1. Wprowadzenie do problematyki bezpieczeństwa systemów komputerowych

Co to jest bezpieczeństwo?

Przedstawienie problematyki bezpieczeństwa systemów komputerowych systemów komputerowych należy rozpocząć od zdefiniowania pojęcia bezpieczeństwa. Niestety trudno skonstruować uniwersalną i jednoznaczną definicję tego pojęcia, która pokryłaby wszystkie oczekiwania stawiane w tej dziedzinie systemom komputerowym. Literatura przedmiotu podaje bardzo dużo, często znacznie odbiegających od siebie definicji. Przykład ciekawej definicji można znaleźć w [1]:

> Def.: **System komputerowy** jest **bezpieczny**, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją.

W myśl tej definicji, możemy system uznać za bezpieczny, jeśli np. można od niego oczekiwać, że wprowadzone na stałe dane nie zostaną utracone, nie ulegną zniekształceniu i nie zostaną pozyskane przez nikogo nieuprawnionego – ufamy, że system będzie przechowywał i chronił dane.

Bezpieczeństwo jest elementem szerszego kontekstu, nazywanego wiarygodnością systemu komputerowego. W kontekście tym wyróżnia się w sumie cztery atrybuty wiarygodności:

System wiarygodny =
- dyspozycyjny (*available*) = dostępny na bieżąco
- niezawodny (*reliable*) = odporny na awarie
- bezpieczny (*secure*) = zapewniający ochronę danych
- bezpieczny (*safe*) = bezpieczny dla otoczenia, przyjazny dla środowiska

Czynniki decydujące o znaczeniu bezpieczeństwa

O doniosłości problematyki bezpieczeństwa dla współczesnej cywilizacji decyduje przede wszystkim wszechobecność technik komputerowych. W szczególności rozważyć należy następujące zagadnienia:

- rola systemów informatycznych (szczególnie sieci) dla funkcjonowania współczesnej cywilizacji jest nie do przecenienia; nie ma już praktycznie obszaru działalności człowieka, w którym żadne elementy techniki komputerowej (bądź szerzej mikroprocesorowej) nie byłyby obecne. Jako drobny przykład niech posłuży telefonia komórkowa, towarzysząca dziś człowiekowi niemal ciągle i wszędzie;

- trudności związane ze skonstruowaniem i eksploatacją systemu spełniającego wysokie wymagania w zakresie bezpieczeństwa (niedoskonałości technologii, konfiguracji i polityki bezpieczeństwa) stwarzają niebezpieczeństwo niedopracowanego pod względem bezpieczeństwa i niezawodności produktu informatycznego lub nieodpowiedniego pod owym względem wykorzystania tego produktu;

- elementarny konflikt interesów występujący pomiędzy użytecznością systemu a ryzykiem związanym z jego wykorzystaniem rodzi szereg pragmatycznych problemów (często całkowicie pozatechnicznych) związanych z oczywistymi utrudnieniami we wdrożeniu i użytkowaniu systemów o podwyższonym bezpieczeństwie.

Zagrożenia bezpieczeństwa

Zagrożenia bezpieczeństwa mają różną naturę. Mogą być najzupełniej przypadkowe lub powstać w efekcie celowego działania. Mogą wynikać z nieświadomości lub naiwności użytkownika, bądź też mogą być motywowane chęcią zysku, poklasku lub odwetu. Mogą pochodzić z zewnątrz systemu lub od jego środka.

Większość działań skierowanych w efekcie przeciwko bezpieczeństwu komputerowemu jest w świetle aktualnego prawa traktowana jako przestępstwa. Możemy tu wyróżnić w szczególności:

- włamanie do systemu komputerowego
- nieuprawnione pozyskanie informacji
- destrukcja danych i programów
- sabotaż (sparaliżowanie pracy) systemu
- piractwo komputerowe, kradzież oprogramowania
- oszustwo komputerowe i fałszerstwo komputerowe
- szpiegostwo komputerowe

Istotne jest, iż w przypadku jurysdykcji większości krajów europejskich, praktycznie wszystkie przypadki naruszające bezpieczeństwo wyczerpują znamiona przestępstw określonych w obowiązującym prawie.

W Polsce w szczególności mają tu zastosowanie:

- artykuły 267-269 Kodeksu Karnego
- artykuł 287 Kodeksu Karnego

(http://www.gazeta-it.pl/prawo/przestepstwa_komputerowe.html)

Zazwyczaj przestępstwa te nie są ścigane z oskarżenia publicznego, lecz na wniosek pokrzywdzonego.

W kontekście bezpieczeństwa komputerowego powszechnie spotyka użycie popularnego terminu hacker na określenie osoby podejmującej atak. Termin ten oryginalnie nie posiadał wydźwięku pejoratywnego. Wg „The Hacker's Dictionnary" (Guy L. Steele et al.) hacker jest to (1) osoba, której sprawia przyjemność poznawanie szczegółowej wiedzy na temat systemów komputerowych i rozszerzanie tej umiejętności, w przeciwieństwie do większości użytkowników, którzy wolą uczyć się niezbędnego minimum; (2) osoba, która entuzjastycznie zajmuje się programowaniem i nie lubi teorii dotyczącej tej dziedziny. W związku z tym w niniejszych materiałach stosować będziemy bardziej odpowiednie terminy (zależnie od typu rozważanego ataku), takie jak: cracker, intruz, włamywacz, napastnik, wandal czy po prostu – przestępca.

Przykłady ataków na systemy informatyczne znaleźć można w wielu dziedzinach życia osobistego, gospodarki, przemysłu czy funkcjonowania organów państwowych. Przykładowo w 1997 r. CIWARS (Centre for Infrastructural Warfare Studies) odnotował 2 incydenty (w Brazylii i w Australii) zaciekłej konkurencji gospodarczej, w których zaatakowały się wzajemnie (omawianymi później atakami SYN flood) konkurujące ze sobą firmy ISP (operatorzy dostępu do Internetu). Jako działania anarchistyczne można sklasyfikować przykładowo incydent z 1997 r., w którym grupa Damage Inc. zastąpiła witrynę Urzędu Rady Ministrów stroną proklamującą utworzenie Hackrepubliki Polskiej i Centrum Dezinformacyjnego Rządu z odsyłaczami do `playboy.com`. Być może jako terroryzm natomiast – incydent z 1998 r., gdy w akcie protestu przeciwko próbom nuklearnym grupa Milw0rm zaatakowała systemy indyjskiego BARC (Bhabba Atomic Research Center).

Komponenty systemu informatycznego w kontekście bezpieczeństwa

Elementarne składniki systemu informatycznego jakie należy wyróżnić przy omawianiu problematyki bezpieczeństwa to:

- stanowisko komputerowe i infrastruktura sieciowa
- system operacyjny i usługi narzędziowe
- aplikacje użytkowe

Ogólne problemy konstrukcji zabezpieczeń

Problematyka bezpieczeństwa, jak każda dziedzina, podlega pewnym ogólnym prawom, niektórym sformalizowanym, innym – nieformalnym. Można wyróżnić pewne truizmy obowiązujące podczas projektowania i realizowania zabezpieczeń. Niektóre z nich to:

- Nie istnieje absolutne bezpieczeństwo. Wiąże się to z wieloma przyczynami. Jedną z nich jest fakt, iż nigdy nie jesteśmy w stanie przewidzieć z góry wszystkich możliwych zagrożeń, tym bardziej że często należy opracowywać zabezpieczenia z odpowiednim wyprzedzeniem. Szybki rozwój technologii informatycznych implikuje powstawanie coraz to nowych zagrożeń. Czas reakcji na nie nigdy nie jest zerowy i w związku z tym nawet dla najlepiej opracowanego systemu zabezpieczeń istnieje ryzyko powstania okresu dezaktualizacji zastosowanych mechanizmów bezpieczeństwa. Ewolucja zagrożeń pociąga za sobą wyścig atakujących i broniących („policjantów i złodziei"). Innym istotnym powodem niemożliwości osiągnięcia 100% bezpieczeństwa jest ludzka słabość, w szczególności omylność projektantów, programistów, użytkowników systemów informatycznych, skutkująca błędami w oprogramowaniu systemowym i aplikacyjnym oraz niewłaściwym lub niefrasobliwym jego wykorzystaniu.

  Skoro zatem nie mamy 100% bezpieczeństwa, jaki jego poziom można uznać za zadowalający? Otóż wydaje się, że najwłaściwszą odpowiedzią na to pytanie jest – taki, który okaże się dla atakującego na tyle trudny do sforsowania, wymagając operacji żmudnych lub czasochłonnych, iż uczyni to atak nieatrakcyjnym lub nieekonomicznym (lub oczywiście nieopłacalnym wg innego kryterium obranego przez atakującego). Zatem należy na tyle utrudnić włamywaczowi atak, aby z niego zrezygnował widząc marne, choć nadal niezerowe, szanse powodzenia.

- Napastnik na ogół nie pokonuje zabezpieczeń, tylko je obchodzi. Przeprowadzenie skutecznego ataku na jakikolwiek aktywny mechanizm zabezpieczeń jest raczej czasochłonne i stosowane tylko w ostateczności. Zwykle mniej kosztowne i szybsze

jest znalezienie luki w środowisku systemu informatycznego, zabezpieczanego owym mechanizmem niż łamanie jego samego, która to luka pozwoli skutecznie wtargnąć do systemu nie jako „z boku" zabezpieczeń. Przy tej okazji warto wspomnieć, że okazuje się niezmiennie od wielu lat, iż większość ataków przeprowadzanych na systemy informatyczne realizowana jest „od środka", czyli przez zaufanych, poniekąd, użytkowników systemu, którzy znając system jakim się posługują niewątpliwie łatwiej mogą znaleźć i wykorzystać luki bezpieczeństwa.

- Nie należy pokładać zaufania w jednej linii obrony. Z poprzedniej obserwacji wynika, że obejście aktywnego mechanizmu zabezpieczeń często bywa możliwe i może istotnie narażać bezpieczeństwo całego systemu. W związku z tym, naturalną konsekwencją tego jest konstruowanie wielopoziomowych zabezpieczeń poprzez budowanie kolejnych swoistych „linii obrony", z których każda po przejściu poprzedniej stanowić będzie, przynajmniej potencjalnie, kolejną zaporę dla atakującego.

- Złożoność jest najgorszym wrogiem bezpieczeństwa. Skomplikowane systemy są trudne do opanowania, również pod względem bezpieczeństwa. Istotnym usprawnieniem zarządzania systemem jest jego modularna konstrukcja, dająca szansę na zwiększenie kontroli nad konfiguracją i funkcjonowaniem systemu. Dotyczy to również wielopoziomowych zabezpieczeń.

- System dopóty nie jest bezpieczny, dopóki nie ma pewności że jest. Bardzo łatwo popełnić błąd zakładając zupełnie inaczej – dopóki brakuje odnotowanych symptomów, iż bezpieczeństwo systemu zostało naruszone, możemy spać spokojnie. Zaobserwowanie ataku nie jest trywialne nawet w systemie poprawnie monitorowanym. Ponadto symptomy ataku zwykle występują dopiero po jego zakończeniu, kiedy to może być zbyt późno by przeprowadzać akcję ratunkową, kiedy ucierpiały już newralgiczne składniki systemu, poufne dane lub reputacja firmy.

Wzrost poziomu bezpieczeństwa odbywa się kosztem wygody. Użytkownicy systemu pragną przede wszystkim efektywności i wygody swojej pracy.

Strategia bezpieczeństwa

Opracowanie skutecznych zabezpieczeń jest problemem bardzo złożonym. Wymaga uwagi i systematyczności na każdym etapie. Niewątpliwie decydujące znaczenia ma etap projektowy, na którym popełnione błędy mogą być nienaprawialne w kolejnych etapach. Etap projektowy powinien rozpocząć się od wypracowania strategii firmy dotyczącej bezpieczeństwa (i to nie wyłącznie systemu informatycznego). Polega to w ogólnym schemacie na odpowiedzi na następujące pytania:

1. „Co chronić?" (określenie zasobów)
2. „Przed czym chronić?" (identyfikacja zagrożeń)
3. „Ile czasu, wysiłku i pieniędzy można poświęcić na należną ochronę" (oszacowanie ryzyka, analiza kosztów i zysku)

Określenie zasobów = „Co chronić?"

Zasoby jakie mogą podlegać ochronie obejmują m.in. (w zależności od typu instytucji, dziedziny działalności itp.):

- sprzęt komputerowy

- infrastruktura sieciowa
- wydruki
- strategiczne dane
- kopie zapasowe
- wersje instalacyjne oprogramowania
- dane osobowe
- dane audytu
- zdrowie pracowników
- prywatność pracowników
- zdolności produkcyjne
- wizerunek publiczny i reputacja

Identyfikacja zagrożeń = „Przed czym chronić?"

Zagrożenia jakie należy rozważyć stanowią m.in.:

- włamywacze komputerowi
- infekcje wirusami
- destruktywność pracowników / personelu zewnętrznego
- błędy w programach
- kradzież dysków / laptopów (również w podróży służbowej)
- utrata możliwości korzystania z łączy telekomunikacyjnych
- bankructwo firmy serwisowej / producenta sprzętu
- choroba administratora / kierownika (jednoczesna choroba wielu osób)
- powódź

Polityka bezpieczeństwa

Polityka bezpieczeństwa stanowi element polityki biznesowej firmy. Jest to formalny dokument opisujący strategię bezpieczeństwa. Jej realizacja podlega oczywistym etapom:

1. zaprojektowanie
2. zaimplementowanie
3. zarządzanie (w tym monitorowanie i okresowe audyty bezpieczeństwa)

Szczególnie godnym podkreślenia jest etap 3. odzwierciedlający ciągłą ewolucję jaką przechodzą działalność firmy, środowisko rynkowe jej funkcjonowania, zagrożenia i technologie obrony. Wymaga to ciągłego "trzymania ręki na pulsie".

Zakres

Zakres tematyczny jaki powinna obejmować polityka bezpieczeństwa to:

- definicja celu i misji polityki bezpieczeństwa
- standardy i wytyczne których przestrzegania wymagamy
- kluczowe zadania do wykonania
- zakresy odpowiedzialności

Specyfikacja środków

Polityka bezpieczeństwa winna definiować środki jej realizacji obejmujące takie elementy jak:

- ochrona fizyczna
- polityka proceduralno-kadrowa (odpowiedzialność personalna)
- mechanizmy techniczne

Normy i zalecenia zarządzania bezpieczeństwem

Istnieje wiele dokumentacji poświęconej realizacji polityki bezpieczeństwa, w tym również norm i standardów międzynarodowych, którymi należy posiłkować się przy opracowywaniu własnej polityki bezpieczeństwa. Pod tym względem kanonem jest norma ISO/IEC Technical Report 13335 (ratyfikowana w naszym kraju jako PN-I-13335). Norma ta jest dokumentem wieloczęściowym obejmującym następujące zagadnienia:

TR 13335-1 terminologia i modele

TR 13335-2 metodyka planowania i prowadzenia analizy ryzyka, specyfikacja wymagań stanowisk pracy związanych z bezpieczeństwem systemów informatycznych

TR 13335-3 techniki zarządzania bezpieczeństwem:

- zarządzanie ochroną informacji
- zarządzanie konfiguracją systemów IT
- zarządzanie zmianami

TR 13335-4 metodyka doboru zabezpieczeń

WD 13335-5 zabezpieczanie połączeń z sieciami zewnętrznymi

Jednakże norm ISO dotyczących bezpieczeństwa jest wiele. Można tu wymienić chociażby bogaty podzbiór (wycinek listy do roku 1995):

- ISO 2382-8:1986 Information processing systems – Vocabulary – Part 08: Control, integrity and security

- ISO 6551:1982 Petroleum liquids and gases – Fidelity and security of dynamic measurement – Cabled transmission of electric and/or electronic pulsed data

- ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

- ISO/IEC 7816-4:1995 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange

- ISO/IEC 9796:1991 Information technology – Security techniques – Digital signature scheme giving message recovery

- ISO/IEC 9797:1994 Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

- ISO/IEC 9798-1:1991 Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model

- ISO/IEC 9798-2:1994 Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms

- ISO/IEC 9798-3:1993 Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm

- ISO/IEC 9798-4:1995 Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function

- ISO/IEC 10118-1:1994 Information technology – Security techniques – Hash-functions – Part 1: General

- ISO/IEC 10118-2:1994 Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm

- ISO/IEC 10164-7:1992 Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function

- ISO/IEC 10164-8:1993 Information technology – Open Systems Interconnection – Systems Management: Security audit trail function

- ISO/IEC DIS 10181-1 Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview

- ISO/IEC DIS 10181-2 Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework

- ISO/IEC DIS 10181-3 Information technology – Open Systems Interconnection – Security frameworks in open systems – Part 3: Access control

- ISO/IEC DIS 10181-4 Information technology – Open Systems Interconnection – Security frameworks in Open Systems – Part 4: Non-repudiation

- ISO/IEC DIS 10181-5 Information technology – Security frameworks in open systems – Part 5: Confidentiality

- ISO/IEC DIS 10181-6 Information technology – Security frameworks in open systems – Part 6: Integrity

- ISO/IEC DIS 10181-7 Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Security Audit Framework

- ISO/IEC 10736:1995 Information technology – Telecommunications and information exchange between systems – Transport layer security protocol

- ISO/IEC 10745:1995 Information technology – Open Systems Interconnection – Upper layers security model

- ISO 11166-1:1994 Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats

- ISO 11166-2:1994 Banking – Key management by means of asymmetric algorithms – Part 2: Approved algorithms using the RSA cryptosystem

- ISO 11442-1:1993 Technical product documentation – Handling of computer-based technical information – Part 1: Security requirements

- ISO/IEC 11577:1995 Information technology – Open Systems Interconnection – Network layer security protocol

- ISO/IEC DIS 11586-1 Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation

- ISO/IEC DIS 11586-2 Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) service specification

- ISO/IEC DIS 11586-3 Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) protocol specification

- ISO/IEC DIS 11586-4 Information technology – Open Systems Interconnection – Generic upper layers security: Protecting transfer syntax specification

- ISO/IEC DIS 11586-5 Information technology – Open Systems Interconnection – Generic Upper Layers Security: Security Exchange Service Element Protocol Implementation Conformance Statement (PICS)

- ISO/IEC DIS 11586-6 Information technology – Open Systems Interconnection – Generic Upper Layers Security: Protecting Transfer Syntax Implementation Conformance Statement (PICS)

- ISO/IEC DIS 11770-1 Information technology – Security techniques – Key management – Part 1: Framework

- ISO/IEC DIS 11770-2 Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques

- ISO/IEC DISP 12059-7 Information technology – International Standardized Profiles – OSI Management – Common information for management functions – Part 7: Security alarm reporting

- ISO/IEC DISP 12059-8 Information technology – International Standardized Profiles – OSI Management – Common information for management functions – Part 8: Security audit trail

- ISO/IEC DISP 12060-6 Information technology – International Standardized Profiles - OSI Management – Management functions – Part 6: Security management capabilities

- ISO/IEC DTR 13335-1 Information technology – Guidelines for the management of IT security – Part 1: Concepts and models for IT security

- ISO/IEC DTR 13335-2 Information technology – Guidelines for the management of IT security – Part 2: Planning and managing IT security (Future Technical Report)
- ISO/IEC DTR 13335-3 Information technology – Guidelines for the management of IT security – Part 3: Techniques for the management of IT security
- ISO/IEC TR 13594:1995 Information technology – Lower layers security
- ISO/IEC DIS 14980 Information technology – Code of practice for information security management

[1] Simson Garfinkel, "Practical Unix and Internet Security", II ed., O'Reilly, 2003