Ochrona danych w organizacji

AŚ w Kielcach
Instytut Matematyki
Dr Zbigniew Bem

Literatura

- E. Cole, R. L. Krutz, J. Conley, *Bezpieczeństwo sieci Biblia*, Helion 2005.
- M. Kaeo, *Tworzenie bezpiecznych sieci*, Mikom 2000.
- M. Kutyłowski, W.B. Strothmann, *Kryptografia - teoria i praktyka zabezpieczania systemów komputerowych*, Oficyna Wydawnicza READ ME 1998.
- A. Sadowski, *Wybrane zagadnienia kryptologii i ochrony informacji*, Helion 1999.
- E. Schetina, K. Green, J. Carlon, *Bezpieczeństwo w sieci*, Helion 2002.
- B. Schneier, *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, WNT 1995, 2002.
- M. Stawowski , *Badanie zabezpieczeń sieci komputerowych*, ArsKom 1999.
- D. Stinson, *Kryptografia w teorii i praktyce*, WNT 2005.

Ochrona danych - dotyczy tworzenia, przechowywania i posługiwania się zbiorami danych, a także pojedynczymi danymi, mająca na celu administracyjnoprawną ochronę prawa do prywatności.

Regulacje prawne:
- prawo międzynarodowe
- prawo polskie

Utrata cennych danych lub poufnych informacji w firmie, może spowodować nieobliczalne skutki. Kradzież czy zniszczenie informacji nie tylko zagraża sprawnemu funkcjonowaniu przedsiębiorstwa, ale również może doprowadzić do jego bankructwa.
Mówiąc o bezpieczeństwie organizacji należy określić:
- co chronimy
- przed czym chronimy (czyli jakie są zagrożenia).

Ochrona danych jest jednym z najważniejszych zadań zapewniających bezpieczeństwo organizacji (firmie), w głównej mierze polega na:
- zarządzaniu bezpieczeństwem,
- legalizacją i uwierzytelnianiem dostępu do danych,
- zarządzanie treścią.

Do zarządzanie bezpieczeństwem potrzebna jest tzw. polityka bezpieczeństwa.

1.1 Polityka bezpieczeństwa

Zaprojektowanie zasad bezpieczeństwa organizacji to innymi słowy określenie jej *polityki bezpieczeństwa.* Polityka bezpieczeństwa powinna być przygotowana w sposób realistyczny i praktyczny. Oznacza to, że powinna odzwierciedlać faktyczne potrzeby związane z bezpieczeństwem organizacji i faktyczne możliwości jego zapewnienia oraz powinna dawać jasne wytyczne, w jaki sposób system bezpieczeństwa ma być konstruowany i jak ma funkcjonować.
Politykę bezpieczeństwa organizacji pod względem wagi i charakteru porównać można do polityki obronnej państwa. Określaniem polityki bezpieczeństwa zajmuje się zarząd organizacji oraz managerzy odpowiedzialni za bezpieczeństwo. Sposoby realizacji polityki obronnej to strategie obrony, natomiast zadania opracowywania i realizacji taktyk współdzielą kierownicy, administratorzy i użytkownicy.

Formalną podstawą systemu bezpieczeństwa w organizacji jest dokument zwany „Polityką bezpieczeństwa". W nim określa się, które zasoby organizacji mają być chronione i jakie metody powinny być do tego użyte. Dokument ten musi być zgodny z aktualnymi przepisami prawnymi. Poza wymienieniem potrzebnego do zapewnienia założonego poziomu bezpieczeństwa sprzętu, oprogramowania i zasobów ludzkich, musi definiować odpowiednie procedury na wypadek awarii czy włamania.
Politykę należy stosować w organizacji w sposób spójny. Powinna ona stanowić dla pracowników źródło informacji przydatnych podczas wykonywania codziennych obowiązków. Dobrze przemyślana i napisana polityka służy również w charakterze zabezpieczenia dla organizacji i jej zarządu w przypadku potrzeby wskazania odpowiedzialności.
W skład dokumentów polityki bezpieczeństwa wchodzą również standardy, zalecenia, wzorce i procedury.

Źródła polityki bezpieczeństwa.
• Analiza zasobów danych – które należy chronić - znajdujących się w organizacji oraz określenie ich wartości.
• Analiza struktury organizacyjnej.
•Analiza obiegu dokumentów w organizacji, metod ich niszczenia i poziomów dostępu do nich. Dodatkowo przydaje się jasne określenie zakresu informacji niejawnych, zwłaszcza dotyczących systemów informatycznych firmy.
• Analiza struktury fizycznej.
• Analiza ryzyka.

Główną zasadą, którą należy się kierować podczas tworzenia zasad bezpieczeństwa, jest: **„zabronione jest wszystko, co nie zostało bezpośrednio dozwolone".**

Rozpoznanie potrzeb zabezpieczania informacji powinno uwzględniać następujące zagadnienia jak:

- uprawnienia;
- obowiązki;
- zagrożenia;
- silne strony;
- usługi bezpieczeństwa;
- priorytety;
- ograniczenia projektowe.

Definicje
•**Słaby punkt** (podatność) określamy jako słabość procedur bezpieczeństwa systemu, jego projektu, implementacji lub wewnętrznych mechanizmów kontrolnych, która może zostać wykorzystana (przypadkowo lub celowo) i skutkować złamaniem zabezpieczeń lub naruszeniem polityki bezpieczeństwa.
•**Skutek** – różnorodne negatywne efekty, które mogą być wywołane w wyniku wykorzystania słabego punktu. Poziom skutku jest uzależniony od zagrożenia i stanowi relatywną wartość elementów dotkniętej nim infrastruktury i zasobów.

•**Ryzyko** jest funkcją prawdopodobieństwa udanego wykorzystania potencjalnego słabego punktu przez źródło zagrożenia oraz niepożądanego skutku takiego zdarzenia dla organizacji.

•**Zagrożenie** to potencjał wykorzystania (przypadkowego lub celowego) określonego słabego punktu przez źródło zagrożenia.

•**Źródło zagrożenia** jest definiowane jako:

1. Zamiar i metoda celowego wykorzystania słabego punktu.
2. Sytuacja i metoda przypadkowego wywołania negatywnego skutku za pośrednictwem słabego punktu.

Najczęściej spotykanymi typami źródeł zagrożeń są źródła naturalne, takie jak burze czy powodzie i źródła ludzkie, takie jak złośliwe ataki i działania przypadkowe oraz źródła środowiskowe, takie jak zanik zasilania.

Elementy organizacji podlegające ochronie podzielić można na trzy kategorie: zasoby materialne, dane (informacje) przechowywane w organizacji i - reputacja.

Zasoby materialne organizacji to cała infrastruktura produkcyjna (lub usługowa, w zależności od charakteru organizacji) i do jej ochrony stosowane są zwykle powszechnie znane metody zabezpieczeń (alarmy, zabezpieczenia antywłamaniowe, pracownicy ochrony, itp.). Ochrona zasobów materialnych organizacji jest zagadnieniem równie istotnym jak ochrona pozostałych jej elementów. Jednak w niniejszym wykładzie przyjmiemy założenie, że funkcjonowanie organizacji oparte jest na wykorzystaniu systemu informatycznego i bezpieczeństwu tegoż właśnie poświęcona będzie dalsza jego część. Należy jednak mieć na uwadze, iż niedostateczna ochrona organizacji przed fizycznym dostępem osób nie upoważnionych może mieć bardzo poważne konsekwencje.

Reputacja. Wbrew pozorom jest to bardzo ważny element i powinien podlegać szczególnej ochronie. Intruz zwykle podszywając się pod pracownika wysyłając obraźliwe lub nieprawdziwe informacje może wyrządzić wiele szkody. W przypadku podszywania się intruzów pod pracowników przez pewien okres, po niemiłych incydentach może powstać opinia, iż organizacja ta zatrudnia nie godne zaufania osoby (często niesłusznie) lub —już po wyjaśnieniu sprawy — osób nie potrafiących ochronić się przed włamaniem do systemu komputerowego (często słusznie). Taka utrata reputacji może powodować spadek zaufania do instytucji, co często daje w rezultacie wymierne straty finansowe.

Podstawy prawne ochrony informacji

Kodeks karny

•**Art. 267**: Kto bez uprawnień uzyskuje informacje nie dla niego przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne lub inne jej zabezpieczenie, podlega grzywnie, karze ***ograniczenia wolności*** albo ***pozbawienia wolności do lat dwóch.***

•**Art. 268**: Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji (…), jeżeli czyn dotyczy zapisu na komputerowym nośniku informacji, podlega karze ***pozbawienia wolności do lat trzech.***

•**Art. 269**: Kto na komputerowym nośniku informacji niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa (…) administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze ***pozbawienia wolności od sześciu miesięcy do lat ośmiu.***

•**Art. 287**: Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie

informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze ***pozbawienia wolności od trzech miesięcy do lat pięciu.***

Według policji wykrywalność wymienionych przestępstw – tzw. przestępstw przeciwko ochronie informacji – wynosi ponad 60 %.
W sumie co roku stwierdza się w Polsce kilkaset takich przestępstw, a ich liczba stale rośnie.

1.2. Bezpieczeństwo systemu informatycznego

W czasach gdy kluczowe dane dla każdej firmy i organizacji są przechowywane w postaci elektronicznej – bazy danych na serwerach – bezpieczeństwo systemów informatycznych jest sprawą niezwykle istotną. W wielu firmach pokutuje pogląd, że atak może nastąpić z zewnątrz – takie firmy posiadają zwykle doskonałe zabezpieczenia. Jednakże ochrona danych to nie tylko zabezpieczenie ich przed atakami z sieci – to także odpowiednia polityka postępowania wewnątrz firmy. Wiele spośród najgłośniejszych ataków crakerskich przeprowadzono od wewnątrz korporacyjnej sieci. Dlatego ważniejsze od urządzeń zabezpieczających jest świadomość pracowników, dopiero ona, w połączeniu z odpowiednim sprzętem i oprogramowaniem, gwarantuje bezpieczeństwo systemu informatycznego.

Ogólnie przyjęte zasady zabezpieczania systemów informatycznych

- Bezpieczeństwo informatyczne jest elementem ułatwiającym realizację misji organizacji.
- Bezpieczeństwo informatyczne jest integralnym elementem właściwego zarządzania.
- Bezpieczeństwo informatyczne powinno być efektywne pod względem kosztowym.
- Odpowiedzialność właścicieli systemu wybiega poza granice ich organizacji.
- Odpowiedzialność za bezpieczeństwo informatyczne oraz zasady rozliczania użytkowników powinny być jednoznaczne.
- Bezpieczeństwo informatyczne wymaga jasno zdefiniowanego i zintegrowanego podejścia.
- Skuteczność zabezpieczeń systemu powinna być okresowo weryfikowana.
- Bezpieczeństwo informatyczne jest ograniczone czynnikami społecznymi.

Cykl rozwoju systemu bezpieczeństwa

Cykl rozwoju systemu składa się z następujących etapów:

- inicjalizacja;
- wytworzenie lub pozyskanie;
- implementacja;
- użytkowanie i utrzymanie;
- wycofanie z użytku.

System informatyczny - przypomnienie

System informatyczny; system przetwarzający informacje - jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie informacji. Na systemy informatyczne składają się obecnie takie elementy jak:

- sprzęt - obecnie głównie komputery, oraz
  - urządzenia służące do przechowywania informacji
  - urządzenia służące do komunikacji między sprzętowymi elementami systemu
  - urządzenia służące do komunikacji między ludźmi a komputerami
  - urządzenia służące do odbierania informacji ze świata zewnętrznego - nie od ludzi *(na przykład czujniki elektroniczne, kamery, skanery)*

–urządzenia służące do wpływania systemów informatycznych na świat zewnętrzny - elementy wykonawcze *(na przykład silniki sterowane komputerowo, roboty przemysłowe)*
–urządzenia służące do przetwarzania informacji nie będące komputerami

- oprogramowanie
- zasoby osobowe - *ludzie*
- elementy organizacyjne - *czyli procedury korzystania z systemu informatycznego, instrukcje robocze itp.*

Bezpieczeństwo systemu informatycznego obejmuje:

- **Zarządzanie programowe** — zarządzanie bezpieczeństwem informatycznym na odpowiednich poziomach ze scentralizowanym systemem wymuszania i kontroli.
- **Zarządzanie ryzykiem** — proces oceny ryzyka, którego zadaniem jest redukcja ryzyka do akceptowalnych poziomów i utrzymanie tego poziomu ryzyka.
- **Planowanie cyklu rozwoju** — zarządzanie bezpieczeństwem na podstawie cyklu rozwoju systemu. Plan bezpieczeństwa systemu należy opracować przed etapem inicjalizacji cyklu rozwoju systemu, tak aby mógł być uwzględniony w kolejnych jego częściach.
- **Zagadnienia związane z personelem i użytkownikami** — ta kategoria praktyk obejmuje menedżerów, użytkowników i implementatorów oraz ich uprawnienia dostępu do zasobów systemu informatycznego.
- **Przygotowanie do zdarzeń losowych i katastrof**— planowanie zmierzające do zabezpieczenia działania organizacji w przypadku katastrofy lub przerwy w działaniu systemu.
- **Reakcja na wystąpienie incydentów związanych z zabezpieczeniami** — szybkie i efektywne podejmowanie odpowiednich działań na wypadek incydentów związanych z wewnętrznymi lub zewnętrznymi próbami uzyskania nieautoryzowanego dostępu.
- **Świadomość i szkolenia** — zapewnienie szkoleń kształtujących świadomość bezpieczeństwa informatycznego dla wszystkich pracowników mających kontakt z systemami informatycznymi.
- **Zagadnienia bezpieczeństwa w dziedzinie administracji i obsługi** — zastosowanie zasad bezpieczeństwa systemów informatycznych w zadaniach realizowanych przez administratorów systemu i zewnętrzne służby obsługi.
- **Bezpieczeństwo fizyczne i środowiskowe** — implementacja mechanizmów kontroli środowiskowej i fizycznej, takich jak utrzymanie i monitorowanie właściwej temperatury i wilgotności czy też zabezpieczenie komputerów przenośnych i nośników magnetycznych.
- **Identyfikacja i uwierzytelnianie** — implementacja środków kontroli dostępu z wykorzystaniem mechanizmów identyfikacji i uwierzytelniania w celu zabezpieczenia przed dostępem nieautoryzowanych użytkowników do zasobów systemu informatycznego.
- **Logiczna kontrola dostępu** — środki techniczne służące do wymuszania polityki bezpieczeństwa systemu informatycznego na poziomie dostępu do zasobów informatycznych.
- **Analiza zdarzeń** — zapis działań w systemie i zastosowanie środków umożliwiających śledzenie zdarzeń na poziomie poszczególnych użytkowników, detekcji włamań, rekonstrukcji zdarzeń nietypowych i identyfikacji problemów.
- **Kryptografia** — udostępnienie usług bezpieczeństwa, polegających na zabezpieczeniu poufności i integralności informacji poprzez implementację techniki podpisu elektronicznego.

Pierwszym etapem w projektowaniu ochrony informacyjnej firmy będzie określenie zasobów informatycznych organizacji które muszą podlegać ochronie oraz określenie ich wartości. Zasobami takimi mogą być:

•sprzęt — komputery, serwery, urządzenia sieciowe, fizyczna sieć komputerowa, połączenia telekomunikacyjne;
•oprogramowanie — programy używane w firmie, systemy operacyjne;
•dane — bazy danych, kopie bezpieczeństwa, logi systemowe oraz wszelakie transmisje tych danych;
•pozostałe — sieć zasilająca, pomieszczenia.

Następnymi etapami są charakterystyka systemu informatycznego, określenie zagrożeń oraz przyjęcie zasad bezpieczeństwa.

Scharakteryzowanie systemu

W ramach charakterystyki należy posiadać następujące informacje o systemie:
•oprogramowanie;
•sprzęt;
•dane;
•interfejsy systemowe;
•użytkownicy systemu informatycznego;
•personel systemu informatycznego;
•misja systemu;
•znaczenie systemu i danych;
•kluczowość systemu i danych;
•funkcjonalne wymagania w stosunku do systemu;
•polityka bezpieczeństwa systemowego;
•architektura bezpieczeństwa systemu;
•topologia sieci;
•zabezpieczenie nośników informacji;
•przepływ informacji w systemie;
•techniczne mechanizmy kontroli bezpieczeństwa;
•fizyczne środowisko bezpieczeństwa;
•bezpieczeństwo środowiskowe.

Zagrożenia

•Źródła zagrożeń.
•Kradzież i modyfikacja informacji, szpiegostwo.
•Blokowanie usług systemu.
•Działanie nieuprawnionych użytkowników w systemie.
•Zniszczenie danych, oprogramowania.

Najczęściej spotykanymi typami źródeł zagrożeń są **źródła naturalne,** takie jak burze czy powodzie, **źródła ludzkie,** takie jak złośliwe ataki i działania przypadkowe oraz **źródła środowiskowe,** takie jak zanik zasilania -do komputera odłączonego od sieci może podejść pani sprzątaczka i oprzeć wiadro z wodą na wyłączniku głównego UPS-u.

Z tego względu wyróżniamy dwa rodzaje bezpieczeństwa, fizyczne i elektroniczne.

Do zdarzeń fizycznych, przed którymi powinniśmy się zabezpieczać, należą:
- awaria instalacji zasilającej — UPS-y, dublowanie instalacji i układów zasilających,

- pożar — aktywny system przeciwpożarowy, ochrona kopii bezpieczeństwa w specjalnej szafie wytrzymującej wysokie temperatury,
- zalanie — umieszczenie kopii bezpieczeństwa w innej lokalizacji (najlepiej w innym budynku),
- przegrzanie — zdublowanie systemu klimatyzacji, zapewnienie awaryjnego zasilania również klimatyzatorom,
- włamanie — system antywłamaniowy, odpowiednie zabezpieczenia fizyczne,
- nieuprawniony dostęp fizyczny — przestrzeganie procedur dostępu do serwerowni i szafy przechowującej kopie danych, sprzątanie pomieszczeń jedynie podczas pobytu osób uprawnionych.

Do aspektów fizycznych bezpieczeństwa należy też zdefiniowanie obiegu dokumentów w firmie, metod ich niszczenia (niszczarki) i poziomów dostępu do nich. Dodatkowo przydaje się jasne określenie zakresu informacji niejawnych, zwłaszcza dotyczących systemów informatycznych firmy.

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".

Kradzież i modyfikacja informacji, szpiegostwo
Istnieje cały szereg zagrożeń dla bezpieczeństwa systemu informatycznego organizacji. Najbardziej oczywiste są zagrożenia związane z kradzieżą i nielegalną modyfikacją danych. Kradzieży mogą podlegać informacje, które później są wykorzystywane bezpośrednio (np. informacje o planach działań firmy) lub informacje pośredniczące w uzyskaniu innych informacji (np. kradzież haseł przesyłanych kanałami transmisyjnymi). Zdobycie poufnych informacji przez intruza nie musi odbywać się na drodze technicznej; informacje te może wyłudzić lub zdobyć podstępem od użytkowników systemu. Dlatego też niezwykle ważną rolę w ochronie informacji odgrywa czynnik ludzki. Istotnym zagrożeniem jest również niewłaściwe skonfigurowanie usług sieciowych świadczonych przez system informatyczny organizacji. Poufne informacje mogą wówczas „przeciekać" legalnymi kanałami przepływu informacji. Szereg zagrożeń wiąże się również z bezprawną modyfikacją danych. Systemy powinny być w odpowiedni sposób zabezpieczane przed kradzieżą i atakami na autentyczność danych.

Szczególnie niebezpieczną odmianą kradzieży informacji jest szpiegostwo. Szpiegostwo ma na celu zdobycie ważnych, poufnych danych w celu późniejszego wykorzystania ich przeciw właścicielowi. Istnieją różne odmiany tej działalności: szpiegostwo przemysłowe, militarne, polityczne. Znane są przykłady takich działań: włamania do sieci komputerowej Pentagonu czy wspomniana afera polityczna „Computergate". Niebezpieczeństwa wynikające z działalności szpiegów są powszechnie znane i nie wymagają komentarza. Wzrost poziomu tych zagrożeń w ostatnich latach związany jest silnie z dynamicznym rozwojem globalnej sieci komputerowej.

Blokowanie usług systemu
Jednym z najprostszych do przeprowadzenia przez intruza ataków na system jest atak polegający na tak silnym przeciążeniu działania systemu, iż niemożliwa okaże się praca w tym systemie. Ten rodzaj sabotażu może sparaliżować pracę organizacji w takim stopniu, że nie będzie ona mogła normalnie funkcjonować. Napastnik „zaleje" system falą komunikatów, listów elektronicznych, połączeń modemowych i żądań usług sieciowych w tak dużym stopniu, że system nie będzie praktycznie robił nic poza próbami wykonania tych wszystkich zleceń. Bardziej wyrafinowane ataki polegają na przekierowaniu żądań usług systemu w inne, zupełnie niewłaściwe miejsca. Szczególną bolączką jest fakt, że ochrona przed blokadą usług systemu jest bardzo trudna; w praktyce wiąże się z izolowaniem systemu od otoczenia sieciowego.

Działanie nieuprawnionych użytkowników w systemie
Jak wspomnieliśmy wcześniej, zagrożone są również zasoby komputerowe systemu, takie jak: pamięć dyskowa, czas obliczeniowy, pamięć operacyjna. Niezależnie od tego, że działanie w systemie komputerowym organizacji nieproszonych gości przeciąża system, to jest także źródłem powstawania innych, poważniejszych zagrożeń, jak kradzież informacji czy różnorakie formy jej modyfikacji.

Zniszczenie danych, oprogramowania
Zniszczenie danych przechowywanych, systemie komputerowym organizacji może być zarówno aktem wandalizmu, jak i świadomym działaniem konkurencji. Nawet jeśli istnieją kopie bezpieczeństwa systemu, to ponowne instalowanie systemu operacyjnego, specjalistycznego oprogramowania czy danych wiąże się ze stratą pewnej ilości czasu i całkowitym lub częściowym zablokowaniem funkcjonowania instytucji. Istnieją też pewne informacje, które zostaną utracone bezpowrotnie, a mianowicie te, które powstały od czasu utworzenia ostatniej kopii bezpieczeństwa systemu.

1.3. Metody oceny bezpieczeństwa systemu informatycznego
Pierwsza z tych metod polega na przydziale systemowi tzw. *klasy bezpieczeństwa* określonej w ramach szeroko obecnie stosowanego standardu „The Orange Book". Pełna nazwa tego standardu to *Trusted Computer Systems Evaluation Criteria.* Dokument ten opracowany został w Departamencie Obrony USA i zawiera opis kryteriów przydziału analizowanych systemów do odpowiednich klas bezpieczeństwa, informacje na temat sposobu wykonywania analiz bezpieczeństwa, a także zalecenia dotyczące zapewniania bezpieczeństwa systemu informatycznego.
Druga metoda oceny poziomu bezpieczeństwa polega na wykonaniu ekspertyz określanych mianem analizy ryzyka. Cechą charakterystyczną analizy ryzyka jest to, że dokonywana ocena w silnym stopniu uwzględnia prawdopodobieństwo wystąpienia danego zagrożenia - w myśl zasady, że byłoby nierozsądne zajmować się względnie mało prawdopodobnym

ryzykiem wówczas, gdy nie zostały jeszcze odparte zagrożenia potencjalnie bardziej dotkliwe w skutkach.

The Orange Book
W pierwszej części *The Orange Book* zdefiniowane są podstawowe pojęcia i koncepcje omawiane w dalszej części dokumentu. Oto one:
Monitor referencyjny jest mechanizmem wymuszania autoryzowanego Dostępu podmiotów systemu do jego obiektów. Natomiast mechanizm kontroli poprawności odwołania jest implementacją koncepcji monitora referencyjnego. Mechanizm ten służy do sprawdzania poprawności każdego odwołania do danych lub programu przez użytkownika (lub program) pod względem zgodności z listą autoryzowanych typów dostępów dla danego użytkownika. W związku z tym mechanizm kontroli poprawności odwołania musi być:
• odporny na próby niepoprawnego użytkowania,
• zawsze uruchamiany,
• dostatecznie mały, by mógł być poddawany analizie i testom w celu sprawdzenia pewności zabezpieczenia.

Wczesne implementacje mechanizmu kontroli poprawności odwołań znane są pod nazwą *jąder ochrony.* Jądro ochrony jest kombinacją sprzętu i oprogramowania, które realizują koncepcję monitorowania odwołań.
Aby rozszerzyć kryteria oceny bezpieczeństwa również na systemy nie zawierające jądra ochrony, wprowadzono pojęcie *Trusted Computing Base (TCB).* TCB jest „sercem" bezpiecznego systemu komputerowego zawierającym wszystkie elementy odpowiedzialne za realizację polityki bezpieczeństwa i wspieranie izolacji obiektów systemu objętych ochroną. Tak więc TCB zawiera sprzęt i oprogramowanie krytyczne dla ochrony systemu i musi być zaprojektowane i zaimplementowane tak, aby zapewniać założony poziom ochrony. TCB powinna mieć na tyle prostą strukturę, aby możliwe było wykonanie testów i analiz, dających odpowiedź na pytanie, czy system jest godny zaufania.

1.4. Klasy oceny bezpieczeństwa
Ocena poziomu bezpieczeństwa systemu polega na zakwalifikowaniu go do którejś z poniższych klas:
Klasa D: Minimal protection
Do klasy tej włączane są systemy, które były ocenione, ale nie zostały zakwalifikowane do żadnej z pozostałych klas.
Klasa Cl: Discretionary security protection
TCB tej klasy zapewnia separację użytkowników i danych. Uzyskany poziom bezpieczeństwa pozwala użytkownikom chronić dane związane z projektami, nad którymi pracują, czy dane prywatne, uniemożliwiając innym użytkownikom ich odczyt, modyfikowanie lub usuwanie.
Klasa C2: Controlled access protection
Systemy tej klasy wymuszają silniejszy poziom ochrony niż dla klasy Cl poprzez wprowadzanie procedur logowania, mechanizmów audytu i izolacji zasobów.
Klasa B1: Labeled security protection
Systemy te posiadają wszystkie właściwości systemów klasy C2. Dodatkowo wprowadzony jest element *etykietowania* podmiotów i obiektów (opisywania ich właściwości w systemie bezpieczeństwa).
Klasa B2: Structured protection
TCB jest oparta na jasno zdefiniowanej i udokumento-wanej polityce bezpieczeństwa. Ponadto TCB musi być podzielona na część krytyczną pod względem ochrony *(protection-critical)* i resztę. TCB ma posiadać dobrze zdefiniowany interfejs i jest łatwa w testowaniu

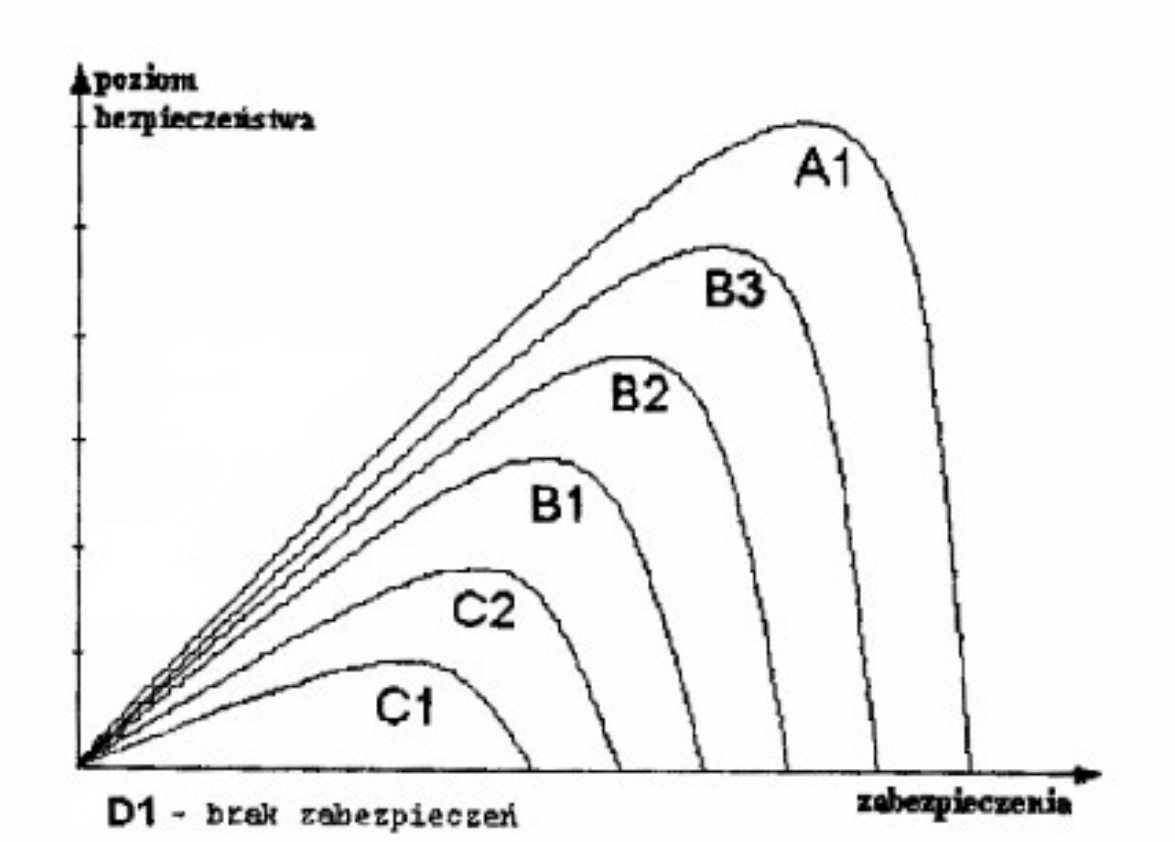
(posiada odpowiednie mechanizmy). Wzmocnione muszą być mechanizmy uwierzytelniania oraz narzędzia administrowania bezpieczeństwem systemu. System musi być *względnie* odporny na penetrację

Klasa B3: Security domains

Zminimalizowana jest złożoność TCB w celu umożliwienia wykonania dokładniejszych analiz. System posiada silne wsparcie dla administracji bezpieczeństwem, mechanizm audytu rozszerzony do reagowania na sygnały związane z bezpieczeństwem. Wymagane jest opracowanie procedur odtwarzania stanu systemu. System jest wysoce odporny na penetrację.

Klasa A1: Verified design

Systemy tej klasy są funkcjonalnie równoważne systemom klasy B3. Różnica polega na tym, że istnieje możliwość weryfikacji, czy TCB jest poprawnie zaimplementowana.



1.5. Analiza ryzyka

Analiza ryzyka to systematyczny podział zagrożeń danych i środków im przeciwdziałających na kategorie oraz określenie planu działania, który skieruje większość zasobów (technicznych i pozatechnicznych) przeciw najbardziej prawdopodobnemu ryzyku.

Istotną sprawą jest uwzględnianie *priorytetów zagrożeń.* Analiza ryzyka nie ma na celu stworzenia planu całkowitej ochrony; ma zapewnić stopień bezpieczeństwa proporcjonalny do wagi chronionej informacji.

Do elementów analizy ryzyka należą:

- zagrożenia, częstość zagrożeń,
- cele,
- odporność na zagrożenia,
- konsekwencje ataków,

- stosunek ryzyka do potencjalnych strat,
- ochrona, koszt ochrony,
- koszt analizy,
- implementacja mechanizmów ochrony.

1.6. 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.

Zarządzanie bezpieczeństwem systemu informatycznego odbywa się metodą zstępującą. Zarząd jednostki musi skonstruować, dystrybuować i wymuszać stosowanie polityki bezpieczeństwa organizacji. Ważnym aspektem tej polityki 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. 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. Opracowując politykę bezpieczeństwa, należy pamiętać, aby była możliwa do zrealizowania; należy uwzględnić istniejące narzędzia ochrony i koszt jej realizacji. Mówiąc o koszcie wdrożenia polityki bezpieczeństwa, należy zaznaczyć, że do jej realizacji nie zawsze musi być używane drogie oprogramowanie komercyjne.
Bezpieczeństwo informatyczne powinno być efektywne pod względem kosztowym - praktyki zarządcze umożliwiają uzyskanie znaczących redukcji ryzyka po rozsądnych kosztach – zależy to od przyjętego modelu bezpieczeństwa.

Modele bezpieczeństwa

Brak ochrony

Jednym z modeli bezpieczeństwa jest brak jakichkolwiek zabezpieczeń. Można go określić mianem „modelu zerowego", ponieważ nie są stosowane żadne środki ochrony informacji. Brak ochrony możemy zaobserwować w organizacjach, których władze uznały, że poziom ryzyka zagrożenia jest niewspółmiernie mały w porównaniu do kosztów wdrożenia polityki bezpieczeństwa, oraz w instytucjach, których władze zaniedbały aspekt bezpieczeństwa (z takich czy innych przyczyn). W sytuacji gdy pojawi się zagrożenie i spowoduje poważne konsekwencje władze organizacji wydają duże środki na zabezpieczanie instytucji i często wielokrotnie większe na likwidację skutków ataku.

Bezpieczeństwo dzięki brakowi zainteresowania ze strony otoczenia

Ten model opiera się na fakcie, że system informatyczny organizacji jest tak mało istotny dla konkurencji i tak mało ciekawy dla włamywaczy włamujących się „dla sportu" lub wandali,

że bezpieczeństwo można oprzeć na dużym prawdopodobieństwie braku prób ataku. Niestety, system ten bywa zawodny zwłaszcza w odniesieniu do ataków włamywaczy „sportowców" i wandali.

Ochrona na poziomie poszczególnych komputerów
Prawdopodobnie najszerzej stosowaną metodą ochrony jest ochrona na poziomie poszczególnych komputerów. Choć w aspekcie pojedynczego komputera metoda ta - jeśli poprawnie zrealizowana - jest jak najbardziej właściwa to w odniesieniu do całego systemu informatycznego organizacji ma tę wadę, że jest trudno skalowalna. Związane jest to faktem, że system jest przeważnie w taki czy inny sposób zróżnicowany; różne mogą być platformy sprzętowe czy systemy operacyjne, dla jednakowych systemów czy programów - różne ich wersje czy konfiguracje. W sytuacji takiej pielęgnacja mechanizmów ochrony w tych wszystkich środowiskach jest złożona i nieefektywna.
Ochrona na poziomie poszczególnych komputerów wymaga dostępu do każdego komputera w trybie specjalnym (jako tzw. *superużytkownik root).* Taka osoba będzie miała specjalne prawa dostępu do komputera, który przecież jest elementem składowym całej sieci. W takiej sytuacji w instytucji pojawi się wielu użytkowników, na których spoczywać będzie odpowiedzialność za bezpieczeństwo systemu. W praktyce wielu spośród tych użytkowników nie będzie miało dość kompetencji i/lub czasu, aby zagadnieniami bezpieczeństwa zajmować się w sposób właściwy.
Jak widać, model ten najprawdopodobniej nie sprawdzi się w przypadku dużych systemów. Jednak całkiem nieźle może funkcjonować dla systemów niedużych.

Ochrona w skali całego systemu (całej sieci komputerowej organizacji)
Dla dużych systemów informatycznych ochrona w skali całego systemu wydaje się rozwiązaniem lepszym niż ochrona na poziomie pojedynczych komputerów. Przy przyjęciu takiego modelu bezpieczeństwa zajmujemy się kontrolowaniem wszystkich dostępów do komputerów czy usług poprzez sieć, a nie ochroną poszczególnych maszyn. Narzędziami wykorzystywanymi w funkcjonowaniu takiego modelu są silne procedury uwierzytelniania (np. Kerberos, procedury z inteligentnymi kartami), architektury separujące (systemy *flrewall)* czy szyfrowanie (programy do szyfrowania poczty czy sesji komunikacyjnych w sieci).

Podsumowanie

Podstawowe wymogi bezpieczeństwa komputerowego
1. Polityka bezpieczeństwa
Musi istnieć jasna i dobrze zdefiniowana polityka bezpieczeństwa systemu. Ponadto muszą istnieć mechanizmy wymuszające jej realizację.
2. Opis obiektów
Dla każdego obiektu systemu muszą być określone następujące informacje: poziom ochrony, do którego obiekt należy (tzn. obiekty muszą być w systemie poklasyfikowane według kryterium bezpieczeństwa) oraz prawa dostępu podmiotów, które potencjalnie mogą starać się o dostęp do obiektu.
3. Identyfikacja
Podmioty muszą być nazwane (w jakiś sposób), aby możliwa była ich identyfikacja.
4. Audyt
Podstawowym celem audytu jest weryfikacja, czy wyznaczone cele zostały osiągnięte lub czy działania są zgodne z zaakceptowanymi standardami. Audyt ocenia także procedury kontrolne celem stwierdzenia, czy przedmiot audytu także w przyszłości będzie odpowiadał ustalonym

wymaganiom. Informacje z audytu muszą być gromadzone, rejestrowane i przechowywane w bezpieczny sposób w celu umożliwienia wykonania dokładnej analizy ewentualnych zagrożeń.

5. Pewność

System komputerowy musi zawierać sprzętowe i/lub programowe mechanizmy zabezpieczeń, które można w sposób niezależny ocenić pod względem stopnia spełniania wymogów 1 - 4.

6. Ciągła ochrona

Mechanizmy ochrony muszą być stale chronione przed nieautoryzowanym dostępem. W przeciwnym wypadku niemożliwe jest utrzymanie odpowiedniego poziomu ochrony.

Należy pamiętać, że osiągnięcie całkowitego bezpieczeństwa informatycznych dzisiejszych systemach informatycznych jest w praktyce nieosiągalne. Związane jest to z faktami, iż:
•systemy komputerowe często są systemami „otwartymi"; zaimplementowanie w nich „stuprocentowego" bezpieczeństwa mogłoby spowodować, że straciłyby swój charakter,
•koszt wprowadzenia absolutnego bezpieczeństwa mógłby być tak wysoki, iż przerósłby wartość samego systemu.

Ocena bezpieczeństwa systemu informatycznego może jednak uświadomić, jakie istnieją w nim luki i niedociągnięcia, a przez to znacząco przyczynić się do podniesienia poziomu ochrony
informacji przechowywanych i przetwarzanych w tym systemie.
Formalny proces inżynierii bezpieczeństwa systemów informatycznych udostępnia solidną podstawę do określania, projektowania, implementacji i oceny systemów wysokiej jakości, cechujących się znacznym poziomem bezpieczeństwa informacji. Zarządzanie ryzykiem oraz zasady bezpieczeństwa systemu informatycznego, zastosowane w ramach cyklu rozwoju systemu zapewniają obsługę systemu na akceptowalnym poziomie ryzyka od fazy rozwoju po fazę wycofania z użytku.

W kolejnym wykładzie zostaną opisane narzędzia i techniki zarządzania bezpieczeństwem systemu informatycznego, w tym procedury administracyjne, metody przywracania, wykonywanie kopii zapasowych krytycznych danych, bezpieczeństwo fizyczne, zagadnienia prawne i kwestie odpowiedzialności.