Bezpieczna poczta elektroniczna

- **Bezpieczeństwo wewnętrzne**
  - **Poufność korespondencji**
  - **Spójność korespondencji**
  - **Dostępność przesyłki i systemu pocztowego**
  - **Niezaprzeczalność autorstwa**
- **Bezpieczeństwo zewnętrzne**

Zagrożenia dla bezpieczeństwa systemu przekazywania poczty elektronicznej

☞ ***Zagrożenia celujące w poufność korespondencji:***

- **Podsłuch w sieci**
- **Podgląd korespondencji podczas jej obsługi przez system pocztowy**
- **Podgląd informacji w skrzynce pocztowej odbiorcy**
- **Możliwość ujawnienia informacji podczas działania klientów pocztowych**
- **Atak kryptoanalityczny na zawartość przesyłki**

☞ ***Zagrożenia celujące w spójność przesyłki***

- **Robaki internetowe oraz wirusy rozpowszechniane poprzez pocztę elektroniczną**
- **Modyfikacja korespondencji poprzez zmianę treści wiadomości na jednym z serwerów**
- **Darmowe serwisy obsługujące pocztę elektroniczną**

Zagrożenia dla bezpieczeństwa systemu przekazywania poczty elektronicznej

☞ ***Zagrożenia umożliwiające manipulację autorstwem przesyłki***

- **Brak wymagania autoryzacji użytkownika podczas wysyłania korespondencji**
  - **Rozsyłanie tzw. *spamu***
  - **Wysyłanie tzw. bomb pocztowych**
  - **Zapisywanie ofiary do wielu list dyskusyjnych**

- **Ataki na narzędzia kryptograficzne do tworzenia podpisów cyfrowych**
- **Fałszowanie poczty przy użyciu błędów w programach pocztowych**

☞ ***Zagrożenia dla dostępności przesyłki lub systemu pocztowego***

- **Brak systemu podtrzymywania napięcia**
- **Ataki typu „odmowa usługi”**
- **Spowolnienie działania systemu w skutek zbytniego obciążenia zasobów**
- **Przerwy w działaniu systemu operacyjnego**

Zagrożenia dla bezpieczeństwa na zewnątrz

- **Ataki aktywną zawartością (*active content attacks*)**
- **Ataki przepełnienia buforu (*buffer overflow attacks*)**
- **Konie trojańskie (*Trojan horse attacks*)**
- **Ataki z wykorzystaniem skryptów powłoki (*shell script attacks*)**
- **Ataki w oparciu o błąd sieci (*web bug privacy attack*)**

Inne zagrożenia

- **Ataki z wykorzystaniem luk w agentach przesyłania poczty**
- **Podawanie się za przełożonego lub administratora**
- **Atak na prywatność adresu pocztowego użytkowników**

Zagrożenia związane z protokołem SMTP

- **Brak szyfrowania**
- **Brak autoryzacji nadawcy przy wysyłaniu**
- **Brak kontroli spójności przesyłki na poziomie transportowym**
- **Polecenia RCPT, VRFY, EXPN, HELP**

Zagrożenia związane z protokołem POP3

Zagrożenia związanie z protokołem IMAP4

Pretty Good Privacy (PGP)

- **poufność**
- **uwierzytelnienie źródła**
- **integralność (spójność) wiadomości**
- **niezaprzeczalność nadania**
- **zarządzanie kluczami**

- **IDEA – szyfrowanie danych**
- **RSA – zarządzanie kluczami**
- **MD5 i RSA – spójność i podpisy cyfrowe**

- **Opcjonalny podpis cyfrowy**
- **Kompresja**
- **Opcjonalne szyfrowanie**
- **Opcjonalne kodowanie do transmisji**

Privacy Enhanced Mail (PEM)

- **poufność**
- **uwierzytelnienie źródła**
- **integralność (spójność) wiadomości**
- **niezaprzeczalność nadania**
- **mechanizm zarządzania kluczami**

- **RFC 1421**
- **RFC 1422**
- **RFC 1423**
- **RFC 1424**

Typy wiadomości:
- **MIC-CLEAR**
- **MIC-ONLY**
- **ENCRYPTED**

- **Standaryzacja (kanonizacja)**
- **Zapewnienie integralności i wstawienie podpisu**
- **Opcjonalne szyfrowanie**.
- **Opcjonalne kodowanie do transmisji**

Ochrona przed utratą poufności przesyłki

- **Bezpieczna topologia**
- **Szyfrowanie**
- **Produkty wykrywające programy podsłuchujące**

Zapewnianie spójności przesyłki

- ***md5sum, sum* - oprogramowanie umożliwiające generowanie i sprawdzanie sum kontrolnych**
- ***ccrypt* i inne programy szyfrujące**
- **Stosowanie oprogramowania antywirusowego**
- **Wiązanie stałe adresów MAC**

Ochrona przed niechcianą pocztą

- ***Procmail***
- **Restrykcje w przekazywaniu poczty**
- **Bazy RBL**
- **Programy *Advanced E-mail Protector, Spam Exterminator, EmC* itp.**
- ***Mailfilter***
- ***Sam Spade***
- ***BombSquad, MailDeleter***

Ochrona przed atakami zagrażającymi dostępności systemu pocztowego

Ochrona przed atakami wyprowadzanymi poprzez system pocztowy

- **Oprogramowanie antywirusowe**
- ***Procmail sanitizer***
- **Uaktualnianie oprogramowania i staranna konfiguracja**
- **Niestandardowe oprogramowanie i niestandardowe instalacje**

BIBLIOGRAFIA

[1] **Allman E. Costales B.:** ***Sendmail. Wydawnictwo HELION*****. Gliwice 2001.**

[2] **Comer D. E.:** ***Sieci komputerowe TCP/IP*****. Tomy 1-3. WNT. Warszawa 1997.**

[3] **Frisch A.:** ***UNIX – Administracja systemu. Wydawnictwo RM*****. Warszawa 1997.**

[4] **Garfinkel S. Spafford G.:** ***Bezpieczeństwo w Unixie i Internecie*****. Wydawnictwo RM. Warszawa 1997.**

[5] **Hawker M. i inni :** ***The Three Steps to Super.Human.Software: Compare, Coexist, Migrate From Microsoft Exchange to Lotus Domino Part One: Comparison*****. IBM. 1999.**

[6] **Hunt C.:** ***TCP/IP Administracja sieci*****. Oficyna wydawnicza Read Me. Warszawa 1996.**

[7] **Schneier B.:.** ***Applied Cryptography: Protocols, Algorithms and Source Code in C*****, John Wiley & Sons, Inc., 1994**

[8] **Schneier B.:** ***Ochrona poczty elektronicznej*****. WNT. Warszawa 1996.**

[9] **Scrambray J., McClure S., Kurtz G.:** ***Hakerzy – cała prawda*** **Wydawnictwo Translator. Warszawa 2001.**

[10] **Powell K. I inni :** ***Implementacja i Obsługa Exchange Server 5.5*****. Wydawnictwo Robomatic. Wrocław 1998.**

[11] **Praca zbiorowa:** ***Internet, Agresja i Ochrona*****. Wydawnictwo Robomatic. Wrocław 1998.**

[12] **Praca zbiorowa:** ***Linux, Agresja i Ochrona*****. Wydawnictwo Robomatic. Wrocław 2000.**

[13] **Praca zbiorowa: Lotus Domino –** ***The Power to Connect People – Easily, Securely, Reliably. Administering the Domino System Vol 1*****. Cambridge, USA. 1999.**

[14] **RFC 821. Postel J.:** ***Simple Mail Transfer Protocol*****.. 01/08/1982**

[15] **RFC 1939. Myers J., Rose M.:** ***Post Office Protocol - Version 3*****. 1996.**

[16] **RFC 2060. Crispin M.*****: Internet Message Access Protocol - Version 4rev1*****. 1996.**

[17] **RFC 2821. Klensin, J. Ed.:** ***Simple Mail Transfer Protocol*****. 2001.**