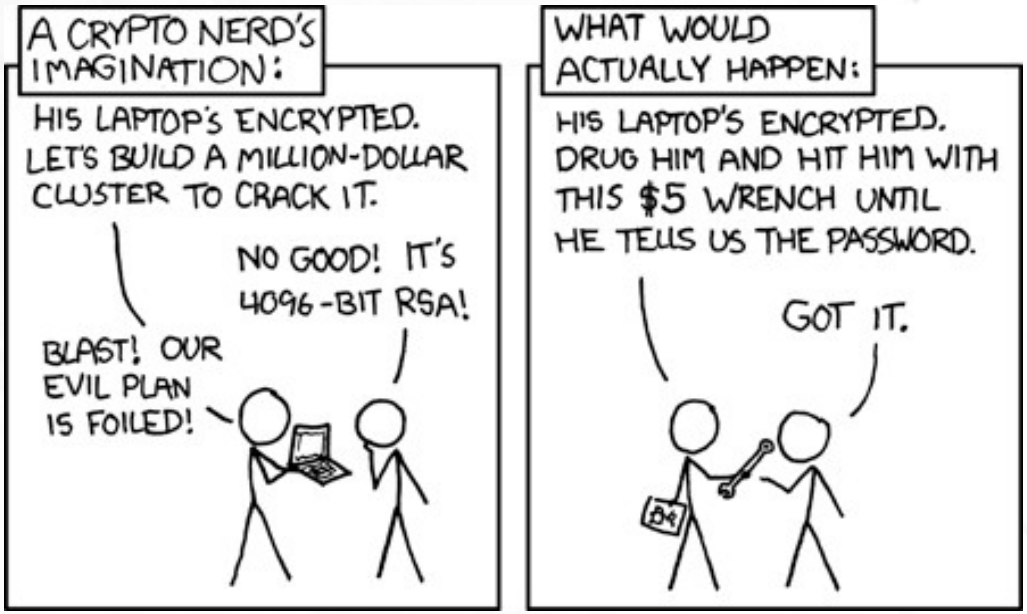
Tietoturvapolitiikka turvallisuuden perusta

TkT Pekka Jäppinen
Lappeenrannan Teknillinen yliopisto
PROSTEK-yhteistyöfoorumi 18.4.2013

Turvallisuus on yhtä vahva kuin sen heikoin lenkki


© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com
SURE, SARAH'S THROUGH THERE - GO STRAIGHT THROUGH
search ID: sha0416
Sid Sly ©M.Hague/S.Harrison 2008


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.


info security
STRATEGY /// INSIGHT /// TECHNIQUE
Home
The Magazine
Advertising/ Lead Gen
Contacts
Links
View UK Content
View US Content
No Preference
infosecurity EUROPE
News
Blog
You are here: Home / News / Nuclear secrets revealed after unencry
News
Nuclear secrets revealed after unencrypted USB stick found in Cumbria hotel room
19 October 2010


Security study – Most government employees fall for planted USB sticks
July 1st, 2011 by Agent Smith (0) DLP,Research and Studies,security breach
Tweet
Share
Curiosity is stronger than any sense of security or any fear of hackers and other malicious individuals, this was the conclusion of a security study run by the US Department of Homeland Security. The study proved how easily hackers and other individuals outside companies can easily go beyond firewalls and other security measures by simply planting USB sticks or computer disks in the right place.


Layer 8
Michael Cooney
Previous Post
Next Post
Stolen NASA laptop held Space Station control algorithms
Encryption has been a bugaboo for NASA for a long time
By Layer 8 on Thu, 03/01/12 - 10:38am.
Mark Rasch, director of network security and privacy consulting for Falls Church, Virginia-based Computer Sciences Corp., told Bloomberg:
"There's no device known to mankind that will prevent people from being idiots."
This is just as good of a conclusion as the old saying: "Curiosity killed the cat."

Tietoturvapolitiikka

- Kertoo mitä kohteita yrityksessä suojataan ja miksi
- Määrittää prioriteetit eli mihin on tärkeää panostaa
  - Pääsy markkinointimateriaaliin tulee taata 24/7
- Toimii tukena turvallisuusratkaisujen valinnassa ja asentamisessa
  - Menetelmien toiminta arvioidaan politiikkaa vastaan

Tietoturvapolitiikka ja henkilöstö

- Politiikan pohjalta luodaan ohjeistus/säännöt henkilöstölle kuinka toimia
  - Opastaa mitä saa tehdä ja mitä ei
  - Kertoo mitä suojataan ja miksi
    - Palvelin huoneen ovi pidetään kiinni koska palvelimet pitävät sisällään yrityksen salaista tietoa
    - Perusteltua kieltoa noudatetaan paremmin kuin perustelematonta
- Henkilöstö voi myös arvioida toimivuutta

Esityö politiikan luonnille

- **Selvitä** mitä kaikkea tietoa yrityksellä on ja **jaottele** omiin ryhmiinsä niiden vaatiman turvallisuuden kannalta. Esimerkiksi:
  - Erittäin salainen: Tuotekehitys ja markkina informaatio
  - Luottamuksellinen: Yrityksen sisäinen kommunikaatio
  - Markkinointi: Tieto jonka halutaan olla helposti saatavilla kaikille

Esityö

- Käy läpi yrityksen laitteisto, jossa tietoa säilytetään ja käsitellään
  - Tietokoneet, kirjoittimet, usb-kynät, paperit
  - Luokittele laitteisto sen mukaan minkä tasoista tietoa niillä käsitellään.
- Käy läpi tilat joissa tietoa säilytetään tai tuotetaan.
  - Työhuoneet, palvelintilat, kytkinkaapit, kahvihuoneet, kopiohuone jne.

Esityö

- Selvitä kuinka tietoa siirretään paikasta toiseen
  - Yrityksen sisällä: paperikopiot, sposti...
  - Ulospäin: verkot, faksit, puhelimet.
- Selvitä kenellä on tarve päästä tietoon käsiksi
  - Johtaja, tutkija, sihteeri, talouspäällikkö, alihankkija
  - Luokittele ihmiset

Esityö

- Selvitä kenellä on pääsy eri tiloihin ja laitteisiin
  - Täsmääkö tilan, laitteen ja ihmisen luokittelu?
- Analysoi nykyinen tilanne
  - Onko selkeitä aukkoja (esim. siivoojalla pääsy erittäin salaisiin papereihin)
- Käy läpi nykyiset turvamenetelmät ja selvitä kuinka ne suojaavat nykytilanteessa.
  - Hidastaako salausjärjestelmä pääsyn reaaliaikaiseen pörssikurssiin.

Tietoturvapolitiikan sisältö

1. Mitä suojataan

- Jaottelu esityön pohjalta esim. Värimalli
  - Punainen: pitää sisällään erittäin luottamuksellista tietoa tai tuottaa toiminnalle kriittisen palvelun
  - Keltainen: pitää sisällää arkaluontoista tietoa tai tuottaa tärkeän palvelun.
  - Vihreä: voi hakea tietoa punaisilta tai keltaisilta koneilta, mutta ei itsessään pidä sisällään arkaluontoista tietoa
  - Valkoinen: Ei pääse hakemaan tietoa punaisilta tai keltaisilta koneilta, ei voida käyttää kuitenkaan oman verkon ulkopuolelta
  - Musta: ulkopuolelta käytettävissä. Ei yhteyksiä.

Tietoturvapolitiikan sisältö

- Linkitetään laitteisto ja niihin pääsy tieto luokituksiin
  - Helpottaa erityisesti pääsynhallinnan arviointia

Kategoria	Verkko	Access	Tarkistus
Punainen	Punainen	Punaisen turvallisuus luokituksen omistajat	Kuukausittain
Keltainen	Punainen ja keltainen	Yrityksen työntekijät	4 kertaa vuodessa
Vihreä	Punainen, keltainen ja vihreä	Työntekijät ja luotetut alihankkijat	Vuosittain
Valkoinen	Valkoinen	Työntekijät ja alihankkijat	Vuosittain
Musta	Musta	Työntekijät, alihankkijat, yleisö	Kuukausittain

Tietoturvapolitiikan sisältö

2. Oikeudet ja velvollisuudet turvallisuuteen liittyen

- Määrittele yleiset oikeudet ja velvollisuudet
  - Vieraita saa tuoda yleisiin tiloihin
  - Politiikka tulee tuntea ja sen mukaan toimia
  - Politiikan ongelmista tulee raportoida

Tietoturvapolitiikan sisältö

- Sekä ryhmien spesifiset oikeudet ja velvollisuudet
  - Ylläpitäjillä on oikeus tutkia turvallisuuslokeja
  - Ylläpidon tulee käsitellä käyttäjätietoja luottamuksellisesti, EU:n yksityisyydensuoja lakien mukaan.
  - Alihankkijat tarvitsevat erillisen luvan turvallisuuspäälliköltä palvelinhuoneeseen pääsemiseksi.

Tietoturvapolitiikan sisältö

3. Oikea käyttö

- Tehtävänä opastaa oikeaan toimintaan
- Ohjeistus kuinka yrityksen verkkoa, laitteita ja tietoa tulee käyttää.
  - Työkoneilla ei käytetä facebookia
  - Työdokumentit vain salattuna USB-tikulle

Tietoturvapolitiikan sisältö

- Erilliseen dokumenttiin tehtäväkohtaiset ohjeistukset
  - Siivoja ei pyyhi pölyjä palvelimen päältä märällä rätillä
  - Vierailija saa yhteyden Internettiin yrityksen julkisen WLAN palvelun kautta. Tunnukset infosta
  - Tutkimusosastolta ei tuoda mitään papereita ulos
- Tarvittava tieto helposti saatavilla

Ohjeita kirjoittamiseen

- Pidä politiikka ymmärrettävänä
  - Lukematon politiikka on turha
  - On vaikea noudattaa politiikkaa jota ei ymmärrä
  - Kun tiedetään mihin säännöt perustuvat, niitä noudatetaan paremmin

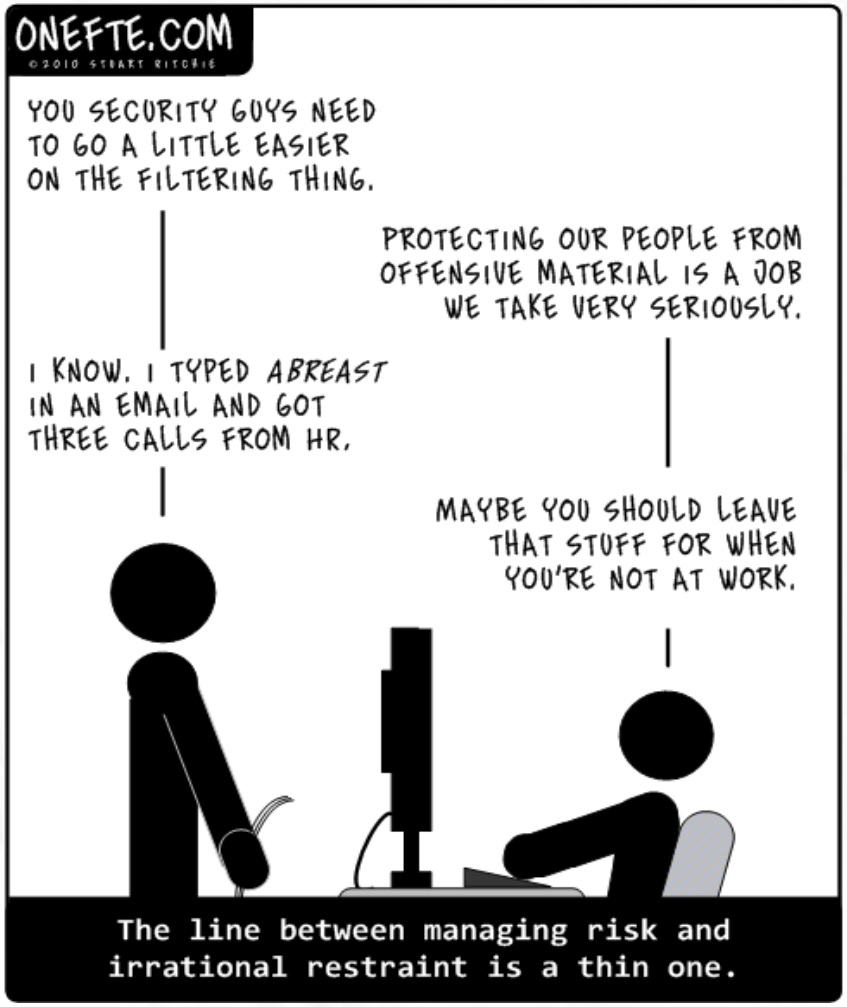
Ohjeita kirjoittamiseen

- Pidä politiikka relevanttina
  - Kukaan ei lue 300 sivuista dokumenttia jossa on kaikki mahdollinen tieto
  - On asioita joita kaikkien ei tarvitse tietää
    - Turvallisuusihmiset tarvitsevat enemmän tietoa kuin esimerkiksi sihteeri
  - Eri ihmisille voi olla erilainen dokumentti, joka koskee vain heille oleellisia asioita tietoturva-politiikasta.

Teesit Tietoturvapoliikkaan

- Hyvä polittiikka nyt on parempi kuin loistava politiikka ensivuonna.
- Heikko politiikka joka on jaettu kaikille on parempi kuin vahva joka ei ole kellään.
- Yksinkertainen politiikka jonka kaikki ymmärtävät on parempi kuin monimutkainen ja hämmentävä jota kukaan ei viitsi lukea.
- Politiikka joka muokkautuu ajan myötä on parempi kuin politiikka, joka muuttuu ajan myötä turhaksi.
- Politiikkaa määrittäessä on usein on parempi pyytää anteeksi kuin odottaa lupaa

Varo ylilyöntejä



Kysymyksiä/keskustelua?

- Olisiko tietoturvapolitiikka auttanut alussa esitettyihin tapauksiin?