5. STANDARDY ORAZ NORMY POLSKIE I MIĘDZYNARODOWE W ZAKRESIE BEZPIECZEŃSTWA SI

5.1. Normy ISO

W 1987 roku Międzynarodowa Organizacja Normalizacyjna - ISO (*International Organization for Standardization*) i Międzynarodowa Komisja Elektrotechniczna - IEC (*International Electrotechnical Commission*), utworzyły **Połączony Komitet Techniczny Nr 1** - JTC 1 (*Joint Technical Committee 1*).

W JTC 1 problematyką bezpieczeństwa zajmują się trzy podkomitety:

- SC 27 - podkomitet ds. technik bezpieczeństwa systemów informatycznych,
- SC 6 - podkomitet ds. telekomunikacji i wymiany informacji między systemami,
- SC 17 - podkomitet ds. kart identyfikacyjnych i urządzeń pokrewnych.

Ponadto, ISO posiada odrębny komitet TC 68 ds. bankowości - bezpieczeństwa i innych usług finansowych.

Komitety ISO/IEC JTC 1 i ISO TC 68 opublikowały ponad 100 dokumentów (norm, raportów technicznych oraz szkiców) bezpośrednio związanych z bezpieczeństwem SI. Obejmują one m.in.: algorytmy kryptograficzne, protokoły kontroli dostępu, protokoły zarządzania kluczami kryptograficznymi oraz sprawy związane z zarządzaniem bezpieczeństwem.

5.2. Polskie Normy

Polski Komitet Normalizacyjny (PKN) utworzył **komisje** zajmujące się opracowywaniem polskich wersji standardów ISO i będące odpowiednikami wymienionych jednostek ISO/IEC i ISO:

- Normalizacyjna Komisja Problemowa Nr 182 ds. Zabezpieczenia Systemów i Ochrony Danych (odpowiednik ISO/IEC JTC 1 - SC 27),
- Normalizacyjna Komisja Problemowa Nr 171 ds. Sieci Komputerowych i Oprogramowania (odpowiednik ISO/IEC JTC 1 - SC 6),
- Normalizacyjna Komisja Problemowa Nr 172 ds. Kart Identyfikacyjnych (odpowiednik ISO/IEC JTC 1 - SC 17),
- Normalizacyjna Komisja Problemowa Nr 271 ds. Bankowości i Bankowych Usług Finansowych (odpowiednik ISO/IEC JTC 1 - TC 68).

5.2.1. Polska Norma PN-I-13335

W latach 1996-2001 komitet ISO/IEC opublikował raport techniczny ISO/IEC TR 13335 pt. *Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych* (ang. *Information technology - Guidelines for the management of IT Security*). Raport ten składa się z 5 części:

- *ISO/IEC 13335-1:1996 - Część 1: Pojęcia i modele bezpieczeństwa systemów informatycznych* (ang. *Concepts and models for IT Security*) ,
- *ISO/IEC 13335-1:1997 - Część 2: Zarządzanie i planowanie bezpieczeństwa systemów informatycznych* (ang. *Managing and planning IT Security*),
- *ISO/IEC 13335-1:1998 - Część 3: Techniki zarządzania bezpieczeństwem systemów informatycznych* (ang. *Techniques for the management of IT Security*),
- *ISO/IEC 13335-1:2000 - Część 4: Wybór zabezpieczeń* (ang. *Selection of safeguards*),

- *ISO/IEC 13335-1:2001 - Część 5: Zabezpieczenia dla połączeń zewnętrznych* (ang. *Safeguards for external connections*).

Cel raportu:

- zdefiniowanie i opisanie pojęć związanych z zarządzaniem bezpieczeństwem systemów informatycznych,
- zidentyfikowanie zależności między zarządzaniem bezpieczeństwem systemów informatycznych a ogólnym zarządzaniem systemami informatycznymi,
- zaprezentowanie modeli, które mogą być wykorzystane do opisu bezpieczeństwa systemów informatycznych,
- dostarczenie ogólnych wytycznych do zarządzania bezpieczeństwem systemów informatycznych.

Uwaga: Raport ISO/IEC TR 13335 dostarcza wytyczne (a nie gotowe rozwiązania) do zarządzania bezpieczeństwem systemów informatycznych, tak, aby osoby odpowiedzialne za bezpieczeństwo SI mogły **przystosować** zawarty w nim materiał do konkretnych potrzeb.

5.2.2. Polska Norma PN-ISO/IEC 17799 (ISO/IEC 27001 i ISO/IEC 27002)

Historia normy:

- 1995 r. - Brytyjski Instytut Normalizacyjny (*British Standard Institute*) opracował normę BS 7799 dotyczącą zarządzania bezpieczeństwem informacji w przedsiębiorstwie,
- 2000 r., - po uproszczonym procesie legalizacyjnym, norma BS 7799 został przyjęty przez ISO i IEC jako standard międzynarodowy - ISO/IEC 17799 *Code of practice for information security management*,

- 2003 r. - Polski Komitet Normalizacyjny przetłumaczył normę i przyjął za w pełni zgodną z oryginałem - PN-ISO/IEC 17799 *Praktyczne zasady zarządzania bezpieczeństwem informacji.*
- 2007 r. - na jej podstawie powstały normy ISO/IEC 27001 i ISO/IEC 27002.

Zawartość normy:

- zalecenia dotyczące zarządzania bezpieczeństwem informacji dla osób odpowiedzialnych za inicjowanie, wdrażanie i utrzymywanie bezpieczeństwa,
- wspólna podstawa (wytyczne) do rozwijania wewnętrznych standardów bezpieczeństwa oraz efektywnego i praktycznego zarządzania bezpieczeństwem,
- wytyczne do zapewnienia zaufania w kontaktach pomiędzy organizacjami.

Norma ta jest stosowana przez firmy, dla których informacja stanowi podstawowy produkt (np. banki, towarzystwa ubezpieczeniowe, sieci sklepów).

Obszary (zagadnienia) mające, wg normy, wpływ na bezpieczeństwo informacji:

- opracowanie polityki bezpieczeństwa,
- organizacja bezpieczeństwa,
- klasyfikacja i kontrola aktywów,
- bezpieczeństwo osobowe,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,
- kontrola dostępu do systemu,

- rozwój i utrzymywanie systemu,
- zarządzanie ciągłością działania,
- zgodność z przepisami prawa i specyfikacją techniczną.

Uwaga: Łącznie ISO/IEC 17799 określa ok. 130 szczegółowych wymagań związanych z szeroko rozumianym bezpieczeństwem informacji.
Nie oznacza to jednak, że dokument ten przedstawia jedyne i wyczerpujące rozwiązania, których zastosowanie zapewni pełne bezpieczeństwo systemów informatycznych i ich danych. Zalecenia normy pozostawiają duży stopień swobody co do ich szczegółowej realizacji.

W polskiej wersji norma zawiera także załącznik ze słownikiem terminów polskich i ich angielskich odpowiedników, które zostały zastosowane w tej normie, a nie były wcześniej uwzględnione w normie PN-I-02000:2002 *Technika informatyczna - Zabezpieczenia w systemach informatycznych - Terminologia*.

5.2.3. Polska Norma PN-I-02000

Polska Norma PN-I-02000 *Technika informatyczna - Zabezpieczenia w systemach informatycznych. Terminologia*:

- opublikowana w 1998 r., a następnie uzupełniona w 2002 r.,
- jest to norma terminologiczna z zakresu techniki informatycznej,
- stanowi pierwsze opracowanie zmierzające do unormowania terminologii polskiej dotyczącej zabezpieczenia systemów informatycznych i ochrony danych,

- pomimo występujących nieprecyzyjności i niezgodności pojęć, norma ta dużo wniosła do polskiego słownictwa z zakresu bezpieczeństwa - próba unormowania tej terminologii jest jej największą zaletą,
- autorzy normy deklarują dalsze prace nad jej udoskonalaniem,
- przeznaczenie: przy opracowywaniu polskich i międzynarodowych dokumentów (np. dokumentacji projektowej i eksploatacyjnej systemów, opisów zabezpieczeń, procedur awaryjnych, umów),
- zawiera ok. 800 terminów, pogrupowanych i dotyczących m.in. klasyfikacji zasobów, technik kryptograficznych, kontroli dostępu i monitorowania, naruszenia zabezpieczeń, ochrony danych, przestępstw komputerowych, audytu i oceny zabezpieczenia systemów.

5.3. Standard BSI „IT Baseline Protection Manual”

Metoda ochrony podstawowej BSI:

- opracowana w latach 90-tych przez niemiecką Agencję ds. Bezpieczeństwa Techniki Informatycznej - BSI (*Bundesamt für Sicherheit in der Informationstechnik*),
- opis metody to ok. 1,5 tysiąca stron tekstu (dostępny także w wersji elektronicznej) w postaci modułowej,
- wdrożona w wielu instytucjach przez czołowe niemieckie firmy doradcze,
- dokumenty opracowane przez BSI są często uznawane za wzorcowe w UE i zalecane do użycia,
- ma zastosowanie w SI o niższych i średnich wymaganiach bezpieczeństwa,
- jest ona elastyczna, praktyczna i gotowa do natychmiastowego wykorzystania,
- spotkała się ona z dużym uznaniem w środowiskach informatycznych - przyznawane są certyfikaty zabezpieczenia systemu metodą BSI

- traktowana jest często jako metoda konkurencyjna do dokumentów ISO/IEC,
- pozwala na obniżenie kosztów zarządzania bezpieczeństwem i skrócenie czasu wdrożenia systemu ochrony (analiza ryzyka jest stosowana wyłącznie tam, gdzie ma to uzasadnienie).

Zasada funkcjonowania metody BSI:

- zastąpienie czasochłonnej i kosztownej analizy ryzyka gotowymi propozycjami zabezpieczeń wypracowanymi przez specjalistów (dla obszarów wymagających lepszej ochrony zalecana jest analiza ryzyka),
- w oparciu o **katalog modułów wzorcowych** opracowanie modelu SI, tzn. ze zbioru gotowych, wzorcowych elementów wybiera się te, które występują w rzeczywistym systemie,
- w oparciu o **katalog zagrożeń** stwierdzenie, na jakie potencjalne zagrożenia jest podatny system oraz w jaki sposób należy go przed nimi chronić (na podstawie **katalogu zabezpieczeń**),

Program *IT Baseline Protection Tool* (GSTOOL):

wspomaga modelowanie systemu informatycznego, ocenę wymagań ochronnych, wybór zabezpieczeń, oszacowanie kosztów ochrony, wdrożenie zabezpieczeń, tworzenie raportów z prac wdrożeniowych oraz czynności audytorskie.

5.4. Standardy FIPS

Narodowy Instytut Standardów i Technologii - NIST (*National Institute of Standards and Technology*) w USA opracowuje standardy dla federalnych systemów informatycznych:

- standardy NIST określane są skrótem FIPS (*Federal Information Processing Standards*),
- zawierają wiele praktycznych rozwiązań z zakresu bezpieczeństwa, które wykorzystywane są na całym świecie (np. standard algorytmu szyfrującego DES, podpisu cyfrowego DSS, funkcji skrótu SHS),
- uznanie przez NIST jakiegoś rozwiązania za standard świadczy o jego dużym znaczeniu i przydatności dla bezpieczeństwa SI,
- znajomość dokumentów FIPS jest przydatna osobom, które chcą wykorzystać sprawdzone i zaakceptowane rozwiązania z zakresu bezpieczeństwa.

Tabela 5. Wybrane dokumenty FIPS z zakresu bezpieczeństwa systemów informatycznych

Numer FIPS	Rok wydania	Tytuł dokumentu FIPS
31	1974	Guidelines for Automatic Data Processing Physical Security and Risk Management
73	1980	Guidelines for Security of Computer Applications
81	1980	DES Modes of Operation
83	1980	Guideline on User Authentication Techniques for Computer Network Access Control
102	1983	Guidelines for Computer Security Certification and Accreditation
112	1985	Password Usage (part 1)
113	1985	Computer Data Authentication
181	1993	Automated Password Generator
185	1994	Escrowed Encryption Standard
191	1994	Guideline for The Analysis of Local Area Network Security
46-3	1999	Data Encryption Standard (DES) - specifies the use of Triple DES
186-2	2000	Digital Signature Standard (DSS)
197	2001	Advanced Encryption Standard
180-2	2002	Secure Hash Standard (SHS)
199	2004	Standards for Security Categorization of Federal Information and Information Systems
200	2006	Minimum Security Requirements for Federal Information and Information Systems
198-1	2008	The Keyed-Hash Message Authentication Code (HMAC)
201-2	2013	Personal Identity Verification (PIV) of Federal Employees and Contractors
186-4	2013	Digital Signature Standard (DSS)
202	2015	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
180-4	2015	Secure Hash Standard (SHS)

Źródło: opracowanie własne

5.5. Dokumenty RFC

Dokumenty RFC (*Requests for Comments*) opracowuje tzw. Sieciowa Grupa Robocza wyodrębniona w ramach Rady ds. Architektury Sieci Internet - IAB (*Internet Architecture Board*).

- Seria dokumentów RFC to ogromny zbiór (ponad 5 tysięcy), publikowanych od roku 1969, technicznych i organizacyjnych opracowań o Internecie (pierwotnie o sieci ARPANET).
- Dokumenty te zawierają zarówno treści informacyjne jak i przyjęte standardy.
- Dokumenty RFC są cennym źródłem informacji na temat technicznej strony funkcjonowania Internetu. Dzięki nim rozpowszechnionych zostało wiele rozwiązań podnoszących bezpieczeństwo Internetu.

Tabela 6. Wybrane dokumenty RFC - standardy internetowe

Mnemonik	Tytuł dokumentu RFC	Numer standardu	Numer RFC
	Internet Official Protocol Standards	1	3600
IP	Internet Protocol	5	791
UDP	User Datagram Protocol	6	768
TCP	Transmission Control Protocol	7	793
FTP	File Transfer Protocol	9	959
SMTP	Simple Mail Transfer Protocol	10	821
MAIL	Standard for the format of ARPA Internet text messages	11	822
PPP	The Point-to-Point Protocol (PPP)	51	1661

Źródło: opracowanie własne na podstawie [RFC www]

Tabela 7. Wybrane dokumenty RFC - szkice standardów internetowych

Mnemonik	Tytuł dokumentu RFC	Numer RFC
RMON-MIB	Remote Network Monitoring MIB Protocol Identifier Reference	2895
RADIUS	Remote Authentication Dial In User Service (RADIUS)	2865
--------	HTTP Authentication: Basic and Digest Access Authentication	2617
HTTP	Hypertext Transfer Protocol -- HTTP/1.1	2616
IPV6	Internet Protocol, Version 6 (IPv6) Specification	2460
DHCP	Dynamic Host Configuration Protocol	2131
PPP-CHAP	PPP Challenge Handshake Authentication Protocol (CHAP)	1994
CON-MD5	The Content-MD5 Header Field	1864
NICNAME	NICNAME/WHOIS	954
BOOTP	Bootstrap Protocol	951

Źródło: opracowanie własne na podstawie [RFC www]

Tabela 8. Wybrane dokumenty RFC - propozycje standardów internetowych

Tytuł dokumentu RFC	Numer RFC
Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols	7817
SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)	7672
HTTP Strict Transport Security (HSTS)	6797
Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)	5910
Generic Security Service API Version 2: Java Bindings Update	5653
Session Description Protocol (SDP) Security Descriptions for Media Streams	4568
A Pseudo-Random Function (PRF) API Extension for the Generic Security Service Application Program Interface (GSS-API)	4401
Security Architecture for the Internet Protocol	4301
DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format	3845
IP Security Policy (IPSP) Requirements	3586
Transport Layer Security (TLS) Extensions	3546
Authentication, Authorization and Accounting (AAA) Transport Profile	3539
Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security(TLS)	3268
Telnet Data Encryption Option	2946
Routing Policy System Security	2725
Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)	2712
Domain Name System Security Extensions	2535
The PPP Triple-DES Encryption Protocol (3DESE)	2420
Security Architecture for the Internet Protocol	2401
FTP Security Extensions	2228
MIME Security with Pretty Good Privacy (PGP)	2015
The PPP Encryption Control Protocol (ECP)	1968
IP Authentication using Keyed MD5	1828
The Kerberos Network Authentication Service (V5)	1510

Źródło: opracowanie na podstawie [RFC www]

5.6. Raporty CERT

CERT (*Computer Emergency Response Team*):

- powstał w 1988 roku jako niewielki zespół zajmujący się przypadkami naruszania bezpieczeństwa w ramach projektu DARPA.
- od kilku lat jest największą organizacją rejestrującą i reagującą na przypadki naruszania bezpieczeństwa w sieci Internet.
- składa się z licznych oddziałów na całym świecie.
- od 1997 roku CERT jest członkiem FIRST (*Forum of Incidents Response and Security Teams*).
- polski oddział CERT utworzony został w 1996 roku, od 2000 roku działa pod nazwą CERT NASK

Do głównych zadań CERT należy m.in.:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo (zgłoszenia przyjmowane są celem udzielenia pomocy i dla celów statystycznych),
- alarmowanie użytkowników o wystąpieniu bezpośredniego dla nich zagrożenia (w ramach obsługi zgłoszonych zdarzeń, CERT powiadamia użytkowników o grożących im niebezpieczeństwach),
- prowadzenie działań zmierzających do wzrostu świadomości na temat bezpieczeństwa teleinformatycznego (szkolenia, konferencje),
- prowadzenie badań i przygotowywanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu,
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa,
- przeprowadzanie audytów bezpieczeństwa.

Raporty i opracowania publikowane przez CERT:

- zasługują na szczególną uwagę ze strony osób odpowiedzialnych za bezpieczeństwo SI,
- przedstawiają aktualny obraz sytuacji w zakresie bezpieczeństwa (statystyki, opisy przypadków, wnioski, itd.) oraz zalecenia, których należy przestrzegać, aby nie dopuścić do wystąpienia przypadków naruszenia bezpieczeństwa systemu.

5.7. Pozostałe dokumenty

Inne organizacje, których publikacje (standardy, dokumenty) wpływają na poziom bezpieczeństwa wykorzystywanych w SI rozwiązań:

- Międzynarodowa Unia Telekomunikacyjna - ITU (*International Telecommunication Union*) - publikuje ona serię norm dotyczących sieci danych i komunikacji w systemach otwartych (*Series X: Data networks and open system communication*). Pośród publikowanych norm są też normy z zakresu bezpieczeństwa ustanowione razem z ISO/IEC.
- Amerykański Krajowy Instytut Standardów - ANSI (*American National Standards Institute*) jest prywatną instytucją reprezentującą blisko 1,5 tysiąca organizacji i agencji rządowych. Nie opracowuje standardów ale publikuje dokumenty, które są wynikiem porozumienia wśród określonych grup specjalistów z danej dziedziny.
- Instytut Inżynierów Elektryków i Elektroników - IEEE (*Institute of Electrical and Electronics Engineers*) opracowuje m.in. standardy z zakresu telekomunikacji i technologii informatycznych, które również dotyczą zagadnień z zakresu bezpieczeństwa systemów informatycznych.

6. ZAGROŻENIA BEZPIECZEŃSTWA SI

6.1. Klasyfikacja zagrożeń

Definicja: *zagrożenie, to potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji* [PN-I-13335-1].

Rodzaje klasyfikacji zagrożeń bezpieczeństwa SI ze względu na:

- **lokalizację źródła zagrożenia:** ***wewnętrzne*** (np. kradzież danych przez użytkownika systemu, awaria urządzenia, błąd oprogramowania), ***zewnętrzne*** (np. atak typu DoS, włamanie do pomieszczeń biura, brak zasilania w sieci energetycznej),
- **przypadkowość** (losowość): ***celowe*** (np. umyślne skasowanie danych, kradzież komputera, akt wandalizmu), ***przypadkowe / losowe*** (np. przypadkowe skasowanie plików, wyrzucenie wydruków do śmieci, wyłączenie komputera w czasie pracy, wichura, uderzenie pioruna, zalanie).
- **skutki** wywołane wystąpieniem zagrożenia: wywołujące utratę atrybutów bezpieczeństwa SI (utratę poufności, utratę integralności, utratę dostępności, utratę rozliczalności, utratę autentyczności, utratę niezawodności systemu).
- **pochodzenie (źródło)** - najbardziej przydatna klasyfikacja ze względu na późniejszy dobór zabezpieczeń.

Klasyfikacja zagrożeń ze względu na ich źródło:

- **działania ludzi:**
  - przypadkowe (błędy ludzi),
  - umyślne (ataki na bezpieczeństwo systemu),
- **awarie urządzeń i narzędzi informatycznych:**

  - sprzętu,
  - oprogramowania,
- **uchybienia i braki organizacyjne,**
- **siły wyższe i zdarzenia losowe.**

6.2. Zagrożenia spowodowane przez działania ludzi

Zagrożenia spowodowane przez ludzi:

- to największa grupa zagrożeń,
- ich charakter jest bardzo zróżnicowany,
- ich rodzaj uzależniony jest od pełnionych przez osoby funkcji, posiadanych umiejętności i ich intencji.

6.2.1. Działania przypadkowe

Zagrożenia wynikające z przypadkowych działań ludzi są najczęściej efektem ich niewiedzy, nieuwagi, bezmyślności, lenistwa lub zaniedbań.

Wśród przyczyn zagrożeń przypadkowych można wyróżnić:

- ludzkie błędy,
- zaniedbania lub zaniechania.

6.2.2. Działania umyślne (ataki na bezpieczeństwo systemu)

Powody ataków:

- wymierne korzyści (bezpośrednie lub pośrednie).
- powody emocjonalne (uzasadnione i nieuzasadnione): pragnienie zemsty, zazdrość, ciekawość, satysfakcja, chęć rozrywki, złośliwość, itp.

Sprawcy i powody ataków [Małachowski; Howard, Longstaff]**:**

- **nielojalni pracownicy** - różne powody ataku: zemsta, zazdrość, ciekawość, osiągnięcie korzyści, itd.,
- **nierzetelni dostawcy usług, sprzętu i oprogramowania** - powód: osiągnięcie bezpośrednich lub pośrednich korzyści,
- **profesjonalni przestępcy** - powód: osiągnięcie bezpośrednich lub pośrednich korzyści (najczęściej finansowych),
- **szpiedzy** - powód: zdobycie informacji na zlecenie, korzyści finansowe,
- **wandale i anarchiści** - powód: chęć uszkodzenia lub zniszczenia systemu informatycznego, rozgłos,
- **voyeurs** - powód: „emocje wywołane uzyskaniem niejawnych informacji”,
- **terroryści** - powód: wywołanie zagrożenia dla osiągnięcia celów lub korzyści politycznych,
- **hakerzy** - powód: chęć potwierdzenia umiejętności, rozgłos, uznanie,
- **pracownicy agencji rządowych i wywiadowczych** - powód: zdobycie informacji.

Klasyfikacja ataków [Kent 1977]:

- **aktywne** (przerwanie, modyfikacja, podrobienie),
- **pasywne** (przechwycenie).

Klasyfikacja ta zakłada, że funkcjonowanie systemu informatycznego polega na **przepływie** informacji od źródła do miejsca przeznaczenia, co pozwala wyróżnić następujące ataki:

- **przerwanie** (ang. *interruption*) - zniszczenie systemu (jego części) lub spowodowaniu jego niedostępności (niemożności użycia). Jest to atak na *dostępność* systemu (np. fizyczne uszkodzenie komputera, przecięcie kabli sieciowych, skasowanie plików).

- **modyfikacja** (ang. *modification*) - uzyskanie dostępu do zasobów systemu i wprowadzeniu w nich niedozwolonych zmian. Jest to atak na *integralność* (np. zmiana zawartości plików, modyfikacja komunikatów w sieci).
- **podrobienie** (ang. *fabrication*) - wprowadzanie do systemu fałszywych obiektów. Jest to atak na *autentyczność* (np. wysłanie fałszywych komunikatów, wygenerowanie fikcyjnych sprawozdań).
- **przechwycenie** (ang. *interception*) - dostęp niepowołanej osoby do zasobów systemu. Jest to atak na *poufność* (np. podsłuch w sieci, nielegalne kopiowanie plików).

Każdy z ww. rodzajów ataku jest, w mniejszym lub większym stopniu, naruszeniem *niezawodności* i *rozliczalności* systemu.

6.2.2.1. Ataki na bezpieczeństwo sieci komputerowej

Rodzaje ataków na bezpieczeństwo sieci komputerowych:

- **włamanie** (ang. *break-in*) - przejęcie oraz wykorzystanie konta i zasobów użytkownika systemu,
- **podsłuch sieciowy** (ang. *sniffing*) - przechwycenie informacji przesyłanych w sieci komputerowej (realizowane za pomocą urządzeń podsłuchowych lub komputerów wyposażonych w dedykowane oprogramowanie),
- **ataki DoS** (ang. *Denial of Service*) i **DDoS** (ang. *Distributed Denial of Service*) - zablokowanie określonych usług serwera (np. www, ftp) poprzez inicjowanie dużej liczby połączeń sieciowych tak, aby komunikacja nie została nawiązana, a serwer przebywał w stanie ciągłego oczekiwania na otwarcie połączeń,
- **podszywanie się** (ang. *spoofing*) - przesłanie pakietów zawierających sfałszowany adres źródłowy, dzięki czemu komputer, który je odbiera, błędnie identyfikuje nadawcę,

- **złośliwe użytkowanie** (ang. *malicious use*) - wykorzystanie zasobów lub usług systemu niezgodnie z ich przeznaczeniem,
- **wykorzystanie furtek** (ang. *backdoors*) - czyli nieudokumentowanych, zostawionych przez ich twórców, wejść do systemu,
- **wykorzystanie *exploit'ów*** - uruchomienie programów generujących błędy w systemie operacyjnym i pozwalających na uzyskanie przez atakującego większych uprawnień,
- **przeciek** (ang. *leakage*) - nieautoryzowane wydobycie informacji z systemu,
- **penetracja** (ang. *penetration*) i skanowanie sieci (ang. *network scanning*) - nieupoważnione rozpoznawanie zabezpieczeń systemu (np. celem znalezienia jego słabych punktów)
- **zmiana strony www** (ang. *website changing*) - podmiana lub zmodyfikowanie zawartości strony internetowej,
- **atak pocztowy** (ang. *mail bombing*) - wysłanie dużej liczby listów na konto pocztowe w celu jego zablokowania.

6.2.2.2. Wirusy komputerowe

Definicja: Wirus komputerowy to program (zestaw instrukcji procesora lub zestaw poleceń języków skryptowych), który wykonuje określone działania - najczęściej destrukcyjne - wbrew woli użytkownika systemu.

Obecnie termin *wirus komputerowy* obejmuje kilka grup programów:

- **wirusy** (ang. *viruses*) - programy, których kod powiela sam siebie i dołącza do innych programów. Oprócz rozprzestrzeniania się wykonują one zazwyczaj niepożądane czynności,

- **konie trojańskie** (ang. *trojan horses*) - procedury ukryte w na pozór pożytecznych programach, które sprawiają, że programy te, oprócz „oficjalnych" zadań, wykonują także bez wiedzy użytkownika niepożądane czynności (np. przechwytują hasła dostępu),
- **bomby logiczne** (ang. *logical bombs*) - wirusy, które pozostają w stanie bezczynności, dopóki nie zostaną spełnione określone warunki (np. nadejście określonej daty lub wykonanie danej czynności),
- **bakterie** (ang. *bacterias*) - wirusy, które do swojego funkcjonowania nie potrzebują programu nosiciela. Powielają się samoistnie w sposób ciągły, powodując wyczerpanie zasobów systemu. Są zdolne w krótkim czasie sparaliżować nawet dużą sieć komputerową.
- **robaki** (ang. *worms*) - wirusy, które rozsyłają swoje kopie między komputerami za pośrednictwem połączeń sieciowych (*internet worms* - rozsyłanie kopii przez internet).

Historia: Pierwszy i zarazem najsłynniejszy robak, napisany został przez Roberta Morrisa, zaraził w listopadzie 1988 roku około 6 tys. komputerów (10% ich ogólnej liczby). Wykorzystując różne techniki przenoszenia się, robak rozprzestrzeniał się w systemach Unix i po dwóch dniach był obecny w komputerach setek uniwersytetów, jednostek wojskowych i medycznych. Doprowadziło to do wyłączenia wielu ważnych komputerów. Za ten czyn Morris został aresztowany i skazany na trzy lata w zawieszeniu oraz grzywnę w wysokości ponad 10 tys. dolarów.

Klasyfikacje wirusów:

Ze względu na **sposób przenoszenia się** można wyróżnić wirusy rozprzestrzeniające się za pomocą:

- **nośników użytych do uruchomienia systemu** (np. dyskietek, dysków CD),
- **plików wykonywalnych**,
- **sieci komputerowej** (w szczególności poczty elektronicznej).

Ze względu na **działania podejmowane po infekcji:**

- **wirusy bez procedur destrukcyjnych** (np. wyświetlające tylko komunikaty),
- **wirusy z wybiórczymi procedurami destrukcyjnymi** (np. niszczące dokumenty edytora MS Word),
- **wirusy z wieloma procedurami destrukcyjnymi**, próbujące zniszczyć cały system komputerowy (np. niszczące system plików, kasujące zawartość BIOS'u).

Ze względu na **obiekty zarażane przez wirusy**:

- **wirusy plikowe** - jest to najstarsza grupa wirusów. Początkowo na ich atak narażone były tylko pliki wykonywalne (*.exe, *.com) oraz wsadowe (*.bat). Obecnie zarażane mogą być także pliki zawierające fragmenty kodu, biblioteki, sterowniki urządzeń (*.bin, *.dll, *.drv, *.lib, *.obj, *.ovl, *.sys, *.vxd).
- **wirusy sektorów startowych dysku** - wirusy zarażające sektory startowe dysku (Master Boot Record lub Boot Record) są szczególnie groźne, ze względu na duże znaczenie atakowanych przez nie obiektów i uruchamianie przez nich procedur, jeszcze nim oprogramowanie antywirusowe zacznie działać.
- **makrowirusy** - są to wirusy, które istnieją dzięki wprowadzeniu do pakietów biurowych (np. MS Office) języków programowania pozwalających na tworzenie makropoleceń (np. Visual Basic for

Applications). Uaktywnienie makrowirusa następuje w chwili otwarcia zainfekowanego dokumentu.

Ze względu na **sposób ukrywania swojej obecności**:

- **wirusy bez mechanizmów ukrywania swojej obecności** - są to wirusy, których kod pozostaje taki sam przez cały czas ich działania. Ułatwia to ich wykrycie i usunięcie, ponieważ możliwe jest wyodrębnienie charakterystycznego wzorca - tzw. *sygnatury wirusa*, po którym wirus może zostać zidentyfikowany.
- **wirusy polimorficzne** - są to wirusy samoczynnie zmieniające swój kod przy każdej infekcji; dzięki temu nie można wyodrębnić ich sygnatury.
- **wirusy *stealth*** - są to wirusy, które podczas sprawdzania programem antywirusowym tymczasowo przywracają zmienione przez siebie dane, aby ukryć swoją obecność.

6.2.2.3. Kradzież

6.2.2.3.1. Kradzież informacji

Uwaga: Kradzież informacji jest bardzo niebezpieczna ze względu na możliwość skopiowania danych elektronicznych bez pozostawiania jakichkolwiek śladów.
W przypadku kiedy czynu tego dokonuje osoba mająca bezpośredni dostęp do informacji - praktycznie oznacza to brak możliwości wykrycia kradzieży.

Odbiorcy informacji uzyskanej podczas kradzieży:

- konkurencja,
- media,
- agencje rządowe (prokuratura, policja),

- właściciel informacji (w przypadku prób szantażu).

6.2.2.3.2. Kradzież mocy obliczeniowej i usług

Kradzież mocy obliczeniowej to wykorzystywanie komputerów do wykonywania określonych zadań, bez zgody ich właściciela.

Historia: Termin „kradzież mocy obliczeniowej" powstał w latach 70., kiedy jedynymi wydajnymi komputerami były superkomputery znajdując się w centrach obliczeniowych, a ich moc była droga i trudno dostępna.

Kradzieży usług - to także kradzież mocy obliczeniowej - ale postrzegana jako wykorzystywanie systemu informatycznego do celów prywatnych lub nie związanych z jego przeznaczeniem.

Kradzieży usług dopuszczają się najczęściej *legalni* użytkownicy systemu. Ich działania obniżają wydajność SI i zmniejszają dostępność jego zasobów, np.:

- odwiedzanie stron www nie mających związku z obowiązkami służbowymi,
- wykorzystywanie poczty elektronicznej do prywatnej korespondencji,
- korzystanie z gier komputerowych,
- instalowanie i wykorzystywanie oprogramowania do celów prywatnych.

Uwaga: Odrębną kwestią - związaną z efektywnością pracownika - jest wykonywanie powyższych działań w godzinach pracy.

6.2.2.3.3. Kradzież urządzeń i oprogramowania

- Miniaturyzacja i popularność urządzeń komputerowych sprzyja ich kradzieży.

- Kradzież zagraża *dostępności* i *poufności* systemu.
- Dużym problemem dla firm programistycznych jest kradzież oprogramowania i kodu źródłowego - często oznacza ona ujawnienie tajemnic związanych ze skradzionym produktem.

6.2.2.4. Sabotaż i wandalizm

Sabotaż systemu informatycznego to zamierzone niszczenie lub uszkadzanie zasobów mające na celu spowodowanie jego dysfunkcji.

Wandalizm to rozmyślne niszczenie zasobów systemu bez konkretnego powodu.

SI jest szczególnie narażony na akty sabotażu i wandalizmu polegające na:

- uszkadzaniu i niszczeniu urządzeń komputerowych,
- uszkadzaniu i niszczeniu oprogramowania,
- uszkadzaniu (modyfikacji) i niszczeniu (kasowaniu) danych.

6.2.2.5. Inżynieria społeczna

Inżynieria społeczna (socjotechnika, ang. *social engineering*) polega na osiągnięciu zamierzonego celu przy pomocy odpowiednich metod perswazji i podstępu.

Atakujący stara się nakłonić atakowaną osobę do bezpośredniego ujawnienia mu informacji (np. hasła) lub do podjęcia działań, które umożliwią ich uzyskanie (np. przesłanie pliku z danymi).

Uwaga: Socjotechnika wykorzystuje zarówno *negatywne*, jak i *pozytywne* cechy człowieka (np. naiwność, łatwowierność, niewiedzę, podatność na zastraszenie, pychę uprzejmość, współczucie, podziw).

Działania socjotechniczne rozpoczynają się zazwyczaj od *przekonania* osoby atakowanej do fikcyjnej tożsamości atakującego (np. podanie się za administratora systemu, serwisanta, pracownika innego działu, kontrahenta, klienta) - w tym celu przedstawiane są jej pewne fakty.

Uwaga: Do inżynierii społecznej zalicza się także:

- uzyskiwanie informacji „z biurka”,
- przeglądanie wyrzucanych śmieci.

Zapobieganie socjotechnice polega przede wszystkim na *uświadamianiu* użytkowników.

Historia: Kevin Mitnick (pseudonim Condor) to obecnie najsłynniejszy na świecie haker. Wsławił się m.in. opracowaniem metody uzyskiwania bezpłatnych połączeń telefonicznych, włamaniami do sieci komputerowych wielu firm i organizacji (w tym NASA) oraz przechwyceniem 20 000 numerów kart kredytowych. Przez wiele lat poszukiwany przez FBI, został aresztowany w lutym 1995 roku i skazany na 46 miesięcy pozbawienia wolności i ponad 4 tys. dolarów grzywny.

6.3. Awarie urządzeń, programów i infrastruktury

6.3.1. Awarie urządzeń

Obecnie:

- urządzenia komputerowe wymagają mniej czynności serwisowych,
- niskie ceny urządzeń pozwalają rozbudowywać system i zwiększyć jego niezawodność.

Awarie urządzeń komputerowych polegają na ich *mechanicznym*, *termicznym*, *elektronicznym* lub *chemicznym* uszkodzeniu i wynikają zazwyczaj z:

- niskiej jakości podzespołów,
- niewłaściwej lub niezgodnej z przeznaczeniem obsługi,
- złego projektu technicznego systemu lub złego doboru komponentów,
- niesprawności dodatkowych urządzeń mających zapewniać właściwą pracę systemu (zasilanie, klimatyzacja, filtry przeciwzakłóceniowe, itp.),
- zdarzeń losowych (np. skoki napięcia, zalanie, uderzenie pioruna, itp.).

Uniknięcie awarii nie jest możliwe, ale można je minimalizować poprzez:

- odpowiedni dobór urządzeń,
- prawidłową obsługę i serwisowanie urządzeń,
- zwielokrotnienie urządzeń.

6.3.2. Awarie oprogramowania

Awarie oprogramowania to efekt:

- błędów popełnianych podczas jego projektowania, tworzenia lub modyfikowania,

- błędów wynikających z niezgodności z innymi programami (np. systemem operacyjnym).

Uwaga: Cechą oprogramowania przekładającą się bezpośrednio na występujące w nim awarie jest jego *jakość*.

Wpływ na awaryjność oprogramowania ma m.in.:

- złożoność oprogramowania - to skutek konieczności spełnienia wielu oczekiwań użytkowników (np. wygodnej obsługi, funkcjonalności),
- wymaganie zgodności wstecznej,
- ewolucja oprogramowania - to skutek konieczności spełnienia oczekiwań użytkowników i konieczność sprostania konkurencji,
- pośpiech przy tworzeniu oprogramowania,
- niewystarczające testowanie oprogramowania.

Historia: Przykładem błędu w oprogramowaniu, który pojawił się po wielu latach, jest tzw. *problem Y2K*, czyli *problem roku dwutysięcznego* - chęć zaoszczędzenia przez programistów kilku bajtów na zapisie daty kosztowała miliony dolarów, które za jego usunięcie musiały zapłacić przedsiębiorstwa, organizacje i rządy wielu krajów.

6.3.3. Awarie infrastruktury

Obecnie:

- uzależnienie przedsiębiorstw od infrastruktury stale rośnie,
- przerwy w dostawach usług infrastruktury są często jednoznaczne z przerwami w funkcjonowaniu SI,

- dużym problemem dla przedsiębiorstw jest fakt, że kontrola nad infrastrukturą znajduje się poza nimi.

6.4. Braki i uchybienia organizacyjne

Uwaga: Sytuacja, w której przedsiębiorstwo nie posiada określonych rozwiązań organizacyjnych (strategii rozwoju, polityk, reguł i zasad postępowania) stanowi zagrożenie nie tylko dla jego SI, ale dla całego przedsiębiorstwa.

W zakresie bezpieczeństwa SI groźna jest błędnie opracowana polityka bezpieczeństwa (lub jej całkowity brak), a przede wszystkim nieprzypisanie użytkownikom zakresu:

- obowiązków,
- uprawnień,
- odpowiedzialności.

6.5. Siły wyższe i zdarzenia losowe

Uwaga: Na działanie sił wyższych i zdarzeń losowych narażony jest każdy system informatyczny.

Siły wyższe - to zdarzenia, których wystąpieniu nie można zapobiec nawet przy dołożeniu największych starań. Najczęściej są to *naturalne katastrofy* - czyli skutki działania sił przyrody (np. powódź, wyładowania atmosferyczne, wichura, trzęsienie ziemi).

Zdarzenia losowe - to przypadkowe sytuacje, którym można było zapobiec, ale których wystąpienia w danym momencie nie można było przewidzieć.

Pochodzą one zazwyczaj z bezpośredniego otoczenia systemu (np. pożar, zalanie, zmiany napięcia prądu, katastrofy budowlane).

Uwaga: do zdarzeń losowych zaliczyć należy także nieprzewidzianą nieobecność lub utratę personelu (np. z powodu choroby, wypadku, śmierci, strajku, urlopu).

Siłom wyższym nie można zapobiec, a zdarzenia losowe trudno jest przewiedzieć - w praktyce jedynym sposobem jest *minimalizowanie skutków ich wystąpienia* (np. poprzez posiadanie kopii zapasowych, nadmiarowych urządzeń, procedur postępowania w sytuacjach zagrożenia).