przy każdym logowaniu nazywa się **hasłem statycznym.** W organizacji może istnieć wymóg okresowych zmian haseł, na przykład raz na miesiąc, raz na kwartał lub w innych odstępach czasu, w zależności od stopnia poufności danych zabezpieczanych tymi hasłami.

W niektórych przypadkach zamiast hasła może być stosowana **fraza** (ang. *passphrase).* Fraza jest ciągiem znaków, z reguły dłuższym od dopuszczalnej długości hasła. Fraza jest konwertowana przez system na formę wirtualnego hasła.
Hasła mogą być generowane w sposób automatyczny z użyciem kart pamięci o rozmiarach karty kredytowej, kart magnetycznych lub urządzeń przypominających niewielki kalkulator (tzw. **token).** Generatory haseł stanowią implementację uwierzytelniania typu 2.

Biometryka

Biometryka jest zdefiniowana jako zautomatyzowane techniki identyfikacji lub uwierzytelniania osób z wykorzystaniem ich charakterystyki fizjologicznej lub behawioralnej. Biometryka należy do mechanizmów uwierzytelniających typu trzeciego. Biometryka znajduje zastosowanie zarówno do identyfikacji, jak i do uwierzytelniania.
W celu identyfikacji biometryka jest stosowana w wyszukiwaniach typu „ **jeden do wielu",** gdzie cechy biometryczne są odnajdywane w większej bazie danych zapisanych cech biometrycznych. Przykładem takiego wyszukiwania może być próba dopasowania odcisków palców sprawcy za pomocą bazy danych, zawierającej odciski palców wszystkich obywateli. Uwierzytelnianie obejmuje wyszukiwanie typu **„jeden do jednego",** ponieważ polega na sprawdzeniu, czy użytkownik poddany sprawdzeniu jest tym, za kogo się podaje. Przykładem takiego wyszukiwania może być porównanie odcisków palców danej osoby z jej odciskami palców, zapisanymi w bazie danych pracowników firmy. Biometryka w zastosowaniach kontroli dostępu jest wykorzystywana do identyfikacji w mechanizmach kontroli fizycznej i do uwierzytelniania w mechanizmach kontroli logicznej.

Urządzenia biometryczne

Urządzenia kontroli dostępu oparte na technikach biometrycznych należą do urządzeń fizycznej kontroli dostępu. Techniki biometryczne mogą być użyte do identyfikacji lub uwierzytelniania.

Typowe cechy biometryczne wykorzystywane do unikalnej identyfikacji lub uwierzytelnienia użytkownika obejmują:

- linie papilarne;
- skanowanie siatkówki;

- skanowanie tęczówki;
- skanowanie twarzy;
- skanowanie dłoni;
- geometria dłoni;
- głos;
- dynamika ręcznego podpisu.

Kerberos

Czasami do przeprowadzania uwierzytelniania użytkownika, rozpoczynającego pracę w systemie lub zgłaszającego chęć skorzystania z jakiejś usługi, stosowane są „duże" systemy uwierzytelniające, działające zwykle w oparciu o tzw. *bilety* (np. system *Kerberos).* System taki przyznaje użytkownikowi *bilet,* który upoważnia np. do załogowania się do systemu. Bilety posiadają szereg zabezpieczeń, m.in. znaczniki czasowe zapobiegające ponownemu użyciu biletu (np. skradzionego przez napastnika).
Kerberos nosi swoją nazwę na pamiątkę trójgłowego psa z mitologii greckiej, strzegącego wejścia do świata podziemnego.
Kerberos stosuje technikę kryptografii z użyciem kluczy symetrycznych, opracowaną przez Project Athena w Massachusetts Institute of Technology. Jest to zaufany protokół uwierzytelniający, który działa w sieci i zapewnia bezpieczny sposób kontroli dostępu do jej zasobów.
Mechanizmy Kerberos opierają się na założeniu, że komputery przyłączone do sieci stanowią publicznie dostępne, niegodne zaufania lokalizacje. Z tego wynika, że komunikaty mechanizmu Kerberos przesyłane w sieci mogą być przechwytywane przez intruzów. Twórcy Kerberos uważali jednak, że niektóre lokalizacje można zabezpieczyć na tyle, aby działały jako zaufane mechanizmy uwierzytelniające, dostępne dla wszystkich klientów i usług w sieci. Te scentralizowane serwery nazywa się centrami dystrybucji kluczy (ang. *Key Distribution Center,* KDC), usługami przyznawania biletów (ang. *Ticket Granting Service,* TGS) oraz usługami uwierzytelniania (ang. *Authentication Service,* AS).

Podstawowe zasady mechanizmu uwierzytelniania systemu Kerberos

1. KDC posiada informacje o tajnych kluczach wszystkich klientów i serwerów w sieci.
2. KDC wymienia z klientem informacje inicjalizujące z wykorzystaniem właśnie tych tajnych kluczy.
3. Kerberos uwierzytelnia klienta żądającego usługi serwera. W tym celu wykorzystuje się serwer TGS, który generuje tymczasowe symetryczne klucze sesji na potrzeby komunikacji pomiędzy klientem a KDC, serwerem a KDC oraz pomiędzy klientem a serwerem.
4. Teraz rozpoczyna się komunikacja pomiędzy klientem a serwerem, w trakcie której wykorzystuje się wcześniej wspomniane, tymczasowe symetryczne klucze sesji.

Wymiana danych w systemie Kerberos rozpoczyna się od wpisania przez użytkownika hasła na jednej ze stacji skonfigurowanej w tym systemie. W stacji hasło użytkownika jest przekształcane na klucz tajny użytkownika. Ten klucz tajny jest zapisywany tymczasowo w stacji. Następnie klient przesyła identyfikator użytkownika w postaci nieszyfrowanej do usługi przyznającej bilety (TGS). W odpowiedzi na to żądanie TGS wysyła klientowi klucz sesji TGS-klient — Ktgs,c — zaszyfrowany kluczem tajnym klienta. Ponadto TGS wysyła bilet dający prawo do otrzymywania innych biletów (ang. *ticket granting ticket,* TGT) zaszyfrowany kluczem znanym tylko TGS. Po otrzymaniu tych komunikatów klient odszyfrowuje Ktgs,c używając klucza tajnego użytkownika.

Oprogramowanie do kontroli dostępu do systemu

- Standardowe oprogramowanie systemów operacyjnych do kontroli haseł
- Oprogramowanie dodatkowe
- Inne techniki związane z uwierzytelnianiem

Standardowe oprogramowanie systemów operacyjnych do kontroli haseł

W wielu systemach operacyjnych (praktycznie we wszystkich „większych") istnieje standardowe oprogramowanie służące do uwierzytelniania użytkowników. Najczęściej spotykane metody wykorzystują hasła. W wielu systemach zaimplementowano oprogramowanie do sprawdzania „zawiłości" proponowanego przez użytkownika hasła. Oprogramowanie to sprawdza propozycję hasła użytkownika zgodnie z pewnym zbiorem reguł (który często może być przez administratora poszerzany) oraz poprzez sprawdzenie czy hasło nie jest którymś z wyrazów z przechowywanego w systemie słownika trywialnych haseł. Sprawdzenie według reguł polega na przykład na skontrolowaniu, czy hasło nie jest odwróceniem nazwy użytkownika, jej łatwą modyfikacją, poszerzeniem itp.

Oprogramowanie dodatkowe

Oprócz standardowych programów systemów operacyjnych stosowane jest również oprogramowanie dodatkowe. W funkcji takiej występuje często oprogramowanie służące oryginalnie do łamania haseł (np. powszechnie znany program *Crack* często wykorzystywany jest przez administratorów do sprawdzania haseł).

Innym rodzajem oprogramowania jest to służące do wykonywania alternatywnej lub dodatkowej kontroli autentyczności użytkownika. Programy takie uruchamiane są zamiast standardowych procedur uwierzytelniania systemu lub po ich wykonaniu.

Czasami do przeprowadzania uwierzytelniania użytkownika, rozpoczynającego pracę w systemie lub zgłaszającego chęć skorzystania z jakiejś usługi są systemy uwierzytelniające, (np. wspomniany system *Kerberos).*

Inne techniki związane z uwierzytelnianiem

Oprócz haseł w systemach stosowane są inne sposoby zabezpieczania przed nielegalnym dostępem. Należą do nich na przykład:

• blokowanie konta, do którego wykonano wiele kolejnych nieudanych prób dostępu,

• automatyczne kończenie sesji roboczej użytkownika w przypadku długiego okresu braku sygnałów z terminala świadczących o pracy,

• prowadzenie historii haseł i uniemożliwianie ponownego używania wykorzystywanych w przeszłości haseł.

2.7.2.Narzędzia ochrony systemu plików

Kolejna grupa narzędzi realizacji polityki bezpieczeństwa związana jest z kontrolą dostępu nie do samego systemu, a do jego zasobów. Jednym z podstawowych zasobów jest system plików i, ponieważ w wielu systemach (np. unixowych, Windows z NFS) stosowany jest jako element reprezentujący pozostałe zasoby, dostęp do zasobów plikowych właśnie będzie tu omówiony.

Mechanizm grup i praw dostępu do plików

Jest to bardzo często stosowana metoda kontroli dostępu. Użytkownicy podzieleni są na grupy, np. zgodnie ze strukturą organizacji, czy z uczestnictwem w określonych projektach, czy też z koniecznością dostępu do określonych zasobów. Każdy plik (czy zasób, np drukarka, czytnik CD-ROM) ma określone prawa wykonywania odpowiednich operacji (czytania, pisania, wykonywania, usuwania itp.) dla użytkownika będącego jego właścicielem, dla określonej grupy użytkowników i dla wszystkich pozostałych użytkowników systemu. Mechanizm ten jest powszechnie znany i dlatego nie będzie

opisywany dokładniej. Konieczne jest rozważne tworzenie grup i podziału pracowników instytucji na grupy, gdyż znane są przykłady stwarzania poważnych zagrożeń związanych z nie przemyślanym przypisywaniem użytkowników do grup.
W niektórych systemach stosowany jest bardziej złożony mechanizm kontroli dostępu do zasobów. Są to tzw. *listy kontroli dostępu.* Lista taka przypisana jest do pliku (zasobu) i pozwala w sposób bardziej szczegółowy opisać prawa określonych użytkowników czy grup. Listy kontroli dostępu funkcjonują jako uzupełnienia omówionych powyżej praw dostępu.

Oprogramowanie do szyfrowania

Do metod realizacji polityki bezpieczeństwa należy również szyfrowanie danych. Szyfrowaniu podlegać mogą:

- dane przechowywane w pamięci zewnętrznej (oprogramowanie do szyfrowania plików, dysków, np. *SafeGuard* na PC, *crypt* w Unixie),
- zdalne (a jeśli jest taka potrzeba - i lokalne) sesje robocze użytkowników (np. pakiet *Secure Shell),*
- informacje przesyłane przy rozpoczynaniu zdalnej sesji użytkownika - w szczególności hasła przesyłane przez sieć lub łącza telefoniczne (np. szyfrowanie sprzętowe),
- informacje przesyłane pocztą elektroniczną.

2.7.3.Oprogramowanie separujące system lub jego fragmenty

Często efektywnym sposobem zabezpieczenia systemu przed atakami z zewnętrznego otoczenia sieciowego jest odseparowanie go od tegoż otoczenia przez zastosowanie tzw. architektury „ściany ogniowej" (ang. *firewall).* Jest to bardzo popularna metoda ochrony systemów informatycznych przed atakami „z zewnątrz".
W architekturze takiej system informatyczny organizacji - mający połączenie z globalną siecią komputerową — podłączony jest do tej sieci za pośrednictwem specjalnej struktury sprzętowo-programowej (może to być jeden komputer lub pewna podsieć z odpowiednim oprogramowaniem).
„Ściana ogniowa" wykonuje dwojakiego rodzaju działania:

- Zajmuje się filtrowaniem (kontrolowaniem) komunikacji sieciowej między systemem organizacji a zewnętrzną siecią komputerową.
- Służy jako tzw. *serwer pośredniczący* (ang. *Proxy server).*

Filtrowanie (kontrolowanie) komunikacji

Filtrowanie (kontrolowanie) komunikacji sieciowej między systemem organizacji a zewnętrzną siecią komputerową odbywa się na poziomie sprawdzania przesyłanych pakietów sieciowych. Często zdarza się, że komputer, za pośrednictwem którego sieć organizacji podłączona jest do sieci zewnętrznej - tzw. *gateway* - pełni również rolę „ściany ogniowej". Wówczas do jego zadań należy nie tylko przesyłanie pakietów między siecią wewnętrzną a siecią zewnętrzną, ale również sprawdzanie, czy dany pakiet *można* przesłać. Sposób działania „ściany ogniowej" wynika ż przyjętej w organizacji polityki bezpieczeństwa i jest określany przez odpowiednie skonfigurowanie oprogramowania.

Prosty przykład sposobu filtracji pakietów przez „ścianę ogniową":

- blokowane są wszystkie połączenia z komputerami sieci zewnętrznej, uznanymi za niegodne zaufania,
- blokowane są wszystkie przychodzące połączenia oprócz połączeń pocztowych (aby możliwe było odbieranie poczty),
- udostępniane jest świadczenie przez system organizacji wszystkich standardowych usług (poczta, *ftp, www)* oprócz uznanych za niebezpieczne (np. *telnet).*

Serwer pośredniczący

Firewall jako tzw. *serwer pośredniczący* (ang. *proxy server).* Wówczas komputery wewnętrznej sieci organizacji zwracają się z żądaniami wykonania określonych usług nie

bezpośrednio do interesujących ich komputerów sieci zewnętrznej, lecz do serwera pośredniczącego, działającego na „ścianie ogniowej", który przesyła je dalej. Również odpowiedzi od właściwych serwerów przekazywane są za pośrednictwem serwerów pośredniczących. Takie działanie nazywane bywa niekiedy *ochroną na poziomie aplikacji.*

Podsumowanie

Proces inżynierii bezpieczeństwa systemów informatycznych udostępnia solidną podstawę do określania, projektowania, implementacji i oceny systemów wysokiej jakości, cechujących się znacznym poziomem bezpieczeństwa informacji. Wielowarstwowa strategia ochrony dogłębnej wykorzystuje procesy inżynierii systemów, inżynierii bezpieczeństwa systemów informatycznych oraz zarządzania ryzykiem, dzięki którym jest możliwa efektywna implementacja strategii zabezpieczenia granicy enklawy.

Należy pamiętać o zagrożeniach które możemy podzielić

- Ze względu na miejsce lokalizacji źródła niebezpieczeństwa:
  - Wewnętrzne (statystycznie ponad 70 %)
  - Zewnętrzne
- Pod względem specyfikacji zagrożeń:
  - Włamanie do systemu
  - Utratę poufności informacji, określonych odpowiednią klauzulą tajności
  - Utratę integralności informacji
  - Utratę autentyczności informacji
  - Utratę dostępności usług systemu i informacji
  - Podszywanie się pod innego użytkownika

Ważnym aspektem polityki bezpieczeństwa jest odpowiedni personel, wyszkolony w świadomości jej wymogów. Gdy polityka i związane z nią procedury są już opracowane, należy posłużyć się narzędziami zarządczymi, które pozwolą na zapewnienie odpowiedniego poziomu wprowadzanych rozwiązań. Ważnym elementem polityki jest plan przywracania systemu po awariach który ma na celu zapewnienie funkcjonowania organizacji w przypadku wystąpienia awarii.

Innym elementem zarządzania bezpieczeństwem jest implementacja właściwych środków bezpieczeństwa.

Najlepsza polityka bezpieczeństwa, istniejąca tylko na papierze bądź nie realizowana dostatecznie starannie, nie zapewni dobrej ochrony.

3. Bezpieczeństwo sieci komputerowej

Podstawowe zagadnienia ochrony sieci komputerowych

Utrzymanie wysokiego poziomu bezpieczeństwa sieci komputerowej staje się bardzo skomplikowanym zadaniem z uwagi na złożoność technologiczną i dynamiczny rozwój tego środowiska.

Dla wielu osób największym ogniskiem zagrożenia jest Internet. W praktyce dużo większe zagrożenie stwarzają użytkownicy lokalni, posiadający legalny dostęp do określonych zasobów systemu, którzy z pewnych względów dokonują przejęcia lub modyfikacji strategicznych informacji.

Budując system ochrony sieci komputerowej należy uwzględnić wszystkie możliwe zagrożenia, a w szczególności te, które bezpośrednio wynikają z nielegalnej działalności lokalnych użytkowników.

Każdy atak na stację roboczą związany z siecią prędzej czy później kończy się uruchomieniem
jakiegoś kodu. Kod ten można zaklasyfikować do jednej z następujących kategorii:
kod złośliwy — obejmuje wirusy, robaki i konie trojańskie. Kod tego typu może być uruchomiony w imieniu legalnego użytkownika przez aplikację obsługującą skrypty, na przykład przez przeglądarkę WWW;
usługi sieciowe — w tym przypadku napastnik włamuje się do systemu przez sieć i uzyskuje dostęp do stacji roboczej poprzez otwarty port.

Bezpieczeństwo w sieci komputerowej
Do grupy elektronicznych środków ochrony należą np. FIREWALL, mikroprocesorowe karty uwierzytelniające tożsamość użytkowników, programy antywirusowe. Elektroniczne zabezpieczenia powinny zawierać wiele różnych, ubezpieczających i uzupełniających się wzajemnie elementów.
Ogólnie system ochrony sieci komputerowej można przedstawić w formie warstwowej struktury:
–Warstwa ochrony danych przesyłanych w sieci publicznej (VPN).
–Warstwa ochrony sieci komputerowej z zewnątrz (FIREWALL).
–Warstwa ochrony danych przesyłanych w sieci prywatnej (szyfrowanie).
–Warstwa ochrony sieci komputerowej od wewnątrz.
–Warstwa ochrony systemu operacyjnego.
–Warstwa ochrony aplikacji użytkowych.

Jak dotąd nie ma i prawdopodobnie jeszcze długo nie będzie jednego, uniwersalnego produktu, który sprostałby zadaniu pełnej ochrony sieci komputerowej. Stąd koniecznym jest łączenie oprogramowania wielu różnych producentów.

Najpierw należy wyjaśnić nagminnie źle używane pojęcie, jakim jest hacker. **Hacker** jest to pasjonat i entuzjasta, który zajmuje się badaniem działania różnorodnego oprogramowania i poprawianiem błędów przez siebie znalezionych. Jeśli naszą siecią zainteresuje się hacker, to najprawdopodobniej dostaniemy od niego informację o błędach, jakie popełniono, i dziurach w zabezpieczeniach. Hacker na pewno nie zniszczy ani nie uszkodzi żadnego z systemów. Osobą, która zajmuje się działalnością destrukcyjną, jest właśnie **cracker**.

Bezpieczeństwo sieciowe jest ważnym elementem bezpieczeństwa informatycznego w organizacji. Stacja robocza i cała sieć w strategii ochrony stanowią kluczową pozycję. Aby skutecznie odpierać różnego typu ataki należy zapoznać się z metodami stosowanymi przez włamywaczy. Takie podejście daje administratorowi możliwość odkrycie próby włamania i podjęcie odpowiednich środków zaradczych.

3.1. Włamanie do sieci
Rozpoznanie terenu:
-zbieranie danych,
-skanowanie,
-identyfikacja systemu operacyjnego.
Metody włamań:
-uzyskanie dostępu,
-destabilizacja pracy.

3.1.1. Rozpoznanie terenu.
3.1.1.1.Zbieranie danych
•Szukamy jelenia
Jednym ze sposobów poszukiwania informacji o firmie jest wykorzystanie ogromu informacji zindeksowanych w bazach wyszukiwarek internetowych, list referencyjnych firmy czy w serwerach grup dyskusyjnych. Jest to banalne, ale nowoczesna firma, działając w epoce Internetu, pozostawia wiele śladów — jak ranny jeleń w lesie**.** Przykładowo dane na temat imion i nazwisk chociaż niektórych pracowników nie są na pierwszy rzut oka niebezpieczne, ale jak się później przekonamy, mogą stanowić dodatkową pomoc na pewnych etapach włamania.

•Inżynieria społeczna, inżynieria socjalna, socjotechnika, (ang. ***social engineering*****)**
Drugim etapem może być próba tzw. inżynierii społecznej. Cracker może zadzwonić do sekretariatu na numer, podany na stronie WWW, i przedstawiając się jako administrator poprosić o hasło, ponieważ musi je zweryfikować — cokolwiek by to znaczyło. Przykładową metodą jest telefon do firmy z prośbą o króciutkie wypełnienie ankiety dla jakiejś znanej firmy informatycznej. Może się okazać, że skuszony obiecanym losowaniem nagród, pracownik dobrowolnie udzieli wyczerpujących informacji o swoim systemie operacyjnym, firewallu, routerach itp. Intruz może również wejść do jednego z pokoi, podając się za pracownika serwisu komputerowego, poprosić o dostęp do komputera, ponieważ wykryto w nim uszkodzenie karty sieciowej. Ostatnio modnym „prezentem" stają się niszczarki dokumentów. Czasami w papierach wyrzucanych do kosza można znaleźć bardzo wartościowe informacje.

•Whois
Kolejnym krokiem, jaki podejmie cracker, będzie najprawdopodobniej skorzystanie z baz danych za pomocą polecenia whois lub interfejsu WWW - przykładowo *http://www.ripe.net/db/whois-free.html.* Może on w nich znaleźć przynajmniej zakres adresów IP przydzielonych firmie, dane administratora sieci rejestrującego adresy oraz dane dostawcy Internetu.

•DNS
Kolejnym etapem będzie sprawdzenie adresów IP serwerów DNS firmy i próba dokonania transferu strefy za pomocą polecenia *nslookup* lub *dig.* Dzięki temu craker otrzyma listę wartych zainteresowania hostów w sieci firmy, oczywiście tylko wtedy, gdy administrator zezwolił na dokonywanie transferów strefy.

•Mapa sieci
Na tym etapie włamywacz posiada już podstawowe informacje o hostach, sprawdza jeszcze poleceniem *ping,* które z nich aktualnie działają. Każdy system obsługujący stos protokołów TCP/IP powinien używać protokołu ICMP, a przynajmniej odpowiadać na *Echo Request* komunikatem *Echo Reply.* Posiłkując się zarejestrowanym dla twojej firmy w bazach *whois* zakresem adresów IP, może sprawdzić, które z nich są wykorzystywane przez działające serwery. Podstawowym zabezpieczeniem przed tymi metodami jest blokowanie komunikatów ICMP na firewallu. Jednak nie wszystkie komunikaty można blokować.

Teraz cracker może spróbować wykonać mapę sieci firmy za pomocą polecenia *traceroute.* Sprawdzi w ten sposób rozkład routerów i wstępnie zdefiniuje schemat połączeń w sieci. Jeśli filtrowane są na firewallu pakiety UDP skierowane na porty 33434 i wyższe charakterystyczne dla tego programu, może użyć kilku innych metod. Najprostszym

rozwiązaniem będzie zmiana numeru portu, od którego traceroute będzie zaczynał odliczanie (numer portu jest zwiększany o 1 z każdym wykrytym routerem). Może skorzystać z jakiegoś narzędzia *(apsend),* które będzie wysyłało pakiety UDP ze zdefiniowanym przez niego portem źródłowym i docelowym. Czasami pakiet wysłany z portu 53 (DNS) może przejść przez firewall i włamywacz otrzymuje wtedy upragnioną informację zwrotną ICMP. Cracker raczej spróbuje skorzystać z jakiegoś narzędzia stworzonego głównie do takich zastosowań, przykładowo *firewalk.* Główną metodą zabezpieczenia przed tworzeniem mapy jest odpowiednia konfiguracja firewalla i nieprzepuszczanie niepożądanych pakietów UDP do sieci.

3.1.1.2. Skanowanie

W sumie można powiedzieć, że włamywacz już rozpoczął skanowanie sieci. Jednak w porównaniu z możliwościami, które zaraz opiszę, tamten etap możesz potraktować jako bardzo niewinny. Tak jakby przespacerował się wokół domu, obejrzał kraty w oknach, ocenił psa i poplotkował trochę sąsiadami. Teraz jednak przedostanie się przez ogród i sprawdzi, jakich zamków używamy.
Wcześniej cracker wyczerpał już możliwości leżące w protokole ICMP. Ale przecież można wykorzystać UDP. Każda stacja, otrzymawszy pakiet UDP skierowany na zamknięty port, powinna odpowiedzieć komunikatem ICMP *Port Unreachable.* Jeśli skan trafi na otwarty port UDP, nie otrzymamy żadnej informacji. Do skanowania może wykorzystać polecenia systemowe lub użyć specjalistycznego oprogramowania.

3.1.1.3. Identyfikacja systemu operacyjnego

Przyjmijmy, że crackerowi sprawdzającemu naszą sieć udało się skanowanie. Ma już informacje, które komputery są aktywne i jakie usługi udostępniają. Bardzo przydatną informacją byłyby jeszcze rodzaje i wersje ich systemów operacyjnych. Proces wykrywania systemu określany jest w literaturze mianem *fingerprinting.*

•Winietki

Najprostszą metodą jest po prostu przejrzenie winietek *(banner)* zwracanych przez usługi działające na danym systemie. Możemy tego dokonać nawet za pomocą telnetu lub netcat.

•Nmap

Podstawowym narzędziem do wykrywania systemu operacyjnego jest nmap. Użyty z opcją -0 wykonuje serię testów, za pomocą których próbuje zidentyfikować system, z którym ma do czynienia.
NMapWin jest wersją pracującą pod kontrolą Windows.

Do skutecznego wykrywania systemu operacyjnego nmap potrzebuje jednego otwartego portu i jednego zamkniętego niefiltrowanego; jeśli podamy mu dwa takie porty do przeskanowania, to zmniejszymy prawdopodobieństwo wykrycia. Ponieważ nmap nie wykona standardowego skanowania, nie spowoduje dużego ruchu, więc kilka pakietów wysłanych z naszego hosta może umknąć systemom bezpieczeństwa. Oczywiście musimy najpierw znać te dwa porty, ale jeśli testowany komputer nazywa się *www,* to z dużym prawdopodobieństwem można wnioskować o otwartym porcie 80.

•Xprobe2

Ofir Arakin i Fyodor Yarochkin (twórca programu nmap) pracują nad narzędziem o nazwie Xprobe2. Xprobe, tak jak inne narzędzia tego typu, korzysta z bazy sygnatur odpowiedzi systemów operacyjnych na wykonywane na nich testy, jednak program ten opiera się na wielu testach sprawdzających zachowanie się systemu operacyjnego wobec protokołu ICMP.

Programy narzędziowe i dokumentacja

•**Nmap** — *http://www.nmap.org* — bardzo dobry darmowy skaner portów oraz program do identyfikacji systemu operacyjnego. Istnieje wersja dla Windows.
•**Netcat** — *http://www.atstake.com/research/tools/index.html #networkutilities* — proste narzędzie przydatne do wielu zastosowań, jego głównym zadaniem jest wysyłanie na określony port ciągu znaków lub nasłuchiwanie na porcie.
•**Hping** — *http://www.hping.org/* — narzędzie do generowania różnorodnych pakietów. Może służyć do testowania firewaili, zaawansowanego skanowania portów, testowania sieci przy użyciu różnorodnych protokołów i ich ustawień (TOS, fragmentacja) itp.
•**Firewalk** — *http://www.binarii.com/files/security/firewalk-LO.tar.gz* — program analizujący odpowiedzi na wysyłane przez siebie pakiety, służy do tworzenia mapy badanej sieci, wykrywania firewaili i określania ich reguł. Ma interfejs graficzny.
•**Xprobe2** — *http://www.sys-security.com/archive/tools/ xprobe2/xprobe2-0. lrcl.tar.gz.*
Opis działania Xprobe2: *http://www.sys-security.com/archive/papers/Xprobe2.pdf.*

3.1.2. Metody włamań

Po etapie zbierania informacji o naszych systemach cracker przystępuje do działania. Najczęściej ma już dokładne dane na temat struktury sieci, używanych systemów operacyjnych, wersji oprogramowania świadczącego usługi w sieci. Poza tym ma wiele dodatkowych informacji o firmie, może również mieć dane o pracownikach. Jest to bardzo wiele informacji, pozwolą mu one dokładnie przygotować narzędzia, którymi posłuży się podczas włamania. Dlatego musimy dbać, aby sieć w firmie dostarczała włamywaczowi jak najmniej informacji. Jedyną przeszkodą między nim a serwerami jest administrator, na jego barkach spoczywa właściwa konfiguracja sieci i jej bezpieczeństwo.

Istnieją dwa cele ataków sieciowych:
- uzyskanie dostępu do systemu,
- zdestabilizowanie pracy systemu komputerowego.

3.1.2.1. Uzyskanie dostępu

Rozpoczyna się ono najczęściej etapem wyszukiwania odpowiedniego narzędzia *(exploita),* które posłuży do włamania. Exploita włamywacz szuka na podstawie informacji, które zdobył za pomocą wcześniej podanych metod. Korzysta oczywiście z własnych zbiorów oraz z wielu serwisów tzw. „hackerskich".
Najprostszym sposobem osiągnięcia pierwszego celu jest zdobycie nazwy użytkownika w systemie *(login)* i używanego przez niego hasła *(password).* Zdobycie *loginu* na ogół nie jest trudne (najczęściej wystarczy zdobyć adres poczty elektronicznej danego użytkownika). Jeśli system operacyjny umożliwia takie działania, cracker zajmie się lokalnym zwiększaniem uprawnień zdobytego konta, tak aby opanować serwer. Działanie takie opiera się oczywiście na wykorzystywaniu błędów w systemie operacyjnym i aplikacjach oraz błędów popełnionych przez administratora podczas konfiguracji.
Statystyki podają, że najczęściej użytkownicy sieci komputerowych stosują hasła łatwe do złamania za pomocą **metody słownikowej** (korzystając ze słownika zawierającego odpowiednią liczbę słów). Dlatego należy dbać, aby hasła użytkowników były jak najbardziej skomplikowane, (p wykład 2). Ponadto warto ustawiać możliwość np. trzykrotnego błędnego logowania się, a następnie system powinien przez pewien czas (kilka minut, godzin) uniemożliwiać logowanie tego użytkownika, równocześnie raportując taką sytuację w dziennikach systemowych. Ze względu na dużą czasochłonność takiego działania, rzadko stosowane jest łamanie haseł poprzez sieć.
Starą metodą jest podstawienie programu, udającego program logujący do systemu. W ten sposób użytkownik podaje swoje hasło, a program włamywacza zdobywa je w postaci

niezaszyfrowanej. Następną metodą jest nasłuchiwanie *(sniffing);* polega ona na podłączeniu do sieci komputera z uruchomionym oprogramowaniem do ściągania wszystkich ramek ethernetowych w danym segmencie sieci. W tym momencie cracker uzyskuje dostęp do wszystkich haseł, które transmitowane są otwartym tekstem w swojej domenie kolizji (np. odczytywanie poczty za pomocą protokołu POP, transmisja plików protokołem FTP).
Pod nazwą *sniffing* zaszeregowane są również metody podsłuchu promieniowania elektromagnetycznego wydzielanego przez transmisje w kablach sieciowych lub w kablach monitorowych. Na przykład istnieją urządzenia umożliwiające oglądanie (oczywiście zaszumionego) obrazu wyświetlanego na monitorze znajdującym się kilkanaście metrów od nas, za kilkoma ścianami.
Znanym problemem są usługi umożliwiające zdalną pracę: telnet, rlogin, rsh, rep, których system zabezpieczeń jest zupełnie niewystarczający. Aktualnie są coraz rzadziej stosowane i najczęściej nie wykorzystywane. Zastąpione zostały usługą bezpiecznego połączenia **ssh** *(**S**ecure **Sh**ell).*
Jedną z kategorii zagrożeń stanowią tzw. **furtki** *(backdoors)* lub **włazy** *(trapdors),* będące nieudokumentowanymi funkcjami aplikacji, pozostawionymi przez programistów. W systemie Linux, dzięki pełnej dostępności źródeł programów, bardzo szybko są wykrywane i usuwane tego typu problemy. Systemy komercyjne nie dają nam tej pewności. Często nazwę backdoor stosuje się do tylnego wejścia pozostawianego przez włamywacza po opanowaniu systemu. Może on dzięki niemu dostać się do systemu nawet po poprawieniu błędu, dzięki któremu dostał się do niego za pierwszym razem.
Ponadto istnieje olbrzymia liczba metod korzystających ze słabości specyficznych dla systemu operacyjnego i oprogramowania użytkowego. Z tego powodu administrator sieci powinien również dobrze znać zagadnienia związane z bezpieczeństwem systemów operacyjnych komputerów i serwerów używanych w jego sieci. Przykładowo dobrze znane są problemy z bezpieczeństwem protokołu NetBIOS.

•Exploity

W jaki sposób działają te programy? Należy pamiętać o tym, że ciągle są wykrywane błędy w oprogramowaniu i powstają exploity je wykorzystujące. Ciągle powstają nowe sposoby ochrony przed działaniem takich programów i metody przełamywania ochrony. Z tego powodu należy stale monitorować strony i listy dyskusyjne zajmujące się tymi zagadnieniami. Miejsce na stronie producenta twojego systemu operacyjnego, dotyczące poprawek i zabezpieczeń, powinno być najczęściej odwiedzanym przez ciebie miejscem w Internecie.
Każda usługa sieciowa w jakiś sposób komunikuje się ze światem i działa w środowisku systemu operacyjnego najczęściej na wysokich uprawnieniach. Wiąże się to z otwieraniem portów poniżej 1024 zarezerwowanych dla superużytkownika (administrator, root). Jeśli włamywaczowi uda się zmusić taką usługę, aby coś dla niego wykonała, operacje te zostaną wykonane z uprawnieniami, z których korzystała ta aplikacja.
Aby zmienić działanie programu, cracker musi zmienić zawarty w pamięci serwera kod wykonującego się zadania. Najpopularniejszą metodą jest tzw. **przepełnienie buforu** *(buffer overflow).* Drugą metodą jest używanie niebezpiecznych **łańcuchów formatujących** (*format string).*

•Spoofing

Jedną z niebezpieczniejszych technik włamań jest „podszywanie się" *(spoofing).* Bardzo ogólnie można powiedzieć, że polega ono na wysyłaniu datagramów IP z nieprawdziwym adresem źródłowym, przez co komputer je odbierający błędnie identyfikuje ich nadawcę. Najczęściej jest to właśnie wykorzystywane do podszywania się pod — przykładowo — stronę WWW banku, w którym obsługujemy nasze konto. Agresor może podszywać się, korzystając z różnych warstw modelu sieciowego i z różnych mechanizmów, jednak

wszystkie prowadzą do sytuacji, że tak naprawdę komunikujemy się z kimś innym niż chcielibyśmy.
Metody te są tak bardzo niebezpieczne ze względu na możliwość niezauważonej modyfikacji danych w przejętym przez crackera połączeniu. Cechą wspólną podszywania się jest konieczność unieszkodliwienia stacji, z którą chcemy się połączyć, tak aby pakiety przez nią generowane nie przeszkadzały w pracy włamywacza. Dokonuje się tego różnymi metodami, począwszy od fizycznych ataków, poprzez np. wyłączenie prądu (w sieci lokalnej), odcięcia od sieci poprzez uszkodzenie (zmianę konfiguracji) urządzenia sieciowego, z którego stacja ta korzysta, na ataku DoS *(Denial of Service)* skończywszy.
Jednym z rodzajów tego typu połączeń jest przypadek, gdy włamywacz przechwytuje połączenie (przechodzi ono przez jego komputer) i na bieżąco przekazuje je pomiędzy serwerem a klientem. Metodę tę nazwano „człowiek w środku" — **MITM** *(man in the middle).* W takim przypadku włamywacz może modyfikować informacje przesyłane w dowolnym kierunku. Przed tą metodą nie są bezpieczne nawet połączenia szyfrowane. Po prostu klient nawiązuje połączenie z serwerem włamywacza, a serwer włamywacza nawiązuje połączenie z serwerem docelowym i przekazuje pomiędzy nimi dane. Takie działanie możemy wykryć, sprawdzając w trakcie połączenia certyfikat serwera.

3.1.2.2. Destabilizacja pracy

Czasem crackerowi nie zależy na włamaniu do sieci, a na zdestabilizowaniu działania usług sieciowych i uniemożliwieniu zaatakowanemu serwerowi świadczenia usług. Na takie akcje **mówimy atak typu „odmowa usługi" DoS** *(Denial of Service).*

•Pochłanianie pasma

Aby uniemożliwić dostęp z Internetu do twoich serwerów i odciąć użytkowników sieci lokalnej od Internetu wystarczy po prostu zająć całe dostępne pasmo twojego łącza „na świat". Najprościej wykonać taką akcję, jeśli agresor posiada o wiele większe od ciebie łącze. Uruchamia po prostu ogromną liczbę połączeń, które wysycają całe pasmo.
Atak typu *Smurf* polega na wysłaniu wiadomości ICMP „echo" (ping) na adres rozgłoszeniowy jakiejś sieci, z adresem źródłowym ustawionym na IP twojego serwera. W tym przypadku wszystkie działające komputery w tej sieci odpowiadają komunikatami ICMP *echo reply* skierowanymi do twojego serwera.

•Pochłanianie zasobów

Tego typu działaniem jest ostatnio popularna metoda unieruchamianiu serwisów WWW. Polega ona na wysyłaniu olbrzymiej liczby zapytań do serwera WWW, który próbując je wszystkie obsłużyć, zostaje zablokowany. W celu obsłużenia wzrastającej liczby nawiązanych połączeń, usługa będzie zajmowała coraz więcej zasobów systemowych, aż do unieruchomienia serwera.

•Ataki w warstwie aplikacji

Są to ataki wykorzystujące słabości protokołów aplikacji. Istnieje osobny rodzaj ataków polegający na generowaniu dużej ilości poczty elektronicznej. Przykładowo agresor może zapisać atakowanego użytkownika równocześnie na kilkaset pocztowych list dyskusyjnych, z których każda generuje dużą ilość codziennych wiadomości. Istnieje wiele metod utrudniania życia za pomocą poczty elektronicznej, począwszy od przepełnienia skrzynki pocztowej, tzw. *mail-bombing,* poprzez wysyłanie wielu reklam, tzw. *spam,* aż do podszywania się pod znane użytkownikowi adresy i wysyłanie wymyślnych informacji wykorzystujących inżynierię społeczną (łańcuszki, informacje o pseudowirusach itp.).

•DDoS

Pierwsze ataki typu DDoS miały miejsce w lutym 2000 roku. Zostało wtedy unieruchomionych wiele serwisów należących do korporacji internetowych i medialnych.

Rozproszone ataki typu odmowa usługi (*Distributed Denial of Service)* — bo tak się one nazywają— wykorzystują skoordynowane w czasie ataki DoS dokonywane z dużej ilości hostów. Przygotowanie tego ataku jest mrówczą pracą wielu crackerów, polegającą na włamywaniu się do wielu słabo zabezpieczonych stacji, najczęściej prywatnych komputerów podłączonych bezpośrednio do Internetu.

Zagrożenia wewnętrzne

Większość różnorodnych metod zdobywania informacji i ataków opisanych przeze mnie wcześniej da się wykorzystać wewnątrz sieci lokalnej. Ponadto dochodzą inne zagrożenia, wynikające z możliwości, jakie ma użytkownik naszej sieci LAN.

Transmisja w wielu dotychczas powszechnie używanych protokołach — POP, IMAP, FTP, HTTP, telnet — nie jest szyfrowana. Jeśli więc ty korzystasz z tego typu protokołów, to nie możesz już być pewny tajności swoich haseł i haseł innych osób znajdujących się w twojej domenie kolizji. Z tego powodu twoja stacja robocza zawsze powinna być podłączona bezpośrednio do przełącznika sieciowego.

Najczęstszą metodą sniffingu jest programowe przełączenie karty sieciowej w tryb odbierania całego ruchu, nie tylko skierowanego na adres MAC tego interfejsu. Włączenie takiego trybu (jednoznacznie wskazującego na podsłuch) możemy wykryć, wykorzystując błąd w stosie TCP/IP niektórych systemów operacyjnych — m.in. starszych Linuksów.