FUJITSU

shaping tomorrow with you

Onko meitä petetty, mihin voi enää luottaa?

TUAMK 4.2.2014

Markku Siltanen
CISA, CGEIT, CRISC, KATAKRI LA

Tietotekniikan kulmakivi?

- Mielestäni koko tietotekniikan kulmakivi on:

  LUOTTAMUS, esimerkiksi

- Siihen, että asiat tapahtuvat niin kuin ne on määritelty tapahtuviksi
- Siihen, että alan toimijat tekevät tehtävänsä niin kuin ovat luvanneet
- Siihen että, tekniikka toimii niin kuin sen on kuvattu toimivan

Kuitenkin tiedämme että

- Tietotekniikan yleistyttyä jokapäiväiseksi ja internetin leviämisen jälkeen on kiinnostus rikolliseen toimintaan ja tiedusteluun lisääntynyt merkittävästi
- Rikollisuutta vastaan on taisteltu jo pitkä tovi ja siitä tietoturvallisuuden ammattilaiset ovat leipänsä myös saaneet
- Tiedustelu taas on mielletty sotilaalliseksi toiminnaksi ja yritysten sekä tavallisten ihmisten silmissä sillä ei ole ollut merkitystä
- Todellisuudessa kuitenkin erityisesti yrityksiin kohdistuvaa tiedustelua on tehty jo varsin pitkän aikaa, myös Suomessa.
- Sekin on ikään kuin ”luonnollista” että yritykset vakoilevat toisiaan ja yrittävät hyötyä siitä

Jo viime vuosituhannella

- 1990-luvulla USAssa säädettiin laki (Clinton), jolla Yhdysvaltain tiedustelupalvelut velvoitettiin auttamaan USAlaisia yrityksiä niiden kilpaillessa mm. eurooppalaisia yrityksiä vastaan, jolloin tehtiin mm. tietomurtoja (EU kauppaneuvotteluiden alla) ja lukuisiin yrityksiin murtauduttiin ja käytettiin saatuja tietoja hyväksi kauppojen voittamiseksi.
- Tehokkaiden salausmenetelmien käyttö estettiin USAssa, koska NSA ei kyennyt purkamaan niitä
- Teknologiaan alettiin upottaa dokumentoimattomia osia ja takaportteja, joita voitiin käyttää hyväksi maailmanlaajuisesti tietomurroissa (niin laitteet kuin ohjelmistotkin)
- Viranomaiset saivat teknologiatoimittajilta avaimet urkintaan ja valtuudet tehdä mitä parhaaksi näkivät
- NSAn resurssit olivat jo 1970-1990 – luvuilla ylivoimaiset, vaikka internetiä ei käytännössä nykymuodossaan edes ollut, silloin tiedot kerättiin vähän nykyistä alkeellisemmin

Näin

Reuters: NSA maksoi tietoturvayhtiölle miljoonia hakkeroimansa salauksen käytöstä

21.12.2013 17:38

Laura Halminen
HELSINGIN SANOMAT

CHRIS HELGREN / REUTER

RSA Securityn kenties tunnetuin tuote on tämä salaustyökalu, joka toimii satunnaisluvuilla. NSA:n väitetään maksaneen RSA:lle, jotta se käyttäisi murrettua salausta toisessa tuotteessaan nimeltä BSafe.

Yhdysvaltojen kansallisen turvallisuuden virasto NSA maksoi tietoturvayritys RSA:lle kymmenen miljoonaa dollaria siitä, että yhtiö käytti tuotteissaan viraston murtamaa salausta, **kertoo uutistoimisto Reuters.**

2000-luku muutti kaiken

- 11.9.2001 jälkeen resurssit eri tiedusteluorganisaatioilla räjähtivät. Niin USA, UK, Venäjä, Kiina, Ranska ja pieni Ruotsikin panostivat verkkotiedusteluun oleellisesti enemmän kuin siihen asti
- Tämä kehitys teki NSAsta erittäin merkittävän toimijan kumppaneineen maailmanlaajuisesti
- SoMe tuli ja jäi haaviin kaikkine applikaatioineen, jolloin tavalliset ihmisetkin olivat terroristien ja rikollisten kanssa samassa tietomassassa.
- Echelon ”paljastui” ja monet muut yritykset imeä viestintätietoa internetistä ja muista kanavista.
- Jne, näitä riittää lukematon määrä

Jo vuosia sitten mm. Microsoft

Microsoft® Online Services

Global Criminal Compliance Handbook

U.S. Domestic Version

March 2008

What are the Various E-mail Services Microsoft Provides?

- Several different domains:
  - @hotmail.com
  - @msn.com
  - @live.com
- Microsoft also provides some country specific domains such as .co.uk, .fr, .it, .de, .es, .th, .tk, .co.jp
  - Currently all e-mail service customer data is stored in the U.S. even if the account name contains a country specific domain.
- E-mail accounts may be either free or associated with a paid service
  - Accounts that start out as paid accounts may later become free ~OR~ accounts that start out as free may later be associated with a paid service.
  - Therefore, the records available in response to law enforcement requests will vary depending on the type of e-mail service.

What are Microsoft Online Services?

- E-mail Services
- Authentication Service: Windows Live ID
- Instant Messaging: Windows Live Messenger
- Social Networking Services: Windows Live Spaces & MSN Groups
- Custom Domains: Windows Live Admin Center & Office Live Small Business
- Online File Storage: Office Live Workspace & Windows Live SkyDrive
- Gaming: Xbox Live

Ei uutta

NSA Follows You With Google's Cookie Trail

The US National Security Agency (NSA) is using Google cookies in order to track potential targets, according to a new report published Dec. 10 in The Washington Post.

The report is based on material leaked by whistleblower Edward Snowden and explains how the NSA uses cookies for their own purposes. Cookies are widely used on the Internet today by advertisers in order to track users, in a bid to customise ads and deliver more personalized user experiences.

No one is surprised

Security experts contacted by *eWEEK* were not surprised by the latest NSA spying revelation.

Robert Hansen, security researcher and director of product management at WhiteHat Security told *eWEEK* that Google's tracking has become so prolific and so accurate that the government can and does now leverage this information for exploitation.

"We have long advocated that Google should not be tracking users in this way for exactly these kinds of reasons; if tracking occurs, it can be leveraged by adversaries," Hansen said. "Really, Google can't help but break people's privacy. It is the foundation of their $40 billion dollar a year advertising business despite the fact that we now know for certain that it can and is being leveraged by at least one set of government actors."

Hansen added that from his perspective, this is the sort of nightmare scenario he and others in the security community have been warning about for years. If you track users at all, it will be used against them at some point.

Mikä on sitten ongelmana?

- Yritykset ja muu yhteiskunta on tullut hyvin riippuvaiseksi internetistä ja siihen liittyvästä tekniikasta
- Tälle osattiin antaa viimeinkin nimi:

CYBERUHKA

- Jonka uskallan väittää syntyneen ihan tarkoituksellisesti, jolloin sitä voidaan käyttää aseena hyvin monessa asiassa. Sen muodostavat valtiolliset voimat, ei hakkerit ja tavalliset ihmiset
- Nyt yhteiskuntia ja yrityksiä voidaan häiritä, tuhota ja uhata esim. Stuxnet tyyppisillä madoilla, mahdollisuudet ovat rajattomat mm.:
  - tietoliikenteen lamauttaminen
  - sähköverkkojen lamauttaminen
  - talouden horjuttaminen, rahaliikenne
  - vedensaannin häirintä
  - liikenteen (ilma, raide, vesi, maantiet) häirintä ja lamauttaminen
- Tämäntyyppisten tilanteiden varalta tiedonkeruu (sirpaletiedot eri lähteistä) on parhaillaankin käynnissä, uskallan väittää…

NSA:n työkalupakki pöyristyttää: "Otteet kuin tieteiskirjallisuudesta"

30.12.2013 21:53

Laura Halminen
HELSINGIN SANOMAT

ANDREW BURTON / REUTERS

Esimerkiksi iPhone voidaan esityksessä esitellyn dokumentin mukaan ottaa haltuun tekstiviestillä tai GPRS-yhteyden kautta.

Miksi?

NSA urkkii videopelaajia – asiantuntija ei yllättynyt

Julkaistu: 13.12.2013 9:14

Google-mainokset

Onko kaikki menetetty?

- Ei mielestäni, jos tilanne ymmärretään oikein
- Luottamus horjuu niihin, jotka ovat osallisia tähän, ongelma ei ole pelkästään USAlaisessa teknologiassa, vaan muutkin nousevat tähdet on syytä noteerata, varsinkin Kiina
- Kaikki jo tehty työ turvallisuuden toteuttamiseksi on hyvä pohja jatkaa tehostamista ja kunnon ratkaisujen toteuttamista
- Toimittajia, tuotteita ja palveluita on syytä tarkastella kriittisesti ja toimia parhaan kyvyn mukaan
- Tiedon suojaaminen on joka tapauksessa avainasia ja tiedon arvon ymmärrys

Tähänkö mennään?

Asiantuntija: Vakoilukohu voi tuhota koko avoimen internetin

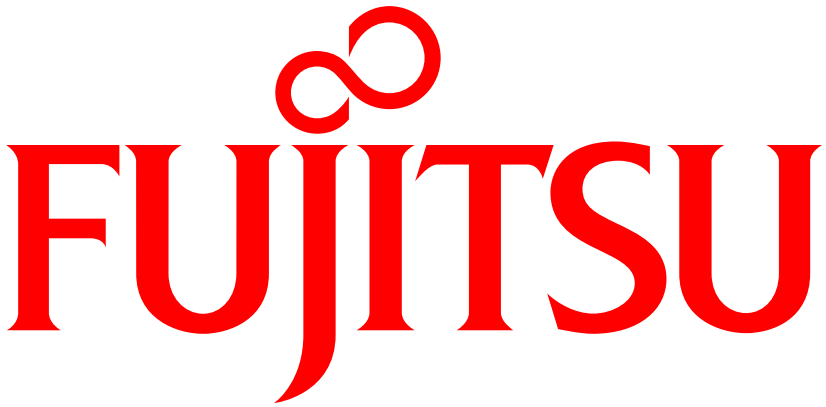
Mikko Hyppösen mukaan vakoiluskandaali voi koitua yhtenäisen Internetin tuhoksi. *Kimmo Mäntylä*

Onko meitä petetty?

- Tähän vastaaminen riippuu siitä mistä päin asiaa katsoo
- ON, jos asiaa katsoo LUOTTAMUKSEN näkökulmasta ja huomioi sen, että suurin osa ongelmista on aiheutettu ihan tarkoituksella, kuten turvallisuustuotteiden ja –tekniikoiden käpälöinti. (SSL salaus, moni muu reikäinen turvallisuusratkaisu, viranomaisten toiminta)
- EI, jos asiaa katsoo vaikka kuluttajan kannalta (s-posti, FB, YT jnee..) kukaan ei ole luvannut niiden koskemattomuutta ja puhtautta. Kuinka moni on lukenut ja sisäistänyt pienellä painetut ehdot, saadakseen painaa ACCEPT nappulaa asennuksessa?
- Itse en ole pettynyt, koska olen ollut asian kanssa sinut jo riittävän monta vuotta, eli minua ei ole petetty

Ihmettelyä…

- Edelleä poimintoja aiheeseen liittyvistä uutisista ja kommenteista, joista osa ollut myös yllättäviä, kuten alan gurujen järkyttyminen näistä paljastuksista.
- Kaikkea ei ole vielä kuultu ja tosiasioiden peittely on käynnissä



shaping tomorrow with you