

Tietojärjestelmien itsepuolustus Reaktiivisuudesta ennakointiin

*IBM Tietoliikennepalvelut
Sami Kuronen, CCIE#4522*



Agenda



- ▶ IBM ja Cisco -lyhyt historiikki
- ▶ Tietoturvaratkaisujen haasteet
- ▶ Ciscon visio tietoturvasta
- ▶ IBM ja Cisco -yhteistyö
- ▶ Yhteenveto

Agenda



- ▶ IBM ja Cisco -lyhyt historiikki
- ▶ Tietoturvan toteuttamisen haasteet
- ▶ Ciscon visio tietoturvasta
- ▶ IBM ja Cisco –yhteistyö
- ▶ Yhteenveto



Lyhyt historiikki



IBM luopui omasta teknologiasta '99

04/1999

- AT&T ostaa IBM Global Network:n

IBM:stä tietoliikenteen järjestelmäintegraattori

2001

- Cisco Gold Partner – status Euroopassa

IBM:stä maailman suurin Cisco –yhteistyökumppani. Suomessa Gold -sertifiointi

21/2001

- IBM:stä maailman suurin Cisco -kumppani

09/1999

- Cisco Systems ostaa IBM Networking Hardware Division:n

2000-2002

- IBM kehittää osaamistaan ja hankkii yhteistyökumppaneita

10/2002

- Suomessa Cisco Gold Partner -status



Agenda



- ▶ IBM ja Cisco -lyhyt historiikki
- ▶ Tietoturvan toteuttamisen haasteet
- ▶ Ciscon visio tietoturvasta
- ▶ IBM ja Cisco –yhteistyö
- ▶ Yhteenveto



Avoimuuden tuomat haasteet



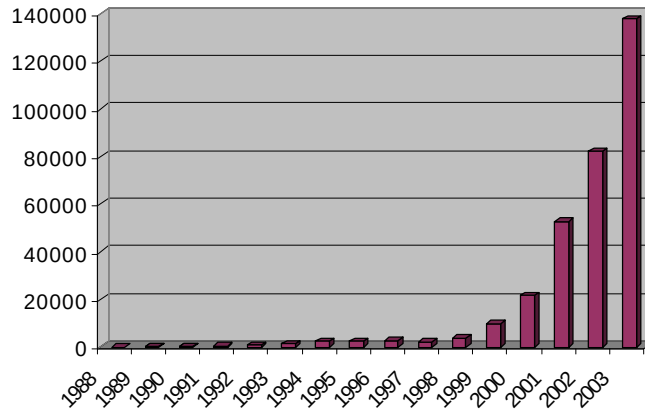
- ▶ Yritysten ja yhteisöjen **tulee avata** tietoverkkonsa ja palvelunsa asiakkaille, kumppaneille ja toimittajille
- ▶ Yrityksen **tulee estää** haitallisten käyttäjien/ohjelmien tunkeutumiseen verkkoon ja järjestelmiin



Ja samaan aikaan...



Tietoturvaloukkausten määrä kasvaa huimaa vauhtia!!



CISCO SYSTEMS
CORPORATE
ALLIANCE

Lähde: www.cert.org

IBM

Ja vielä lisäksi...



1980-1990
Oli viikkoja tai kuukausia aikaa hoitaa suojaus



2000-2002
Hyökkäykset kehittyivät ja niiden vaikutus oli huomattavissa tunneissa



2003-
Hyökkäykset siirtyivät **sekuntien** vaikutusaikaan

Puolet siitä ajasta, jonka käytit tämän kalvon lukemiseen riittää tukkimaan koko verkkosi ja kaikki sen sovellukset!!

SQL Slammer mato:
Tuplantuminen joka 8,5 sekunti
3 minuutissa : 55M skannausta/sek
1Gb linkki **saturoitui** minuutissa

SQL Slammer oli varoitus.
Uudet "turbomadot" voivat olla vieläkin nopeampia.

CISCO SYSTEMS
CORPORATE
ALLIANCE

IBM

Millä toteutan tietoturvan?



- ▶ Sopivan tietoturvaratkaisun valitseminen, toteuttaminen ja ylläpito on haaste
 - **Kustannustehokkuus** on oleellisen tärkeää
 - **Kuka integroi** eri tietoturvan toteuttamiseen vaadittavat komponentit?
- ▶ Tämän lisäksi prosessit ja politiikat tulee olla kunnossa
- ▶ Ja tämäkään ei vielä riitä...



Eli tarvitaan koulutusta!!



Lähde: Tietoviikko 22.4.2004

TIETOVIIKKO

Vastauksia.
Nokia 6600 -puhelin.

Tuolla >>

Talentum.com > Tietoviikko > Viikon uutiset

☐ ETUSIVU
☐ UUSIN LEHTI
☐ MIELIPIDE
☐ IT-KATSAUS
☐ BAROMETRI
☐ 250 SUURINTA
☐ TIVI MOBILE
☐ YRITYSTIEDOTTEET
☐ KESKUSTELU
☐ PALKKATUTKIMUS

☐ **VIIKON UUTIS**

Salasanan saa suklaapatukalla

[Kauko Ollila 22.4.2004, 07:39]

Toimistotyöntekijät eivät ole edelleenkaan kovin tietoturvaan suuntautuneita. Lontoolaisen katukyselyn perusteella on ihme, että asiat tietojärjestelmissä eivät ole paljon paremmiin.

Infosecurity Europe -tietoturvatapahtuman toimeksiannosta tehtiin katukysely Lontoolaisella Liverpool Streetin metroasemalla. 172 kulkijaa vastasi muutamaa työpäivän tietoturvaan liittyvään kysymykseen. Haastattelijat kysyivät ihmisiltä muun muassa näiden työpäivän tietokoneen salasanaa.

Peräti 38 prosenttia vastaajista kertoi salasanaan sitä kysyttäessä. Toinen 34 prosenttia paljasti sen, kun tuihtuntematon kysyjä totesi jotain sellaista kuin "lyön vaikka vetoa, että se liittyy lapsesi tai lemmikkisi nimeen."

Suklaapatukalla olisi saanut salasanan 71 prosentilta vastaajista.

"Admin" on yleisin salasana

Oma perhe oli yleisin salasanan perusta, käytössä 15 prosentilla haastateluista. Seuraavina suosikkilistalla olivat jalkapallojoukkueet (11 prosenttia) ja lemmikit (8 prosenttia).

Kaikkein yleisin yksittäinen salasana oli "admin".

Kun kysyttiin, antaisivatko vastaajat salasanaan jollekulle, joka kertoo soittavansa työnantajan IT-osaston nimissä, 53 prosenttia

Palvelinympäristöjen kokonaiskustannukset (€)

Yritystiedot tarjoaa	Haku:
Suomesta	
Tietoviikosta	

Lähde: IDC
Pohjois-Amerikan markkinat

Lue koko tutkimus

Toimitus
[Mediatiedot](#)
[Tilaa Tietoviikko](#)
[Osoitteenmuutos](#)
[Palvelulahakemisto](#)
[Palauta](#)



Agenda



- ▶ IBM ja Cisco -lyhyt historiikki
- ▶ Tietoturvaratkaisujen haasteet
- ▶ Ciscon visio tietoturvasta
- ▶ IBM ja Cisco –yhteistyö
- ▶ Yhteenveto



Ciscon tietoturvavisio



- ▶ Tarvitaan **automatisoitu** tietoturvajärjestelmä ennalta arvaamattoman uhan torjumiseen
 - *Reaktiivisten prosessien kustannushaaste*
 - *Reaktiivisuudella ollaan yleensä myöhässä*
- ▶ Tietoturva otettava käyttöön **useilla kerroksilla** järjestelmässä
 - *Vastaamaan monitasoisiin uhkakuviin*
 - *Puolustamaan kompleksisia hyökkäyksiä*
- ▶ Kaikki tietoturvan elementit pitää olla **integroituna**, jotta saadaan hallittu vaste hyökkäyksille



Ciscon tietoturvväisio – Itsepuolustautuva verkko



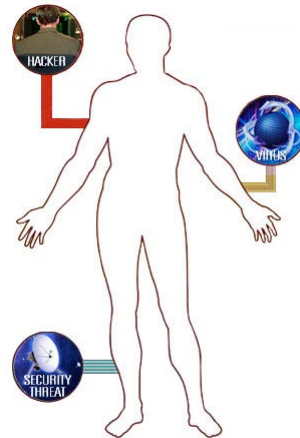
IBM liittyi hankkeeseen 13.2.2004



Ciscon tietoturvväisio – Analogiaa



- ▶ IT-infrastruktuurin ja verkkojen pitää toimia kuin elävät organismit
- ▶ Virukset ovat osa jokapäiväistä elämää
 - Kannamme niitä mukana
 - Ne leviävät erilaisten kontaktien välityksellä
- ▶ Ihmiskeho toimii kokonaisuutena vaikka kannamme viruksia ja tauteja

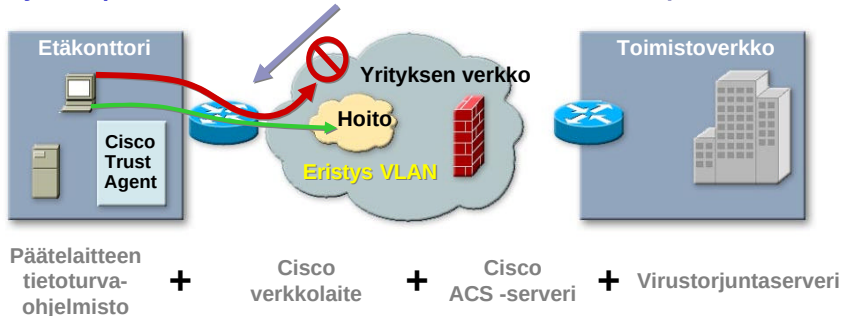


Ciscon tietoturvasisio – Toimintaperiaate



**Cisco Network Admission Control (NAC) on koko
Cisco Self-Defending Network-arkkitehtuurin perusta.**

1. Epäkelpo päätelaite yrittää päästä verkkoon
2. Eristys ja hoito
3. Saastuminen ei leviä muihin päätelaitteisiin



Agenda



- ▶ IBM ja Cisco -lyhyt historiikki
- ▶ Tietoturvaratkaisujen haasteet
- ▶ Ciscon visio tietoturvasta
- ▶ IBM ja Cisco –yhteistyö
- ▶ Yhteenveto



IBM ja Cisco – tunnetut tietoturvatoimittajat (1)



Panostukset tietoturvan hallinnan tuotteissa ja tietoturvapalveluissa

- Käyttäjien ja käyttöoikeuksien hallintajärjestelmät
- Tietoturvapalvelut
- Kannettavien ja pöytäkoneiden sisäänrakennetut turvaominaisuudet
- Palvelinlaitteiden sisäänrakennetut turvaratkaisut

Panostukset tietoturvatuotteissa

- VPN:t
- Palomuurit
- Hyökkäysten tunnistus ja esto
- Päätelaitteiden tietoturva



Asiakkaat odottavat kattavia ratkaisuja tunnetuilta valmistajilta



IBM ja Cisco – tunnetut tietoturvatoimittajat (2)



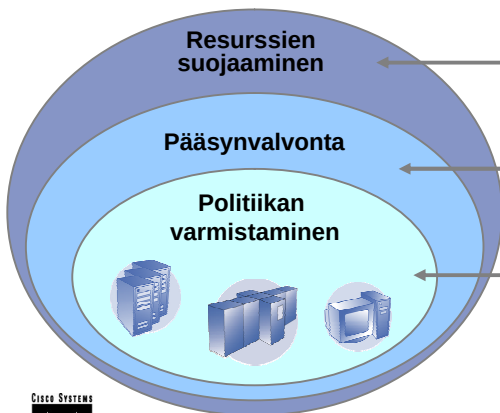
- ▶ Huomasimme, että IBM:n ja Ciscon ratkaisuissa on paljon samaa
- ▶ Ne ratkaisevat samaa ongelmaa, mutta näkökulma oli eri
 - Ciscon vahvuutena verkon turvaaminen
 - IBM:n ratkaisu lähestyy asiaa sovellusten, järjestelmien ja prosessien näkökulmasta



IBM ja Cisco – yhteistyöllä integroitua tietoturvaa



IBM and Cisco
Tarjoaa tietoturvaa
monelle kerrokselle



CISCO SYSTEMS
CORPORATE
ALLIANCE

Resurssien suojaaminen

Suojaa verkko ja tietokoneet

- Tunne verkossa olevat laitteet
- Evää epäkelpo yritys verkkoon
- Suojautu viruksia vastaan
- Varautu tietoturvaloukkauksiin

Pääsynvalvonta

Suojaa käyttäjät, sovellukset ja data

- Tunne luvalliset käyttäjät
- Kontrolloi käyttäjiä ja heidän tekemisiä
- Suojaa transaktiot ja data
- Tee tietoturvasta läpinäkyvä käyttäjille

Poliitiikan varmistaminen

Takaa eheys ja luottamuksellisuus

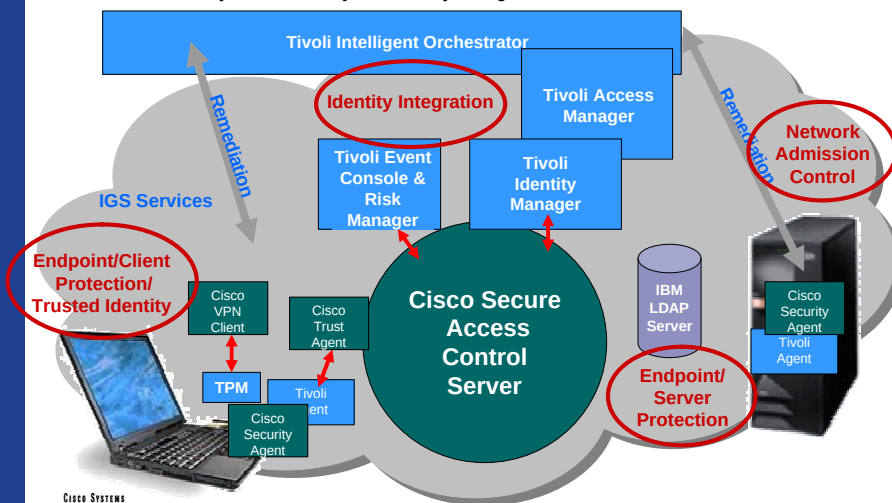
- Huomioi viranomaismääräykset
- Pakota yhdenmukaiset politiikat
- Integroitu audit trail
- Tietoturvariskien hallinta

IBM

Järjestelmäarkkitehtuuri



Life-Cycle User Identity and Security Management



CISCO SYSTEMS
CORPORATE
ALLIANCE

IBM

Järjestelmäkomponentit



- ▶ **Tivoli Intelligent Orchestrator**
 - *IT-infran keskitetty hallintäjärjestelmä*
- ▶ **Tivoli Event Console & Risk Manager**
 - *sovellus tapahtumien ja tietoturvaloukkausten hallintaan*
- ▶ **Tivoli Identity Manager**
 - *hallintasovellus käyttäjätunnusten luomiseen ja työvuon/prosessin automatioon*
- ▶ **Tivoli Access Manager**
 - *sovellus end-to-end - pääsynvalvontaan*
- ▶ **Tivoli Agent**
 - *Tivoli-arkkitehtuurin työasemasovellus*
- ▶ **Trusted Platform Module**
 - *kannettaviin integroitu tietoturvapiiri käyttäjätunnisteen tallennukseen*



Järjestelmäkomponentit



- ▶ **Cisco VPN Client**
 - *VPN-työasemasovellus turvallisia etäyhteyksiä varten*
- ▶ **Cisco Trust Agent**
 - *työaseman turvatietoja ylläpitävä sovellus (esim. antivirus-päivitysten ajanmukaisuus)*
- ▶ **Cisco Security Agent**
 - *IDS-funktion toteuttava työasemasovellus*
- ▶ **Cisco Secure Access Control Server**
 - *keskitetty Cisco-verkkolaitteiden tietoturvaominaisuuksien hallintasovellus*



Mitä hyötyä tästä sitten on?



- ▶ Yhtenäisellä tietoturvaratkaisulla saadaan katettua koko IT-infrastruktuuri verkoista päätelaitteisiin, palvelimiin ja sovelluksiin
- ▶ Yhtenäistämällä uhkien torjuntaan ja käyttäjien hallintaan liittyvät hallintaratkaisut voidaan pienentää operointikustannuksia



Agenda



- ▶ IBM ja Cisco -lyhyt historiikki
- ▶ Tietoturvaratkaisujen haasteet
- ▶ Ciscon visio tietoturvasta
- ▶ IBM ja Cisco –yhteistyö
- ▶ Yhteenveto



Yhteenveto



- ▶ Tietoturva-vaatimusten kehitys vie eittämättä kohti ennakoivia ratkaisuja
 - *reaktiivisuudella ollaan valitettavan usein myöhässä*
- ▶ Yhtenäisellä ratkaisulla saadaan monia etuja
 - *kustannussäästöjä operointikustannuksissa*
 - *vähennetään itse tehtävää integrointitarvetta*



Mietittävää...



- ▶ Kumpi on vaarallisempaa terveydenhuollossa/sairaalamailmassa
 - *sairaalebakteeri vai*
 - *tietokonevirus/mato?*
- ▶ Mikä on tilanne nyt vs. viiden vuoden kuluttua?

