Biztonságos levelezés

Számítástechnika tanár szak
Rendszertechnika II.
előadás

Az e-mail szerepének változása

- Az e-mail használat változásaival kapcsolatban a **Symantec** végzett átfogó kutatást
- Kérdések:
  - A folyamatosan növekvő e-mail használat miértje és következménye
  - A növekvő e-mail használat hatásának vizsgálata az üzleti életre
  - A felhasználók e-mail függőségének elemzése
  - Az e-mailekben tárolt adatok fontossága, értéke
- A kutatásról:
  - Független kutatás az 500 főnél többet foglalkoztatók körében
  - 1700 alkalmazottal és IT menedzserrel folytatott interjú
  - 17 európai országban

A kutatás eredményének gyors áttekintése

- Manapság az alkalmazottak munkaidejük egyre nagyobb részét töltik e-mailezéssel
- Egyre több embernél alakul ki függőség
- Az e-mailek száma jelentősen növekszik
  - az e-mailekre utaltság miatt
  - spam és egyéb levelek
- Terjed az e-mailezés mobil eszközökön is, ami oda vezet, hogy a felhasználók mindig és mindenhol ellenőrzik leveleiket

A függőség

- Az alkalmazottak 75%-a szerint könnyű rászokni az e-mail használatára
- 21% már folyamatosan kényszert érez az e-mailek ellenőrzésére
- Az e-mailezők típusai
  - Túlterhelt (6%)
  - Függő (21%)
  - Elutasító (10%)
  - Tudatos (49%)

Üzleti hatás

- Az IT menedzserek 91%-a szerint átlagosan 47%-al nőtt az e-mailek mennyisége az elmúlt években
- A felhasználók több mint fele (52%) napi 2 órát tölt levelezéssel (hetente 1 munkanap)
- 15% napi 4 órát fordít a levelezésre
- Legfontosabb felhasználási területek:
  - Tárgyalás paramétereinek ellenőrzése (74%)
  - Dokumentumok keresése (74%)
  - Kontakt adatok keresése (62%)
  - Személyes jellegű kommunikáció (60%)

A mobil e-mailezők

- A megkérdezett személyek 31%-a vallotta magát mobil e-mailezőnek
- 27%-uk szerint ez rossz hatással van a munka/magánélet egyensúlyára, növeli a stresszt
- A mobil e-mailezők harmada ellenőrzi leveleit közvetlenül lefekvés előtt és ébredés után
- A mobil e-mailezők többsége a mobileszközt munkahelyi ügyek intézésére használja még baráti, családi társaságban is
  - szabadság alatt 40% lép be a levelező rendszerbe
  - betegség esetén 38% ellenőrzi a leveleit
  - a gyerek születésnapján is van 5% aki ezzel foglalkozik

Az e-mailek biztonsága

- A vállalatoknak csak 23%-a rendelkezik valamiféle irányelvvel az e-mailek tárolásáról
- A dolgozók nem tudják, hogy melyik levelet kell tárolni és melyiket törölhetik
- Biztonsági másolat
  - az alkalmazottak 50%-a úgy gondolja, hogy az ő feladata a biztonsági másolat készítése
  - 47% úgy gondolja, hogy ez az IT részleg dolga
  - 64% abban a tudatban van, hogy az IT részleg minden fogadott és küldött e-mailről másolatot készít
  - 80% úgy tudja (tévesen), hogy a cég a törölt levelekről is őriz másolatot
  - A vállalatoknak csak 44%-a készít automatikus mentést a felhasználó merevlemezére mentett e-mailekről

A tárolt információ értéke

- A mobil eszközön is e-mailezők 78%-a nyilatkozott úgy, hogy az e-mailekben (és a notebookon) tárolt adatok jelentő értéket képviselnek
  - Átlagos érték 200 millió forint …
  - Legnagyobb érték a kutatás során: 1,5 milliárd forint
- Megállapítható, hogy ezek az adatok jelentős értéket képviselnek
- A cégeknek így az adatok védelmére is célszerű lenne áldozni a hardware vásárlás mellett
- Jelenleg kevés vállalat van felkészülve az ellopott, megsemmisült adatok visszanyerésére

Megoldás az e-mailek biztonságos tárolására

- Központilag minden beérkező és elküldött e-mailről egy másolat tárolása
  - Beérkezett üzeneteknél egy másolat marad a kiszolgálón
  - Elküldött leveleknél nehezebb a helyzet, más (külső) kiszolgálók is használhatók a küldéshez
- Központi szabályzatok kidolgozása és következetes alkalmazása
- Felhasználók képzése, oktatása

E-mailek biztonsági problémái

- Minden e-mail a feladótól a címzettig számos gépen halad keresztül
- A célba ért levelek is könnyen elolvashatók (megfelelő jogosultságok birtokában)
- Sem a feladó, sem a címzett nem veszi észre ha más is olvasta az e-mailt
- A hagyományos POP vagy IMAP kapcsolatok esetén az üzenetet kívülállók is elfoghatják
- A különböző szegmensek biztonságosabbá tétele:
  - A küldőtől a címzettig: üzenetek titkosítása, aláírása
  - A levelezőszerver és a levelezőkliens között: biztonságos IMAP vagy biztonságos POP használatával, alagútazás segítségével

Leggyakoribb visszaélések

- E-mailben küldött információk lehallgatása
- Levélbombák (postafiók megtöltése, levelezőrendszer összeomlása)
- Megszemélyesítés a levél feladójának megváltoztatásával
- Vírusok terjesztése
- Lánclevelek "hoax"-ok indítása
- A levelezőszerver kontrolljának megszerzése egyéb támadások indításához

Levelek titkosítása - Pine

- Megoldás: a PinePGP használata
- A PinePGP telepítése:
  - Pine normál futtatása (~/.pinerc állomány létrhozása)
  - PinePGP letöltése és telepítése
    - pinegpg-install
      (csak a címzett tudja visszafejteni az üzenetet)
    - pinegpg-install c-ta@ttk.pte.hu
      (megadott e-mail cím (feladó) is vissza tudja fejteni)
- A pine a leveleket a ~/.pinerc állomány sending-filters és display-filters változóival szűri

Üzenetek kezelése PinePGP-vel

- Üzenet küldése
  - Küldéskor (CTRL-x) a pine megkérdezi, hogy milyen szűrőt használjon
    - send message (filtered thru "gpg-sign")?
    - send message (filtered thru "gpg-encrypt")?
    - send message (filtered thru "gpg-sign+encrypt")?
  - Aláírásnál meg kell adni a használt kulcs jelszavát
- Üzenetek olvasása
  - Titkosított üzenetnél a pine bekéri jelszavunkat és ha ez helyes akkor megjeleníti az üzenetet
  - Az üzenet elején és végén a [PinePGP] jelölés található

Levelek titkosítása - Mozilla

- Enigmail (enigmail.mozdev.org) használata
- Üzenet küldése
  - Levél írása hagyományos módon
  - Rendelkeznünk kell a címzett nyilvános kulcsával
  - Küldés (Send) helyett az Enigmail opciót használjuk
    - titkosítás, aláírás, titkosítás+aláírás
- Üzenetek olvasása
  - Titkosított levél megnyitásakor a Mozilla bekéri a kulcshoz tartozó jelszavunkat

Biztonságos SSL kapcsolatok

- A legtöbb levelezőkliens támogatja
- A legtöbb kereskedelmi levelezőszerver viszont nem
- Az SSL támogatás módja a levelező szerverekben
  - Az SSL élesítése a kapcsolat felépítése után
    - IMAP: a szerver a normál 143-as portot figyeli, az SSL élesítése a STARTTLS paranccsal történik
    - POP: a szerver a normál 110-es portot figyeli, az SSL élesítése a STLS paranccsal történik
  - SSL port használata
    - IMAP: 993-as port, SSL egyeztetés a kapcsolat felvétele előtt
    - POP: 995-ös port, SSL egyeztetés a kapcsolat felvétele előtt

POP/IMAP levelezőszerver + SSL

- Legfőbb cél a jelszavaink védelme
- Az adatfolyam (e-mail tartalmának) védelmével nem itt kell foglalkozni
  - Az üzenet tartalma korábbi fázisokban könnyebben megszerezhető
- Az imapd program használata SSL protokollal
- Kliens beállítása SSL protokoll használatára
  - Ha a kliens támogatja a STARTTLS megoldást, akkor nincs több tennivalónk, készen is vagyunk
  - Ha nem, a szerveren önálló portokat kell beállítani

POP/IMAP levelezőszerver + SSL

- Önálló portok élesítése az SSL kapcsolathoz
  - IMAP használatánál
    - service imaps { … disabled = no } (xinetd)
    - imaps stream tcp nowait root /usr/sbin/tcpd imapd (inetd)
    - xinetd vagy inetd konfiguráció újraolvasása Önálló portok élesítése az SSL kapcsolathoz
  - POP használatánál
    - service pop3s { … disabled = no } (xinetd)
    - pop3s stream tcp nowait root /usr/sbin/tcpd ipop3d (inetd)
    - xinetd vagy inetd konfiguráció újraolvasása

POP/IMAP levelezőszerver + SSL

- Tesztelés
  - `openssl s_client -quiet -connect localhost:993`
    - kilépés: `0 LOGOUT`
  - `openssl s_client -quiet -connect localhost:995`
    - kilépés: `QUIT`
- Egy lehetséges kimenet

```
depth=1
   /C=HU/ST=Baranya/L=Pecs/O=PROBA/CN=proba.dravane
   t.hu/emailAddress=akarki@akarhol.hu
verify error:num=19:self signed certificate in
   certificate chain
verify return:0
+OK Hello there.
```

POP/IMAP SSH alagúttal

- A `mailhost` nevű szerverről szeretnénk lekérni üzeneteinket a `myclient` gépünkre
- Válasszunk egy tetszőleges (szabad) TCP portot a gépünkön. Legyen ez most : 12345
- Az alagút felépítése:

```
ssh -f -N -L 12345:localhost:110 mailhost
ssh -f -N -L 12345:localhost:143 mailhost
```

- Levelezőkliens beállítása az 12345 portra

SMTP szerverek

- E-mailek fogadása és továbbítása az Interneten
  - Helyi levelek: a kiszolgáló egy helyi felhasználójához kell kézbesíteni az üzenetet
  - Nem helyi levelek: a kézbesítéshez másik kiszolgálóhoz kell továbbítani az üzenetet
- Open relay szerverek
  - bárki használhatja őket továbbítóként (célszerű kerülni)
  - Problémái:
    - spammerek előszeretettel használják
    - levelezőszerverünk ezáltal feketelistára kerül és használhatatlan lesz
- Szolgáltatók levelező szerverei
  - Általában csak a saját hálózatuk címeiről továbbítanak leveleket
  - A mobil használók szempontjából ez sok kellemetlenséggel jár

SMTP hitelesítés

- Hitelesítés után bármely hálózatból küldhetünk levelet mindig azonos SMTP szervert használva
- Írjuk át a sendmail.mc állományban a következőt

```
DAEMON_OPTIONS(`Port=smtp, Addr=127.0.0.1, Name=MTA`)
```

erre:

```
DAEMON_OPTIONS(`Port=smtp, Name=MTA`)
```

- Engedélyezzük a következő sort a sendmail.mc-ben

```
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN`)
```

- A sendmail konfiguráció újratelepítése

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

- A sendmail újraindítása

```
/etc/init.d/sendmail restart
```

- Felhasználói fiókok létrehozása az SMTP hitelesítéshez

```
/usr/bin/saslpasswd -c c-ta
```

Az SMTP szerver tesztelése

```
c-ta@proba:~$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 proba.dravanet.hu ESMTP Postfix (Debian/GNU)
helo akarmi.akarhol.hu
250 proba.dravanet.hu
mail from:<akarki@akarmi.akarhol.hu>
250 Ok
rcpt to:<c-ta@ttk.pte.hu>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Próba üzenet
Ez egy teszt üzenet
.
250 Ok: queued as 46A442800087
quit
221 Bye
Connection closed by foreign host.
```