Samlink

Tietoturvallisuuden ajankohtaiset haasteet

ISACA Finland 20-vuotisjuhlaseminaari
20.4.2009

Jari Pirhonen – www.iki.fi/japi
Turvallisuusjohtaja, CISA, CISSP, CSSLP
Samlink – www.samlink.fi

Sisältö

- **Ristiriitaisia vaatimuksia ja tavoitteita**
  - → **Tarvitsemme uutta näkökulmaa tietoturvan hallintaan**
- **Uusia johtamis- ja osaamisvaatimuksia**
  - → **Fokuksena liiketoiminnan ja riskien ymmärtäminen**
- **Uusia haasteita**
  - → **Vaatimukset ja uhat lisääntyvät**

We can't solve problems using the same kind of thinking we used when we created them.
-- Einstein

Samlink

Sisältö

- **Ristiriitaisia vaatimuksia ja tavoitteita**
  - →Tarvitsemme uutta näkökulmaa tietoturvan hallintaan
- Uusia johtamis- ja osaamisvaatimuksia
  - →Fokuksena liiketoiminnan ja riskien ymmärtäminen
- Uusia haasteita
  - →Vaatimukset ja uhat lisääntyvät

The chief cause of problems is solutions
-- Eric Sevareid

Samlink

”Ne jyrää meitin. Pojaat! Ne jyrää meitin.”

Viime perjantaina…

Pääkirjoitus

Kauppalehti

PÄÄTOIMITTAJAT ») HANNU LEINONEN (VASTAAVA), EERO TUOMISTO TOIMITUSPÄÄLLIKKÖ ») JUHA RUONALA

VIHREÄ YLLÄTYS Uutisblogi »

«kl.fi»

JYP-KAUPUNKI HÄVISI KAAVAN Nettinapakka »

Pääkirjoitus 17.4.2009

Haittaohjelmista yhä taitavampia

Verkkojen haittaohjelmat vaanivat yhä taitavammin yrityksiä ja kuluttajia. Hyökkäykset ovat niin hienostuneita, että kaikki eivät tiedä olevansa niiden kohteena.

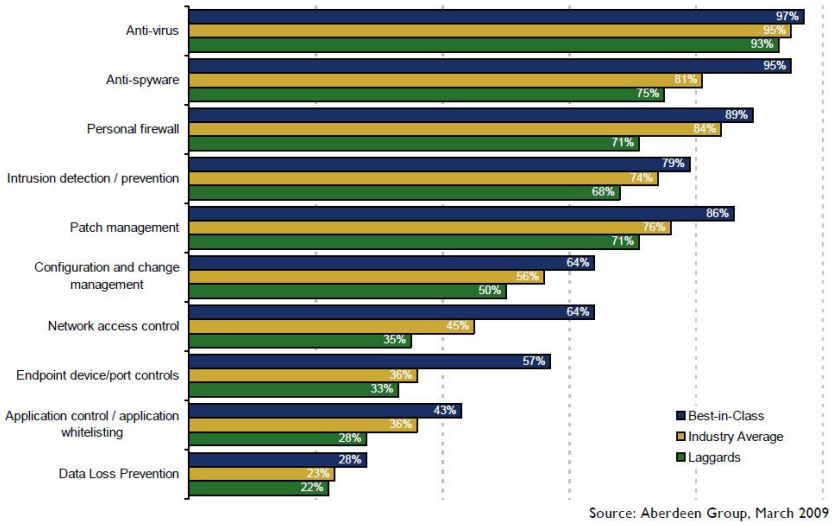
Viestintävirasto arvioi alkuvuoden 2009 aikana Suomessa olleen tuhansia Conficker-haittaohjelman saastuttamia koneita. Maailmalla niitä oli jopa 15 miljoonaa.

Näpakka

Nokia yllätti jälleen

Samlink

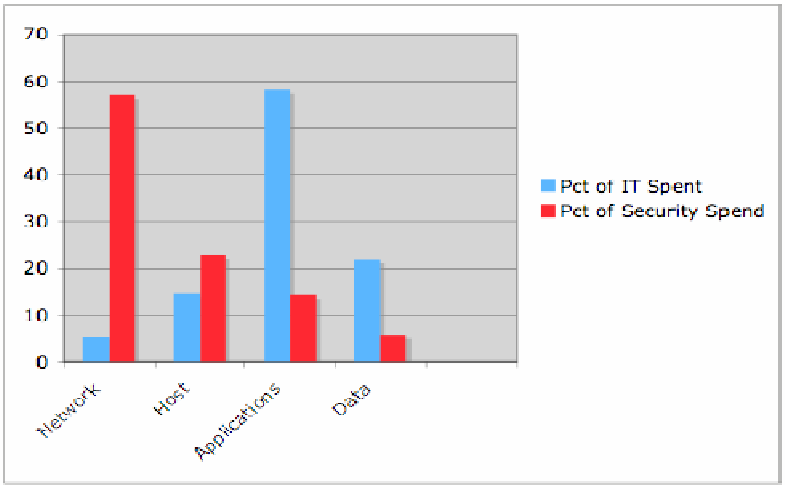
”Ei ne mitään jyrää. Siellä on miinoitus.”



Source: Aberdeen Group, March 2009

Samlink

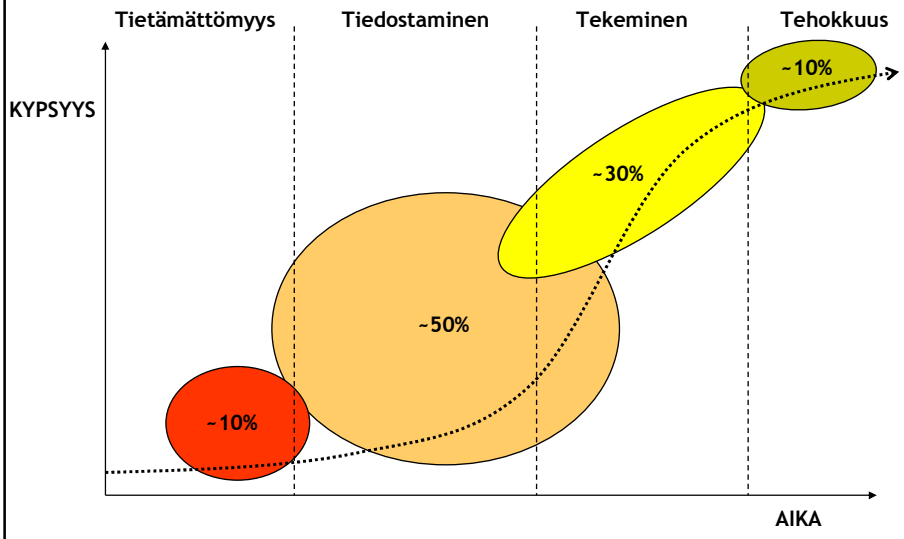
Tietoturvabudjetti epäbalanssissa?



Lähde: http://1raindrop.typepad.com/

Samlink

Arvio yritysten tietoturvakypsyydestä



20.4.2009 Jari Pirhonen **Lähde: Gartner ja Howard Schmidt puhe 29.4.08**

Samlink

Vuosisadan suunnitteluhaasteet


Make solar energy economical


Provide energy from fusion


Manage the nitrogen cycle


Provide access to clean water


Advance health informatics


Engineer better medicines


Prevent nuclear terror


Secure cyberspace


Advance personalized learning

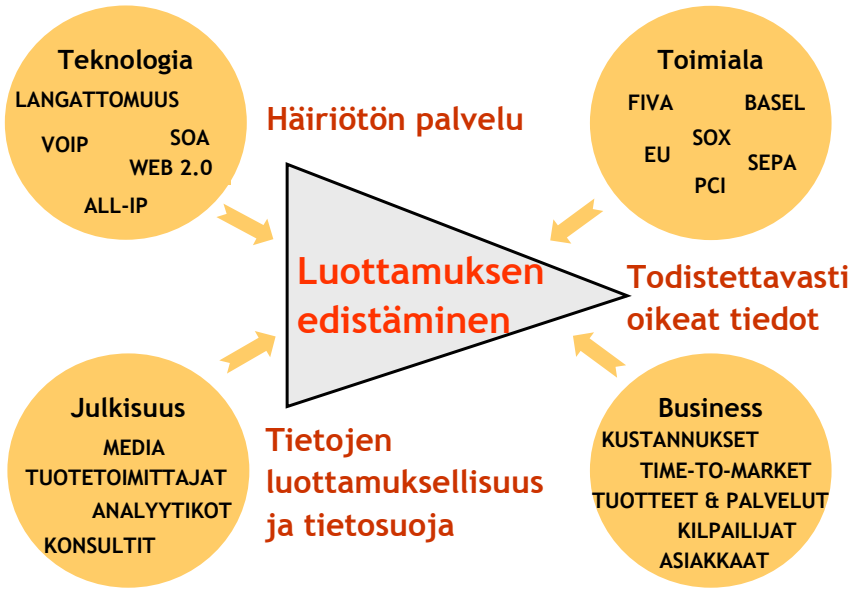

Engineer the tools of scientific discovery

- **Laitteiden, sovellusten, tiedon ja käyttäjien vahva todentaminen**
- **Turvallisten sovellusten tuottaminen ja todentaminen**
- **Tietoliikenteen aitouden ja oikeellisuuden varmistaminen**
- **Tietoturvaratkaisujen helppokäyttöisyys**
- **Kokonaisuuksien turvaaminen**

20.4.2009 Jari Pirhonen **Lähde: http://www.engineeringchallenges.org/**

Samlink

Tietoturvan ristiriitaiset vaatimukset



Samlink

Strategisia ratkaisuja vai tuotteita?

Samlink

Onko tietoturva kilpailutekijä?

- Tuottavuuden määritelmä: ***Kuka pystyy toisten kanssa samassa ajassa ja samaa teknologiaa hyödyntäen tuottamaan eniten ja alimmilla yksikkökustannuksilla tavoitellun laatutason täyttävää tuotetta ja hallitsemaan riskit.***

- Tietoturva EI ole kilpailutekijä, jos:
  - ratkaisut ovat tuotelähtöisiä
  - seurataan sokeasti ”parhaita käytäntöjä”
  - tehdään samaa kuin muutkin
  - keskitytään tietoturvan parantamiseen riskien hallinnan sijaan
  - ratkaisujen tehokkuutta ei mitata

- Olisiko aika kyseenalaistaa ”totuuksia” ja suunnata ”siniselle merelle”?

20.4.2009 Jari Pirhonen

Samlink

Onko aika kyseenalaistaa vanhat totuudet?

LUO
Mitä täysin uusia tekijöitä tarvitaan?

POISTA
Mitkä nyt selviönä pidetyt tekijät ovat turhia?

Uudet arvot ja toimintamallit

KOROSTA
Mitä tekijöitä pitäisi korostaa nykyistä enemmän?

SUPISTA
Mitä tekijöitä pitäisi selvästi supistaa?

Lähde: Kim & Mauborgne, Sinisen meren strategia

20.4.2009 Jari Pirhonen

Samlink

Sisältö

- Ristiriitaisia vaatimuksia ja tavoitteita
  - → Tarvitsemme uutta näkökulmaa tietoturvan hallintaan
- **Uusia johtamis- ja osaamisvaatimuksia**
  - **→ Fokuksena liiketoiminnan ja riskien ymmärtäminen**
- Uusia haasteita
  - → Vaatimukset ja uhat lisääntyvät

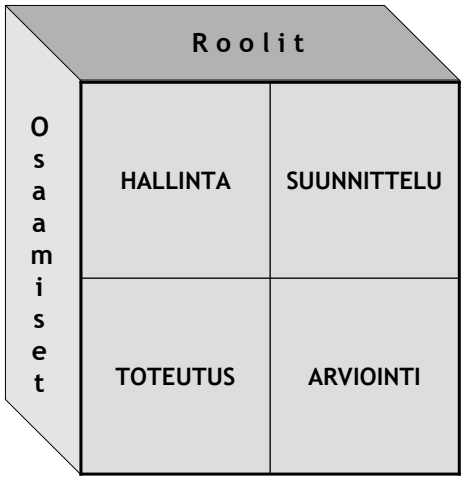
Among the other skills and knowledge you have you need to be able to tell people things they don't want to hear and have them asking for more.
-- anonymous

Samlink

Tietoturva-ammattilaisen osaamisvaatimukset

1. Tietojen suojaaminen
2. Tietorikosten tutkiminen
3. Liiketoiminnan jatkuvuus
4. Poikkeamien hallinta
5. Tietoturvakoulutus ja -tietoisuus
6. IT-järjestelmien operointi ja ylläpito
7. Tietoverkkojen turvallisuus
8. Henkilöstöturvallisuus
9. Fyysinen turvallisuus
10. Tuotteiden ja palvelujen hankinta
11. Ulkoisten vaatimusten täyttäminen
12. Riskien hallinta
13. Strateginen johtaminen
14. Sovellusten turvallisuus

Lähde: IT Security Essential Body of Knowledge
US Department of Homeland Security,
National Cyber Security Division



Samlink

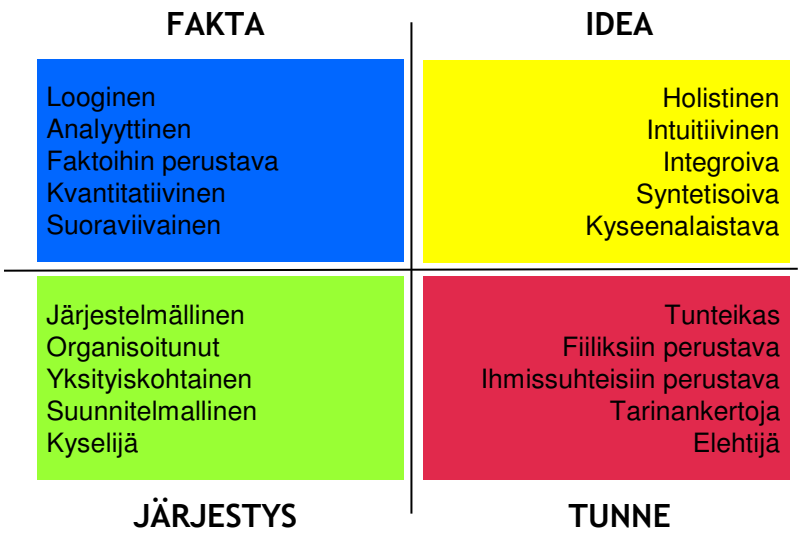
Osaamistarpeet muuttuvat

- Information Security Forumin mukaan organisaatioiden tietoturvavastaavien odotuksena on, että tietoturvafokus muuttuu tulevaisuudessa selkeästi nykyisestä teknologialähtöisyydestä liiketoimintalähtöiseksi
  - Tietoturvan tarkoitus → organisaation strategiaan nivoutunut, liiketoimintaprosesseihin integroitunut
  - Ihmisten osaamistarve → liiketoiminta- ja riskienhallintaosaamista tietoturvaosaamisen lisäksi, innovatiivisuus
  - Tehtävät → riskienhallinta + vaatimustenmukaisuus + tietoturvakonsultointi, IT ja fyysisen turvallisuuden konvergenssi
  - Kommunikointi → riskiperustainen tietoturvatietoisuus
  - Mittarit → BSC, KPI, tietoturvan arvo, ratkaisujen tehokkuus

Lähde: ISF, Role of Information Security in the Enterprise

Samlink

Ihmiset ovat erilaisia



Lähde: Hermann Whole Brain Model

Samlink

Teetkö päätöksiä fiiliksellä vai järjellä?

System 1 (fiilis)	System 2 (järki)
• Automaattinen	• Harkitsevainen
• Vaivaton	• Työläs
• Nopea	• Hidas
• Hitaasti mukautuva	• Nopeasti mukautuva
• Totutun mukainen	• Älyllinen
• Reaktiivinen	• Proaktiivinen
• Spesifinen	• Geneerinen
• Vaikea pukea sanoiksi	• Helppo perustella

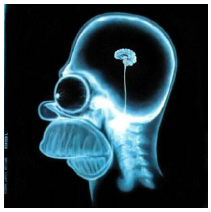
Intuitio, selkärangasta saatu tai kokemukseen perustuva vastaus on usein väärä. Järki pyrkii ennemminkin perustelemaan fiiliksellä saatua vastausta oikeaksi kuin hakemaan oikeaa vastausta.

Lähde: Dan Gardner, RISK - The Science And Politics Of Fear

Samlink

Fiilis vs. järki riskienhallinnassa, esimerkkejä

- Vältämme riskejä varmistaaksemme tuotot - hyväksymme helpommin tappion aiheuttavia riskejä
- Tapahtumien todennäköisyys on helposti manipuloitavissa. Arvostamme näennäistä varmuutta enemmän kuin epävarmuuden vähentämistä - vaikka lopputulos olisi sama
- Sama omaisuus on arvokkaampi itsellä kuin toisella
- Useampi peräkkäinen menetys tuntuu isommalta kuin yksi iso, kokonaisarvoltaan samansuuruinen menetys
- Olemme taipuvaisempia hyväksymään tekemättä jättämisen riskin kuin mahdollisen muutoksen aiheuttaman riskin
- Välitön tuotto/tappio tuntuu merkittävämmältä kuin sama tuotto/tappio tulevaisuudessa
- Meillä on pyrkimys vahvistaa tehtyjä päätöksiä sen sijaan, että arvioimme objektiivisesti nykytilannetta



Lähde: Max H. Bazerman, Judgement in Managerial Decision Making

Samlink

Voiko auditoija olla puolueeton?

- ”Rajoitettu eettisyys” (bounded ethicality)
  - Psykologiset prosessit voivat johdattaa ihmisiä toimintaan, joka on vastoin heidän omia eettisiä periaatteitaan.
- Ristiriitaiset tavoitteet voivat tiedostamattamme vääristää arvioitamme (self-serving bias)
  - Erityisesti, kun auditoijan ja auditoitavan edut ovat kytköksissä
  - Auditoija näkee asiat asiakkaansa etujen näkökulmasta
  - Asiakkaan etu on auditoijan etu
  - Riippumattomuus psykologisesti mahdotonta
- Meillä on taipumus muodostaa ennakkokäsitys ja sen jälkeen pyrkiä todistamaan ennakkokäsitys oikeaksi

Lähde: Max H. Bazerman, Judgement in Managerial Decision Making

Samlink

Sisältö

- Ristiriitaisia vaatimuksia ja tavoitteita
  - → Tarvitsemme uutta näkökulmaa tietoturvan hallintaan
- Uusia johtamis- ja osaamisvaatimuksia
  - → Fokuksena liiketoiminnan ja riskien ymmärtäminen
- Uusia haasteita
  - → Vaatimukset ja uhat lisääntyvät

It is not enough to do your best; you must know what to do, and then do your best.
-- W. Edwards Deming

Samlink

Haaste: Vaatimustenmukaisuus

- Ulkoiset vaatimukset lisääntyvät
- Vaatimukset eivät huomioi yritysten riskinsietokykyä ja halua
- Tietoturvan toteutuminen on todistettava asiakkaille ja kumppaneille
- Vaatimusten täyttäminen ei takaa tietoturvaa

Samlink

PCI DSS

BANK INFO SECURITY®

Heartland Data Breach: Visa Questions Processor's PCI Compliance

Visa Executive: "We've Never Seen Anyone Who Was Breached That Was PCI Compliant"

Linda McGlasson, Managing Editor
March 24, 2009

Despite the **Heartland Payment Systems (HPY) data breach** and other noted compromises, Visa staunchly supports the Payment Card Industry Data Security Standard (PCI DSS).

This is the message from Adrian Phillips, Visa's Deputy Chief Enterprise Risk Officer, who in an exclusive interview hammers home the credit card company's support for the security standard - and suggests that, contrary to Heartland's own statements, the payment processor may not have been PCI compliant when it was breached sometime in 2008.

"We've never seen anyone who was breached that was PCI compliant," Phillips says without specifically naming - or excluding -- Heartland. "The breaches that we have seen have involved a key area of non-compliance."

Interviewed during last week's Visa Security Summit in Washington, D.C., Phillips acknowledges Heartland and other recent breaches, but uses them as an opportunity to support the PCI standard. "Let's remember we've had some bad breaches, but if we had not had PCI DSS, it would have been much worse," Phillips says. "As of today, I am confident that PCI DSS works."

Phillips comments come one week after news that Visa had removed Heartland Payment Systems from its **certified PCI-DSS Compliant Service Providers list**.

Forbes.com

Security

Visa, MasterCard In Security Hot Seat

Andy Greenberg, 03.31.09, 8:00 PM ET

Criminal hackers aren't just hard to catch. They're also hard to blame.

In security breach cases last year, such as Hannaford Bros. supermarket and the card processing firm Heartland Payment Systems, the cybercriminals who gained access to millions of consumers' credit card details haven't been--and may never be--identified or prosecuted.

So in a hearing Tuesday, the House of Representative's Committee on Homeland Security took aim at a more accessible target: credit card companies like Visa and MasterCard, which are responsible for creating and enforcing the Payment Card Industry (PCI) standards that failed to prevent those breaches.

Given that both Hannaford and Heartland had complied with PCI rules, the congressional panel turned the spotlight on the credit card companies, arguing that their security measures need to be redesigned or supplemented with federal laws--a potential crackdown that could require changes on the part of both retailers and financial services companies.

"I don't believe that PCI standards are worthless," said Rep. Yvette Clark, D-N.Y., who led the hearing. "But I do want to dispel the myth once and for all that PCI compliance is enough to keep a company secure. It is not."

Samlink

Tietomurron jälkeinen PCI arviointi

Build and Maintain a Secure Network	Compliance
Requirement 1: Install and maintain a firewall configuration to protect data.	30%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	49%
Protect Cardholder Data	
Requirement 3: Protect stored data.	11%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.	68%
Maintain a Vulnerability Management Program	
Requirement 5: Use and regularly update AV.	62%
Requirement 6: Develop and maintain secure systems and applications.	5%
Implement Strong Access Control Measures	
Requirement 7: Restrict access to data by business need-to-know.	24%
Requirement 8: Assign a unique ID to each person with computer access.	19%
Requirement 9: Restrict physical access to cardholder data.	43%
Regularly Monitor and Test Networks	
Requirement 10: Track and monitor all access to network resources and cardholder data.	5%
Requirement 11: Regularly test security systems and processes.	14%
Maintain an Information Security Policy	
Requirement 12: Maintain a policy that addresses information security.	14%

Lähde: Verizon 2009 Data Breach Investigations Report

Samlink

Haaste: Tietoturvalliset sovellukset

- Sovellukset ovat tietojärjestelmien ytimessä
- Tietoturvallisuus on upotettava systeemityömalliin
- Olemme riippuvaisia sovelluksista, mutta luotettavien sovellusten tekemiseen ei ole mallia
  - Ohjelmoinnin pitäisi olla tiedettä, ei taidetta
  - Onko tietoturvalla mahdollisuutta, jos sovelluskehitys yleensäkin on vielä lapsenkengissään?

Tutkimus 110 isosta projektista (koko keskimäärin 3 M$):

- **68% projekteista epä-onnistuminen todennäköistä**
- **Merkittävän epäonnistumisen mahdollisuus 50% (aikataulun ja/tai kustannusten ylitys 60% ja tulokset alle 70%)**

Lähde: IAG Business Anlysis Benchmark

I regularly and normally find that any requirement specification given to me by a new customer, even if it's approved and being used, has between 80 and 180 major defects per page. This is normally a shock for the people involved: "How can there be so many?"
-- Tom Gilb, www.gilb.com

Samlink

Turvallisten palveluiden tekeminen on vaativaa - yksittäisten ongelmien löytäminen helppoa

ENNEN

Linux + ohjelmointi

⇩

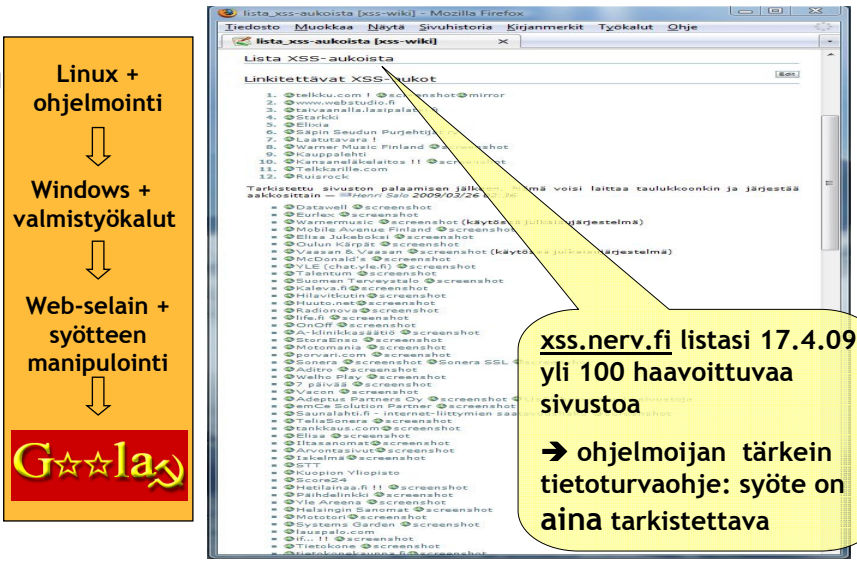
Windows + valmistyökalut

⇩

Web-selain + syötteen manipulointi

⇩

NYT



xss.nerv.fi listasi 17.4.09 yli 100 haavoittuvaa sivustoa

➔ ohjelmoijan tärkein tietoturvaohje: syöte on aina tarkistettava

Samlink

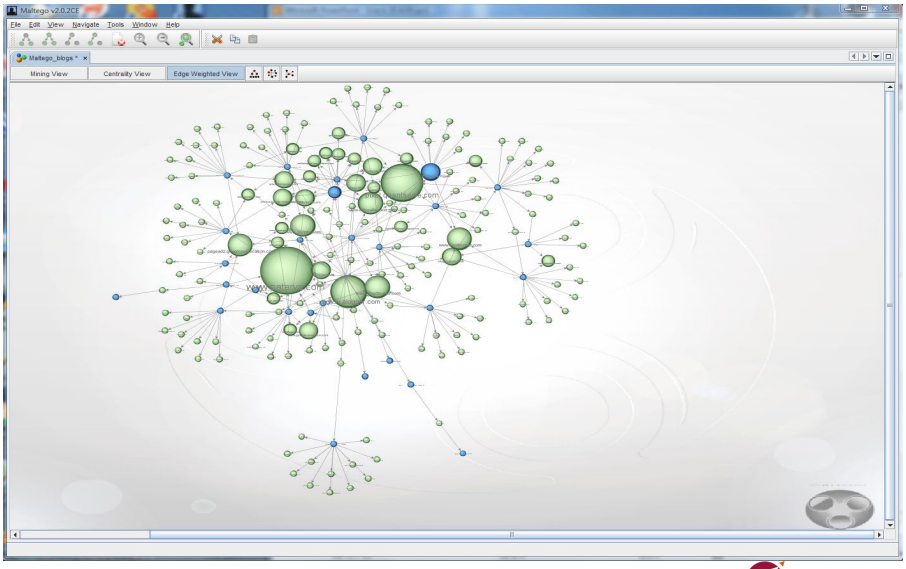
Haaste: Sosiaalinen media

- Yrityksen suhtautuminen: Facebook, Blogit, Twitter,…?
  - Mahdollisuus vai ajanhukkaa?
  - Tietovuodot vs. osaamisen jakaminen
  - Verkostoituminen vs. yksityisyyden suoja


Faking it? How to spot the frauds of Twitter...

Samlink

Maltego – tiedonlouhintaa verkossa



Samlink

Haaste: Tietoturva uusissa arkkitehtuureissa

- Tyypillisesti sovellusarkkitehdit eivät ymmärrä tietoturvaa eivätkä tietoturva-asiantuntijat sovellusarkkitehtuuria
  - Zachman vs. SABSA
- Merkittäviä arkkitehtuurisia muutoksia, joiden tietoturvavaikutuksia ei vielä ymmärretä
  - Virtualisointi
  - Palvelukeskeinen arkkitehtuuri (SOA)
  - Pilvipalvelut
  - Web 2.0, Web 3.0

Samlink

Tee-se-itse verkkopankki?

Web	**Pankkikohtaiset palvelut ja käyttöliittymät. Fokus verkkopankissa.**	**Käyttäjän tunnistaminen, tapahtumien vahvistaminen, verkkopankkisovelluksen turvaaminen.**
Web+	**Kommunikoinnin tehostaminen: VoIP, videoneuvottelu ja pikaviestintä. Fokus verkkopankissa.**	**Uusien teknologioiden tietoturvapiirteet ja osaaminen kypsyvät hitaasti.**
Web 2.0	**Pankkipalvelukomponentit. Mashups. Käyttäjä tekee oman käyttöliittymänsä. Erikoistuneita verkkopankki-liittymiä palveluna. Fokus käyttäjässä.**	**Pankin kontrolli pienenee, käyttötavat voivat olla arvaamattomia, pankki-palvelut integroituvat sovelluksiin. Tietoturvatiedon ja luottamuksen välittäminen.**
Web 3.0	**Räätälöidyt, automaattisesti muodostettavat palvelupaketit, jotka sisältävät usean finanssitalon ja palveluntarjoajan palveluja. Fokus käyttäjän palvelutarpeissa.**	**Tarvitaan mekanismi palveluiden luotettavuuden todentamiseen ja muita kehittyneitä turvapalveluita.**

Second Life banks hacked in virtual crime wave

Tue Nov 20, 2007 2:31pm PST

*By **Eric Reuters***

Last weekend saw a coordinated series of Second Life bank heists netting hackers L$3.2 million (US$11,500), news first broken by Nobody Fugazi of Your2ndPlace.com. Early reports suggest the banks were all using copies of the same software to manage their deposits.

"From what I gather from my scripter it was ATM coding that didn't check for money in people's accounts before allowing the withdraw," said avatar Barton Giovinazzo of Giovinazzo Choice Investments, one of at least five virtual banks hit by thieves, in an instant message to Reuters.

Other unsuccessful attempts were also made. "Our sites were under sustained attack ... 579 attempts from an IP address in Austin," said Mike Lorrey (Second Life: Intlibber Brautigan). Lorrey's bank, BNT Holdings, fended off the attack with its assets intact. Asked about the impact of the thefts on an in-world financials industry already roiled by high-profile defaults, Corey said "I think it will amp up security for those that survive this."

Online game gets banking licence

Online game Entropia Universe has been granted a licence to be a bank.

Issued by the Swedish Financial Supervisory Authority, the licence means the game can be more closely tied to the real world finances of players.

Mindark, the developers of the game, said it aimed to launch a fully-functioning in-game bank within the next 12 months.

At current exchange rates, 10 PED (Project Entropia Dollars) are worth one US dollar.

Entropia has regularly mixed real and virtual finances.

Unlike many other online games, which charge a monthly subscription fee, the software for Project Entropia is free to download and install.

However, players pay real money to get at in-game items, such as guns, armour and other gear, and the micro-payment system pays for Entropia's running costs.

Samlink

Yhteenveto

- **Tarvitsemme uutta näkökulmaa tietoturvan hallintaan**
  - → Vanhat mallit kyseenalaistettava
  - → Riskien ymmärtäminen ja toiminnan mittaaminen avainasemassa
- **Fokuksena liiketoiminnan ja riskien ymmärtäminen**
  - → Tietoturvan rooli muuttuu edelleen riski- ja liiketoimintalähtöisemmäksi
  - → Ihmisten johtamista teknologian hallinnan sijaan
  - → Ajatusprosessimme rajoittuneisuuden ymmärtäminen parantaa riskiarviointia
- **Vaatimukset ja uhat lisääntyvät**
  - → Toimintaympäristö muuttuu monimutkaisemmaksi ja avoimemmaksi
  - → Tietoturva upotettava arkkitehtuureihin ja sovelluksiin

It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change.
-- Charles Darwin

Samlink