Käytännön tietoturvan historia 1960 - 2023

Käytännön tietoturvan koko historia pähkinänkuoressa

Kristian Salmi Tietoturvavastaava (EVP) 20.03.2023

Kuka Kristian Salmi?


CLARITAS SECURITY CONSULTING

Asiakkaidensa toiminnan turvallisuuden ja laadun kehittämiseen erikoistunut yritys.

Turvallisuutta ja laatua

"Claritas tarkoittaa kirkkautta, selkeyttä ja johtajuutta - tulkitsemme kansainvälisetkin standardit ja mallit ymmärrettäviksi ja selkeiksi palveluiksi.

Claritas on v. 1993 perustettu asiakkaidensa toiminnan turvallisuuden ja laadun kehittämiseen erikoistunut yritys. Sen asiakaskunta muodostuu pääasiassa suurista ja keskisuurista yrityksistä, valtion- ja kunnallishallinnon virastoista sekä alan sertifiointi- ja koulutusorganisaatioista ja järjestöistä.

Mikäli etsit ammattitaitoista, vastuullista ja kokenutta osaajaa, olet oikeassa osoitteessa!"

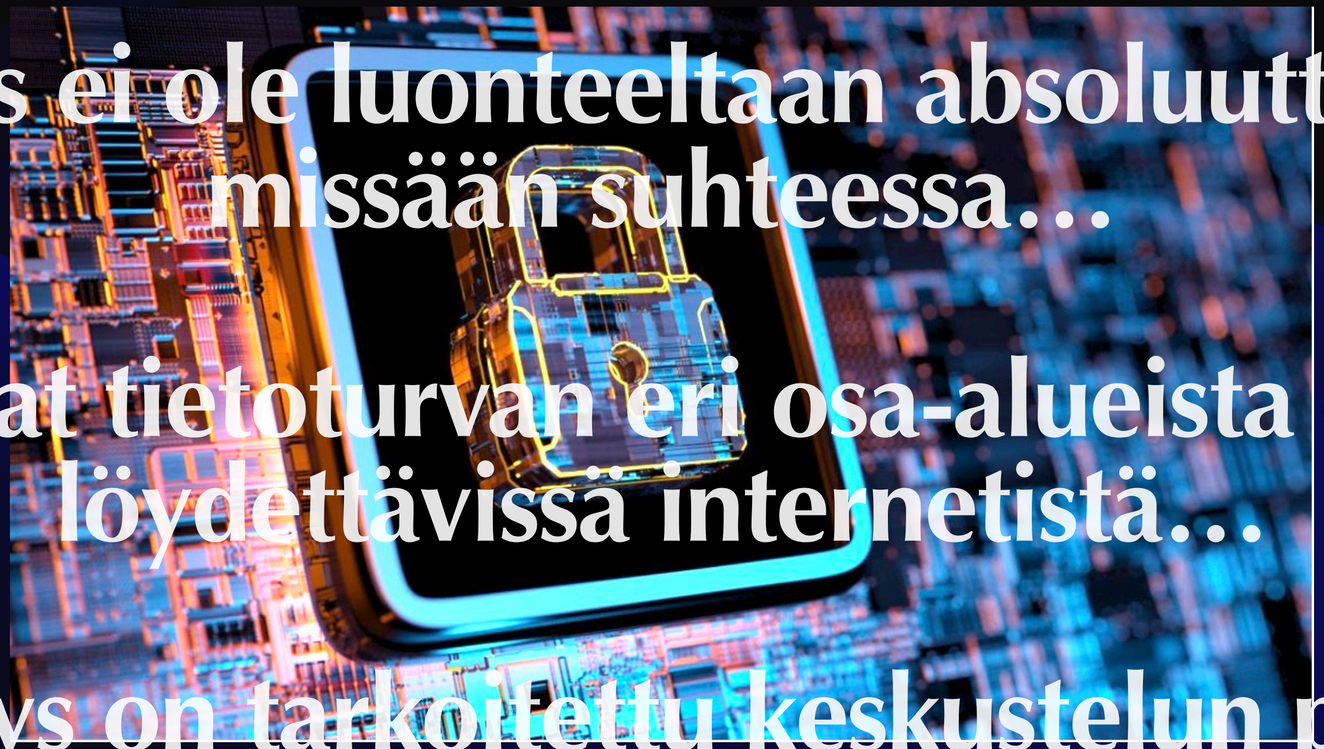
Claritasin pääasialliset toimintamuodot ovat konsultointi, arviointi/tarkastus/auditointi ja koulutus.

Toiminnan lähtökohtina ovat asiakkaiden tarpeet, ammattietiikka, toimialan säädökset ja määräykset sekä kansainväliset ja kansalliset standardit ja mallit, kuten ISO 9000, ISO 20000, ISO 27000, ISO 31000, ISO 38500, COSO, COSO ERM, CMMI, COBIT, GTAG, ITIL, ITAF, PMBOK, P3M3, BS 25999, SoGP, ISM3, JHS, Vahti, Tietoturvataso, KATAKRI, SOPIVA,...

- Peruskoulu Ratakadun kansakoulu + Svenska Normallyceum
- Taloushallinnon merkonomi monimuoto-opiskeluna 1997-2000
- Kielitaito Ruotsi Suomi Engalnti
- VR ryhmäön johtaja Alik. Erikoiskoulutus TSTO AU (Dragsvik)
- 1974 VTKK
- 1975 Konttoritekniikan parissa huolto ja asiantuntija tehtävissä (Rank Xerox)
- 1993 MMM tietopalvelukeskus mikrotukihenkilönä
- 2002 Microsoft 2000 sertifioitu
- 2007 VM-ware 3.7x koulutus
- Kasvintuotannon tarkastuskesus 1993 - 2006 atk suunnittelijana
- EVIRA 2006 - 2011atk suunnittelija, tietoturva otona
- Turvallisuus ja kemikaalivirasto 2011- 2020 tietoturvavastaava
- 2012 ITIL 3.0 sertifioitu ja CISA ja CISM koulutus

- -> Tehnyt kaikkia ICT töitä (paitsi ohjelmointia)
- ->Tietoturvatyö alkanut otona EVIRA:ssa 2000 luvulla (Claritas Kari Pohjola)
- -> Päätehtävänä Tukesissa mm. Teknisenä yhteyshenkilönä ECHA:n

Tästä esityksestä…



Tämä esitys ei ole luonteeltaan absoluuttisen tarkka missään suhteessa…

Esitetyt asiat tietoturvan eri osa-alueista ovat kaikki löydettävissä internetistä…

Tämä esitys on tarkoitettu keskustelun pohjaksi…

1960 - 1980 luku

Alussa automaattinen tietojen käsittely oli harvojen ja valittujen käsissä

Suurin, valtaosa ihmisistä eivät siihen aikaan ymmärtäneet tietämys-koneiden päälle yhtään mitään

Laitteistot olivat isoja ja vaativat paljon vettä ja sähköä sekä erikois-tilat

Koko paletti oli erikois koulutettujen henkilöiden käsissä

Turvallisuus oli edellä mainituista syistä johtuen ”itsestään selvyys”

Tietoturva ei ollut / koettu ongelmana…

1990 - 2000 luku
PC:n valtakausi alkoi

Paikallisverkot

LAN - WAN - MAN

IBM - XT edusti tässä henkilökohtaisen tietojenkäsittelyn kanta isää
(**ei verkkoyhteyksiä**)

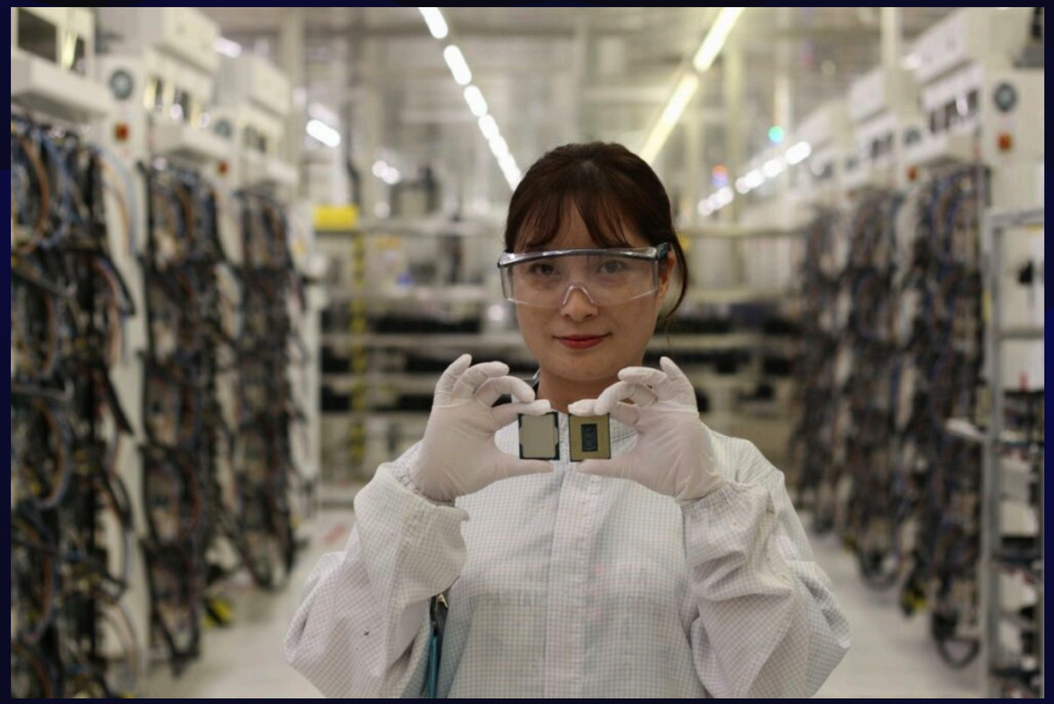
IBM - AT edustaa henkilökohtaista tietokonetta joka kytkettiin verkkoon
(**CSMA AUI - Token ring - 3-com Ethernet**)
ja siinä oli kovalevy (-**Seagate -Winchester**) johon käytettävät ohjelmat ja verkon asetukset voitiin asentaa pysyvästi

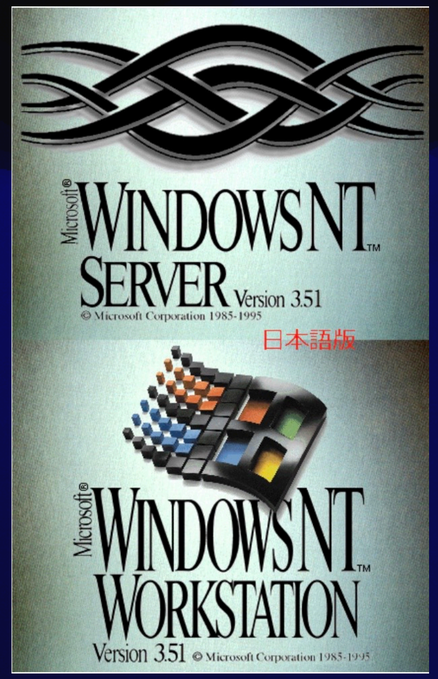
Ensimmäiset haittaohjelmat ilmaantuivat myös Suomen tasolle

Käytössä olleiden levykkeiden (**Verbatim, Parrot**) mukana (jopa asennusmedioissa) seurasi ensimmäiset haittaohjelmat!

Sen sai helposti pois alustamlla levykkeet uudelleen ennen käyttöä.
Kovalevyllä sijaitseva Autoexec.bat tiedostosta poistamalla osoituksen haittaohjelmaan poisti esim. ’palo-auton’ kovalevyltä

2000 luvun vaiheilla
1996 - 2005





Win - tel yhteistyö, asiakkaan parhaaksi?

Microsoft teki ’uuden’ käyttöjärjestelmän (yhdistelmän) > Intel teki uuden emolevyn prosessoreineen joka kolmas vuosi

+ Microsoft käyttöjärjestelmän grafisuudesta johtuen monet ei ATK ihmiset pystyivät omaksumaan tietämys koneen (PC:n) käytön.

+ PC:n hinta suhteessa tehoon laski

+ Muisti ja suorituskyky tuplaantui joka vuosi (Mooren laki)

- *Sekä kovalevyjen että emolevyjen ja VLSI piirien sekä käyttöjärjestelmistä että ohjelmien tietoturvasta ei välitetty (no worries)*

Virustorjunta ohjelmistot

Yleistyivät ja valveutuneimmat jopa pakollistivat ohjelmiston käytön verkkotyöasemissa 1997 luvun jälkeen

Myöhemmin virustorjunta ohjelmistot ilmestyi konehuoneisiin ja palvelimiin

Palomuurit ja IDS ja PAM yleistyivät

Verkkojen segmentointi ja tietoliikenteen kahdentamiset yleistyivät

Silti rikolliset näytti (ja näyttää vieläkin) olevan meitä koko ajan edellä……

Mistä ja miten rikolliset tulivat tietotekniikkaan?

-> Vaikutusvaltaisten ohjelmistotalojen työntekijät osasivat nähdä tulevaisuudet ***eri tavalla kuin talon omaksuma business-linja*** (***MS - Oracle - HP - IBM***)

-> Poikkeavat yksilöt *'poistettiin'* ja *'hilkulla'* olevat ostettiin pois kilpailijoille

-> Rikolliset halusivat myös investoida tietotekniikkaan ja ostivat nämä *'toisinajattelijat'* tekemään heille työtä ja rahaa

-> Samalla myös ohjelmistotalojen tuotteet tuotiin raakileina markkinoille,niitä ei oltu testattu tarpeeksi, niissä ei välillä ollut tietoturvasta tietoakaan siitä seurasi se, että rahan (omaisuuden) ja kriittisen tiedon anastaminen, oli helppo toteuttaa

Mitä 'työkaluja' rikolliset ovat käyttäneet aikojen alusta?

-> Tutkivat sattuman ja erehdyksien kautta asiakkaiden käyttämiä työkaluja omaisuutensa (assets) hallintaan verkossa

-> Toimivat täysin epäloogisesti (irrationaalisesti) tiedon syötössä ja kyselyissä

-> Tekevät (vuosikaudet) töitä löytääkseen heikot kohdat (APT)

-> Hyödyntävät murrettuja kohteita kaikessa hiljaisuudessa pitkän ajan

-> Kun lähde 'ehtyy' ilmoitetaan tietoturva aukosta, ja seurataan paikko-operaatioita.

- Tietorikolliset ovat hyvin perillä mm. **ISO 27000 ja PCI-DSS** standardeista ja niiden vaatimuksista

-> osaavat hyödyntää niitä omiin tarkoituksiinsa

Muutamia tietotuvan virstanpylväitä
(Ehkä satunnaisessa aika järjestyksessä)

- Brain.**A(ensimmäinen IBM PC haittaohjelma?)**
- **APT** = **A**dvanced **P**ersistent **T**hreat (10 - 75?)
- **Rootkit** haittaohjelmat
- **Macro virukset** (.DOC ja .XLS)
- **Stuxnet**
- **Cryptolocker**
- **Solarwind**
- **Phising eri muodoissa**
- Chat**GTP**

Lähteet

=> Technopedia
=> Techrepublic
=> Deloitte, KPMG, NIXU, With-Secure
=> MC Afee, Symantech
=>WSJ, MIT Tech
=> The Hacker News, Bleeping Computer
=> ZDNet, China News
=> CISA, ISO, NIST, Enisa
=> ISACA, Cobit

Suosittelemani kirjat :

Mary Aiken: The cyber effect (2014)
Mikko Hyppönen: If it's smart it's vulnerable(2021)
Jim Collins: Good to Great (2001)

Keskustelua

”Virus ja haitta ohjelmien torjunta, hävittäminen sekä ICT kokonaisuuden saavuttama haitta ohjelma resilienssi on tänä päivänä hyvinkin siedettävällä tasolla. Lepsuiluun ei ole kuitenkaan yhtään varaa”