Internetin tietoturva - kuka on heikoin lenkki?

Markus Peuhkuri

2006-03-15

Luennon aihe

- Turvallisuudesta
- Ohjeita, tapauksia
- Miten hyvät asiat menevät pilalle

Otsikoita turvallisuudesta

- Slammer-mato sulki Davie-Besse ydinreaktorin ohjausverkon 2002
- Blaster-mato viivästytti sähkönsiirtoverkon mittaustietoja ja oli yksi osasyyllinen Koillis-Yhdysvaltojen sähkökatkoon 2003
- Panix.com[1] menetti piirinimensä hallinnan tammikuussa 2005. Asiakkaiden sähköposti ohjautui kolmannen osapuolen palvelimelle.
- 30 000 henkilötietoa varasttiin George Mason University:stä
- Ryhmä varasti väärillä viivakoodeilla tavaraa 1,5 MUSD arvosta Wal-Mart-kauppaketjulta
- Murtautujalla oli pääsy T-Mobilen verkkoon 7 kk ajan ja pääsi käsiksi henkilötietoihin, valokuviin ja FBI:n dokumentteihin
- Englantilainen nainen ei voi nukkua, koska joku varasti aivotahdistimen kaukosäätimen, laitteen vaihtaminen vaatii uuden leikkauksen.
- Teho-osaston koneet olivat käyttökelvottomia, koska niitä käytettiin osana botnettiä.

Kuinka selvitän henkilön salasanan?

- Asenna koneeseen troijalainen tai valvontaohjelma
  - − netbus, back orifice, bo2k
  - \+ salakuuntelu, -katselu, tiedostojen selailu
  - \- antivirusohjelmat tunnistavat
    ⇒ täytyy koodata itse
- Salakuuntele (langatonta)verkkoa nykyään vaikeampaa, mutta sopivia laitteita löytyy verkkoliitäntään asennettaviksi.
- Asenna koneeseen näppäilyt tallentava laite: tallentaa 64Ki näppäilyä, USD90

[1] Iso internet-operattori New Yorkissa

- Hanki TEMPEST-laitteisto
  - ... tai, osta lahjaksi langaton näppäimistö

... tai kysy vain!

- Vetoa ongelmaan – haluan vain auttaa: (keskiviikkoiltana)

  h Ylläpidosta Mika terve; tietomurron takia palvelimet joudutaan asentamaan uudelleen — tiedostot ovat käytettävissä taas maanantaina.

  u Ei tule mitään! Minun pitää saada suunnitelma valmiiksi perjantaihin menessä asiakkaalle tai tulee firmalle isot sakot.

  h Joo, joo. Arvaa oletko ainoa joka sanoo noin? Itselläni on *hauska* viikkonloppu tiedossa.

  u Mikä oli nimesi? Kukas on esimiehesi? Soitan hänelle, niin saa pistää asiat tärkeysjärjestykseen.

  h Huoh... No joo, voin koettaa saada tiedostosi väliaikaispalvelimelle, mutta sitä varten tarvitsen tunnuksesi ja salasanasi.

  u Mitäs...? Eihän ylläpito koskaan kysy salasanaa? Kuka oikein olet?

  h Hei, koetan vain saada ne tiedostosi sinulle! Jos annat salasanasi, voin kopioida sinun tiedostosi nopeasti — toinen vaihtoehto on kopioida koko palvelin; saat tiedostot maanantaina.

  u Njaa...

  h Odotas hetki, käyn hakemassa paperisi... Työntekijänumerosi on 24671 ja eka salasanasi on ollut "changeme98".

  u Äh. Ok. Salasana on "Uuponen02".

  h Hyvä. Tiedostosi ovat näkyvissä puolen tunnin kuluttua.

- Huijaa aloittelevaa työntekijää

  h Tietoturvaosastolta Mika terve, tervetuloa taloon! Oletko saanut jo opastuksen tietoturva-asioista?

  u En vielä.

  h No, käydään sitten läpi perusasioita:

  ... *keskustelua*

  h ...salasanasta vielä, siinä pitää olla sekä isoja ja pieniä kirjaimia että numeroita. Onko salasanassasi niitä?

  u Ei, se on vain tyttönimeni "pienranta".

  h Et olisi saanut sanoa sitä, mutta se ei ole kovin hyvä. Parempi olisi lisätä siihen vaikka kuukausi ja vuosi, esimerkiksi "PienrantaHel03"

  u Joo, vaihdan sen. Osaan tehdä sen.

  ... *keskustelua*

  h Etköhän pärjäile, hyvää työntekoa.

Miten ihmistä huijataan?

- Vastavuoroinen auttaminen
- Auktoriteetti
- Sääli
- "Tiimipelaaja" — auta kaveria pulassa
- Ahneus
- Luottamusta pienin askelin

Turvaongelmat

Protokollaongelmat protokollien suunnittelussa ei riittävää painoa turvaominaisuuksiin

- IP-lähdereititys
- FTP-protokolla

Ohjelmistovirheet syötteen olettaminen

- ohjelmointivirheet (puskureiden ylivuodot yms.)
- virheellinen toteutus protokollasta (esim. ICMP redirect)
- mitään *ei pidä olettaa* käyttäjältä tai verkosta tulevasta datasta
- sovellusten yhteistoiminta

Konfigurointivirheet oletuskonfiguraatio pielessä

- ominaisuudet tärkeämpiä kuin turvallisuus
- yleensä valitetaan "miksi tämä ei toimi"
  $\Rightarrow$ oletusasetukset liian sallivia

Haittaohjelmat

Virus leviää toisten ohjelmien tai dokumenttien välityksellä (2001 lopussa yli 60.000 tunnettua, joista ainoastaan muutamia satoja on tavattu levinneinä "villinä".)

- tuhoaa tiedostoja, jopa laitteistoja
- muuntaa tiedostoja
- heikentää suorituskykyä

Mato leviää itsenäisesti järjestelmästä toiseen verkon yli

- voi heikentää myös verkon suorituskykyä
- CodeRed, Slammer

Troijan hevonen näennäisesti hyödyllinen ohjelma tai dokumentti jolla on salainen toimintatapa

- voi esimerkiksi mahdollistaa murtautumisen koneeseen

- Kukin tyyppi voi
  - paljastaa tietoja, esim. lähtettämällä tiedostoja sähköpostise
  - tarkkailla käyttöä, esim. tallentaa salasanoja
  - mahdollistaa murtautuminen, esim. avaamalla takaportin
- Haittaohjelma voi olla myös *räätälöity* murtautumaan ainoastaan tiettyyn järjestelmään tai paljastamaan yksittäisen käyttäjän tietoja. Tälläistä haittaohjelmaa eivät normaalit virustorjuntaohjelmat välttämättä tunnista. Tämä on eräs tapa teollisuusvakoiluun.

Palomuurit

- Palomuuri eroittaa kaksi *eri turvapolitiikkaa* noudattavaa aluetta
  - yrityksen sisäinen verkko vs. Internet
  - myös yrityksen sisäisessä verkossa esim. osastojen välillä
- Yksikerroksinen palomuuri
  - yksi kone kahden verkon välissä
  - yksinkertainen konfigurointi, virheet vakavia
- Monikerroksinen palomuuri

  - palomuuritoiminnallisuus hajautettu useiden laitteiden välille
  - neutraaliverkko (DMZ) erotettavien verkkojen välillä
- Konekohtainen ohjelmistopalomuuri
  - ohjelmisto tarkkailee koneen liikennettä
  - mahdollistaa ohjelmapohjaisen valtuutuksen: ainoastaan nimetyt ohjelmat saavat liikennöidä tietyllä tavalla verkkoon
    ⇒ hienojakoinen turvallisuus
    ⇒ estää haittaohjelmia
  - turvallisuus riippuu koneen turvallisuudesta: esim. troijalainen voi kytkeä palomuurin pois päältä ennenkuin liikennöi verkkoon. Helppoa koneissa, jossa ei ole erillistä pääkäyttäjää (koti-windowssit), mahdollista myös paremmissa järjestelmissä, mikäli on paikallinen turva-aukko.
- Läpinäkyvyysvaatimus

  > The introduction of a firewall and any associated tunneling or access negotiation facilities *MUST NOT* cause unintended failures of *legitimate* and *standards-compliant* usage that would work were the firewall not present.[1]

- Tuottaa helposti "kova ulkoa, pehmeä sisätä"-suojauksen
  ⇒ *kun* hyökkääjä saa ohitetua palomuurin, ei enää vaikeuksia

Kolme askelta tietoturvaan

(www.tietoturvaopas.fi)

1. Käyttöjärjestelmä ajan tasalle
   - kaikista järjestelmistä löytyy virheitä
     ⇒ säännöllisesti tarkistettava tietoturvapäivitykset
2. Virustorjuntaohjelmisto
   - ei tarpeen, mikäli sovellusohjelmat turvallisia
   - kaupallisissa ohjemissa 20-30 virhettä/KLOC: Mozilla 1.7 1600 KLOC
3. Palomuuri käyttöön
   - ei tarpeen, mikäli järjestelmä turvallinen

Kuinka turvallisuus rakentuu

- Turvallisuus on prosessi, ei tuote
  - uusia turvallisuusongelmia tulee
  - ympäristö muuttuu: verkko, sovellukset, käyttäjät
- Turvallisuus riippuu heikoimmasta lenkistä

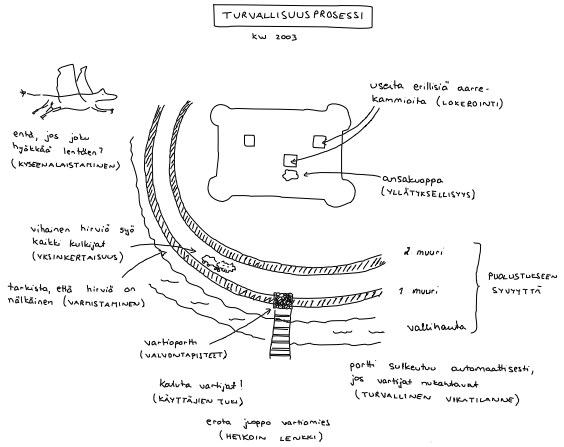
käytäjä	sovellukset	OS	laitteisto	verkko	palomuuri

  Ei ole mitään merkitystä sillä, käytetänkö 40- vai 128-bittistä salausta tai 512- tai 2048-bittisiä RSA-avaimia, jos salasanan saa arvattua, kysyttyä käyttäjältä tai salakuunneltua koneesta.

Kuinka parantaa turvallisutta?

- Lisätään tekniikkaa
  - lisää monimutkaisuutta
  - järjestelmät jäykkiä ⇒ kierrettäviä
  - luotetaan turvajärjestelmiin liikaa
  + lisää liikevaihtoa
- Vaaditaan parempi tunnistus
  - lisää monimutkaisuutta
  - virheellisten estojen määrä kasvaa
- Koulutetaan käyttäjiä
  + motivoitunut käyttäjä erinomainen suoja
  - aina on onnistuttu hämäämään joitakin jonkinaikaa
  - jos turvajärjestelmä estää työnteon, se kierretään

Turvallisuus organisaatiossa



Turvallisuus ↔ vaarattomuus

- Security ↔ safety
- Järjestelmän vaarattomuutta tutkittaessa voidaan hyvin harvinaiset tapaukset jättää huomioimatta
- Turvallisuudessa pitää huomioida myös epätodennäköisiä yhteensattumia
  – hyökkääjä pyrkii saamaan järjestelmän nurin
  – menetelmä voi olla täysin arvaamaton
- Väärien positiivisten ja negatiivisten suhde oltava järkevä
- Absoluuttien turvallisuus tuhon alku (Titanic, Enigma)

Turvallisuuden viisi askelta

1. Mitä haluan suojata?
2. Mitkä ovat riskit?
3. Kuinka hyvin turvaratkaisu suojaa riskeiltä?
4. Mitä muita riskejä turvaratkaisu aiheuttaa?
5. Mitä kustannuksia ja kompromisseja ratkaisusta aiheutuu?

Arvioi riskejä

- Aseta eläimet vaarallisuusjärjestykseen (kuolemantapauksia Yhdysvalloissa)
  - hai
  - koira
  - käärme
  - peura
  - sika
- Todennäköisin kuolinsyy 2000-2003 (Yhdysvalloissa)
  - diabetes
  - junaonnettomuus
  - lentokoneonnettomuus
  - maaliikenneonnettomuus
  - murha
  - salamanisku
  - terrori-isku
  - tulva
- Todennäköisin kuolinsyy 2000-2002 (Suomessa)
  - kurkunpää-, henkitorvi-, keuhkosyöpä
  - diabetes
  - influenssa
  - keuhkokuume
  - astma
  - maaliikennetapaturmat
  - vesikuljetustapaturmat
  - tapat. kaatumiset ja putoamiset
  - hukkumistapaturmat
  - myrkytystapat. pl. alkoholimyrkytys
  - itsemurhat
  - murhat, tapot, muu tahall. pahoinpit.

Ja vastaus on...

- Aseta eläimet vaarallisuusjärjestykseen (kuolemantapauksia Yhdysvalloissa, kokonaismäärä/vuosi)
  1. peura (135)
  2. koira (18)
  3. käärme (15)
  4. sika (?)
  5. hai (0,6)
- Todennäköisin kuolinsyy 2000-2003 (Yhdysvalloissa vuosittain)
  1. diabetes (68 000)
  2. maaliikenneonnettomuus (41 000)
  3. murha (15 600)
  4. terrori-isku (1 000)
  5. lentokoneonnettomuus (631)

6. junaonnettomuus (530)
7. tulva (139)
8. salamanisku (87)

- Todennäköisin kuolinsyy 2000-2002 (Suomessa, 1/100 000)
  1. keuhkokuume (41)
  2. kurkunpää-, henkitorvi-, keuhkosyöpä (32)
  3. itsemurhat (21)
  4. tapat. kaatumiset ja putoamiset (18)
  5. diabetes (9,2)
  6. maaliikennetapaturmat (7,2)
  7. myrkytystapat. pl. alkoholimyrkytys (3,4)
  8. hukkumistapaturmat (2,7)
  9. murhat, tapot, muu tahall. pahoinpit. (2,7)
  10. astma (1,8)
  11. vesikuljetustapaturmat (1,2)
  12. influenssa (1,2)

Riskien arviointi: yleisesti ihmiset

- Aliarvioivat usein ottamansa riskit
- Yliarvioivat riskit
  - joihin eivät voi vaikuttaa
  - harvinaiset
  - huomiota herättävät, uutisoidut
  - personoidut riskit

Pankkikorttien kloonaus: lukija

Lukija paikoillaan

PIN-kamera esitekotelossa

PIN-kamera toimintavalmiina

Mistä tietää kuka siellä vastaa

Katsotaas viestiä tarkemmin (HTML)

- Status-kenttää vaihdetaan 25 ms välein

```
var boodschap = 'https://www.paypal.com/';
function dgstatus()
{
      window.status = boodschap;
        timerID= setTimeout("dgstatus()", 25);
}
```

- Linkissä onkin IP-osoite

```
Follow <a href="http://210.78.22.113/verify.html">this
link</a> located at PayPal server to fill needed information.
```

- PayPal on Kaliforniassa

```
Domain Name: PAYPAL.COM

Administrative Contact, Technical Contact:
   Inc., PayPal  (36270680P)          hostmaster@PAYPAL.COM
   1840 Embarcadero Rd.
   Palo Alto, CA 94303
   US
   408-376-7400 fax: 650.251.1101
```

- `www.paypal.com` on myös

```
www.paypal.com has address 64.4.241.32
OrgName:    PayPal
OrgID:      PAYPAL
Address:    303 Bryant Street
City:       Mountain View
StateProv:  CA
PostalCode: 94041
Country:    US

NetRange:   64.4.240.0 - 64.4.255.255
CIDR:       64.4.240.0/20
```

- Ilmeisesti päivityspalvelin (`210.78.22.113`) ulkoistettu Kiinaan?

```
inetnum:      210.78.22.64 - 210.78.22.128
netname:      SHJITONG-CN
descr:        JiTong Shanghai Communications Co.,Ltd
address:      Room 1001,Lekai Builing,Shangcheng Road,
address:      Pudong Xin district,Shanghai
country:      CN
```

Muita vedätyksiä

- Näytetty linkki ja "oikea" linkki eivät vastaa toisiaan

```
...secure server
<a href="http://www.scam.example/">
https://www.paypal.com</a>...
```

- Melkein sama nimi
  - www.PayPaI.com
  - www.PayPa1.com
  - www.paypal-secure.com
  - homomorfismi: `www.p&#1072;ypal.com`
- http://www.paypal.com:secure.information.update@10.12.80.5/
- http://www.paypal.com%01:secure@10.12.80.5/
- Monia vastaavia huijauksia toteutettu eri yrityksille, tyypillisesti pankeille
- Ensimmäiset suomenkieliset

> Toivoen ymmartamyksen ja kannatuksen Teidan puolelta.
> Kunnioittaen,
> Hallinto

Toinen phishing-hyökkäys

- `From: ITviikko Digilehti <itviikko.digilehti@sanoma.fi>`
- Rekisteröintilinkki

```
Rekisteröidy Digilehden lukijaksi
<A href="http://www.webstudio.fi/itviikko/esittely.html"
target=_top>tästä</A>
```

Ei `itviikko.fi`?

```
domain:    webstudio.fi
descr:     SOPRANO COMMUNICATIONS OY
```

- Sähköpostin lähettäjä:

```
Received: from mail pickup service by mail.swelcom.fi
   with Microsoft SMTPSVC; Thu, 20 Jan 2005 12:50:28 +0200
```

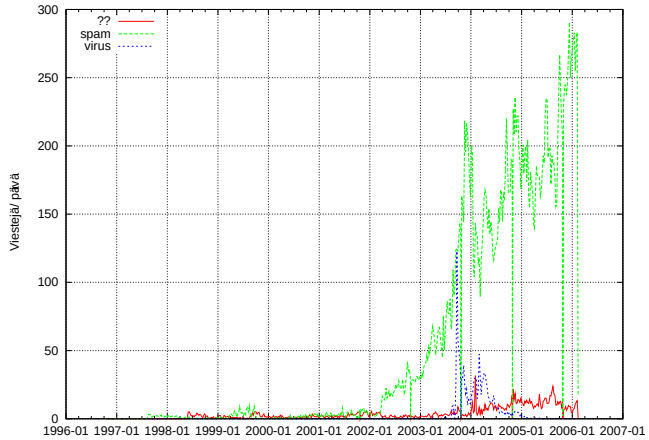
Ehkä murrettu palvelin, ei **itviikko.fi**?

```
domain:    swelcom.fi
descr:     SWelcom Oy
```

- Web-osoite osoittaa jonnekin muulle ja jokin kolmas osapuoli on lähettynyt joku kolmas osapuoli
  ⇒ Phishing-hyökkäys?

Viesti oli kuitenkin “oikea” (varmistettu ITViikon toimituksesta), vaikka siinä oli kaikki phishing-hyökkäyksen merkit. Tavallisen käyttäjän on hyvin vaikea eroittaa “oikeat” ja “huijaus”sähköpostit; teknisesti ei välttämättä mitään eroa.

Roskaposti – kiusasta ongelmaksi



Roskapostin torjunnasta

- Tekninen ratkaisu ei ole lopullinen
  - verkkoliikennettä
  - prosessointia
  - suodattimet ja järjestelmät kierrettävissä
- Ratkaisu saatava polittiselta tasolta
  - pääosa spämmistä on peräisin Yhdysvalloista
  - suurin osa tulee nykyään Kiinan ja Korean kautta
  - oikeuslaitoksen uhka ainoa “todellinen” hidaste
    ⇒ follow the money

Yhteenveto

- Turvallisuus on monen asian summa
- Hyökkäykset muuttuvat ja muttavat pelin sääntöjä
- Turvallisuus on aina valinta ja kompromissi
- Tekniset järjestelmät kierrettävissä
  $\Rightarrow$ huolehdittava siitä, että järjestelmä ei romahda

References

[1] N. Freed. Behavior of and Requirements for Internet Firewalls. Request for Comments RFC 2979, Internet Engineering Task Force, October 2000. (Informational). URL:`http://www.ietf.org/rfc/rfc2979.txt`.