Tietoturvan nykytila tietoturvaloukkausten näkökulmasta

Jussi Eronen

Erityisasiantuntija

CERT-FI

Tietoturvaloukkausten trendejä == Kestoaiheita

- Kohdistetut hyökkäykset
- Haavoittuvien palveluiden murrot suuressa mittakaavassa
- Suuret yksityisyystietojen vuodot
- Internet-rikollisuuden koko ketju
- Verkkoilmiöt: palvelunestohyökkäykset, reitityskaappaukset, ...

Keskeisiä haasteita

- Tietoturvaloukkausten ja uhkien havaitseminen
- Tietoturvaloukkauksista toipuminen
- Oman järjestelmän ja sen tilan ymmärtäminen
- Infrastruktuurin ymmärtäminen
- Turvallinen järjestelmäkehitys

Tietoturvaloukkausten havaitseminen

No silver bullet

Ratkaisujen historiaa (sarkasmivaroitus)

	Introduced	Comment
DRM	1970	Securing who and what?
AntiVirus	1987	less than 70% effective, more than 30 days late?
FireWall	1988	First we lost network perimeter, now with cloud apps the host perimeter?
IDS	1992	Capitalizing noise?
VPN	1994	Bubble gum perimeters
WebFilter	1994	Political security or censorware?
SecurityScanners	1995	Canned (known) vulnerabilities
EmailFilter	1997	Necessity against canned spam, failure as censorware (world moved on)
IPS	1998	Nobody had time to read IDS logs
SIEM	1999	Still nobody had time to read FireWall, IDS, IPS, ... logs
WebAppSecurityScanner	2000	Spidering the wild wild west of sheer attack surface
VulnerabilityManagement	2002	Nobody had time to deal with the findings (vulnerabilities)
UTM	2004	Nobody had time to deal with any add-on-security
DLP	2007	Couldn't stop them getting in, will trip them on their way out

Tuloksettomia tutkimussuuntia

- Yksinomaan tuotteisiin perustuva tietoturva
  - » Hyökkääjä voi aina ostaa saman tuotteen ja varmistaa, ettei hänen hyökkäystään huomata
- Hyökkäysten automaattinen löytäminen verkkoliikenteestä
  - » Useat tutkimukset ovat väittäneet onnistuneensa tässä jollakin testiaineistoilla. Miksi tulokset eivät näy nykyisissä tuotteissa?
- Simuloidut hyökkäysaineistot
  - » Internet on täynnä oikeita hyökkäyksiä ja hyökkääjiä

Toimiviksi havaittuja keinoja

- Havaintovälineiden yhdistäminen ja havaintojen rikastaminen kontekstitiedolla
- Ylläpitäjien tai SOC-toimijoiden kyvykkyys
- Aktiivinen tiedonvälitys (IoC, Indicators of Compromise)
- Aktiivinen havainnointi
  - » Tunnettujen tekijöiden seuranta
  - » Haittaohjelma-analyysi
  - » Hyökkääjän infrastruktuurin seuranta

Tietoturvaloukkauksista toipuminen

Non scholae sed vitae discimus

Tietoturvaloukkaushavainnon jälkeen

- Prioriteetit uhrin näkökulmasta: toiminnan jatkaminen turvallisesti ja vahinkojen korjaus
- Vahinkojen arviointiin tarvitaan kyvykkyyksiä
  - » Haittaohjelma-analyysi
  - » Verkkotekniikka
  - » Forensiikka
- Toiminnan jatkaminen
  - » Turvalliset käyttötapaukset
  - » Toipumissuunnittelu

Järjestelmäymmärrys

Internet, tietotekniikan villi luonto

Määrittelyä kaipaavia termejä

- Analyysi
- Korrelaatio
- Kollaboraatio
- Tilannekuva

Nykyinen ICT-ympäristö

- Järjestelmät eivät ole itsenäisiä
- Kokonaan omassa hallussa oleva infrastruktuuri on harvinaisuus
- Riippuvuuksia muihin toimijoihin ei voida poistaa
- Internet on ympäristönä kompleksinen, hankalasti hallittava ja pitkälti vihamielinen
- Välineet itsenäiseen toimintakykyyn tärkeitä

Infrastruktuurin ymmärrys

- Verkkojen skannausprojektit ovat hyvä alku
  - » Eivät itsenään saata tilannetta kuntoon
- Kompleksisuudet ovat kuitenkin syvemmällä
  - » Alihankkijat, reititys, operaattorit, ylävirrat, kaapelit, maantieteelliset sijainnit, lainsäädännölliset alueet, ...

Turvalliset järjestelmät

Build security in

Tutkimuksesta tuotantoon

- Ohjelmistoturvallisuuteen on ratkaisuja, mm.
  - » Turvalliset ohjelmointikielet
  - » Turvalliset kääntäjät
  - » Valmiit kirjastot ja kehykset
- Järjestelmien turvalliseen rakentamiseen on ratkaisuja, mm.
  - » Käyttöoikeuksia rajoittavat järjestelmätason keinot
  - » Hiekkalaatikkoympäristöt
  - » Haavoittuvuuksien hyväksikäytön hankaloittaminen
- Olemassa olevien ratkaisujen käyttöönotto

Loppusanat

"Nyt kaikki nörttäämään"

- Tietoturvaloukkausten havainnointi kuntoon
- Kyvykkyys tärkeässä osassa kaikissa turvaamisen vaiheissa ja tehtävissä
  - » Välineet avustavassa roolissa
- Nykyisen osaamispotentiaalin aktivointi
  - » Oppilaitosten lisäksi harrastetoiminta tärkeässä roolissa
- Itsenäisen toimintakyvyn säilyttäminen monimutkaisessa ympäristössä muuttuvaa uhkaa vastaan

cert-fi
Viestintävirasto

www.cert.fi
www.viestintävirasto.fi