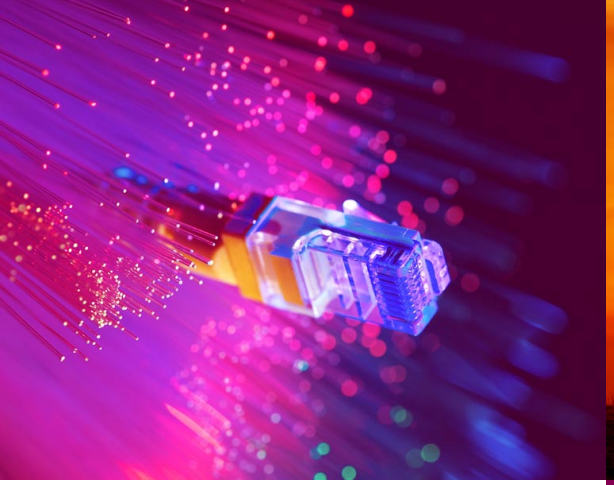


Tietosuojavaatimusten tietoturvallinen toteuttaminen käytännössä

Korkeakoulujen IT-päivät 2018-11-06

Urpo **Kaila**, tietoturvapäällikkö, urpo.kaila@csc.fi

CSC – Suomalainen tutkimuksen, koulutuksen, kulttuurin ja julkishallinnon ICT-osaamiskeskus

HELSINGIN SANOMAT

Tilaa Hesari Kirjau

PÄIVÄN TIMANTTI: Pienellä joukolla on yhteensä satojen miljoonien eurojen ulosottovelat – Ja yksi heistä on omilla luvuillaan

Kotimaa

Tuhansien ylioppilaskirjoituksiin osallistuneiden tiedot pääsivät vuotamaan verkkoon – ”Uhrien oikeudet eivät toteudu”, sanoo tietosuojavaltuutettu

Verkkosivuyhtiön palvelimella ollut tietosuojapuute on aiheuttanut sen, että 7000 suomalaisen ylioppilaskokelaan henkilötietoja on vuotanut internetiin. Lautakunta on tapahtuneesta pahoillaan.

Miten voimme välttää tietovuodot?

HELSINGIN SANOMAT

Tilaa Hesari Kirjaudu

PÄIVÄN TIMANTTI: Pienellä joukolla on yhteensä satojen miljoonien eurojen ulosottovelat – Ja yksi heistä on omilla luvuillaan

Kaupunki

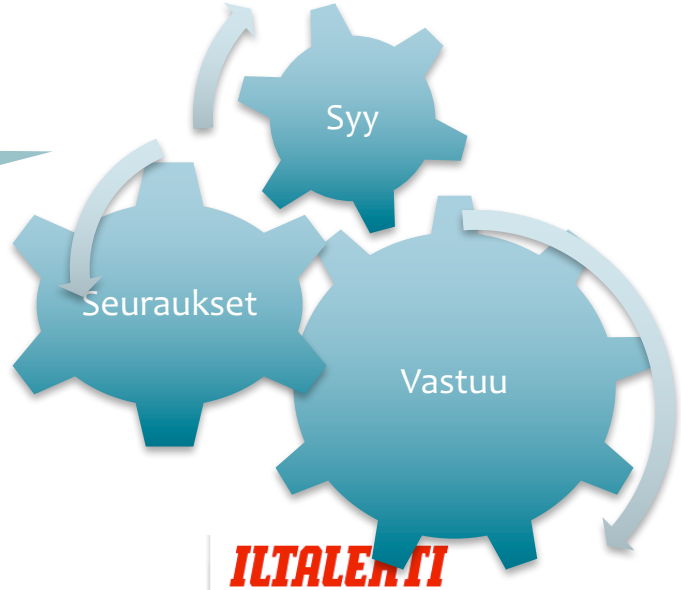
Aalto-yliopiston opiskelijoiden kysely-vastauksia saattoi vuotaa ulkopuolisille tieto-murron vuoksi

Typeform-yritys on ilmoittanut tietomurrosta asiakkailleen. Suomessa yrityksen kyselypalveluita käyttää esimerkiksi Hintsa Performance, joka teki kyselyn Aalto-yliopiston kauppakorkeakoulussa järjestetylle kurssille.

HELSINGIN UUTISET

PUHEENAIHE
6.4.2018 20.00

Suomessa paljastui vakava tietovuoto – Jopa 130 000 salasanaa pääsi ulkopuolisten käsiin



ILTALEHTI

Lopen koululla tietoihin käsiksi päässyt poika kertoo: kansiossa hyvin arkaluontoisia tietoja oppilaista - ”Pelottaa, että joku on ladannut tietojani”

25.05.2018 klo 12:28

Lopen yläkoululla Kanta-Hämeessä on tapahtunut tietovuoto, jossa oppilailla on ollut tietokoneella pääsy kansioon, jossa oli tietoja oppilaista.

Sisältö

- Tietoturva ja tietosuoja
- GDPR ja tietoturva
- Hallintajärjestelmät
- Tietoturvan hallintajärjestelmä
- Tietosuojan hallintajärjestelmä
- Miten saada tietoturva tietosuojaa palvelemaan?
- Riskien hallinnasta
- Korkeakoulut tietoturvan ja tietosuojan toimintaympäristönä
- Miten yhdessä eteenpäin?

Tietoturva ja tietosuoja

- Tietoturva tarkoittaa suojattavien kohteiden (järjestelmät, data, palvelut) turvaamista riskejä vastaan turvallisuuskontrollien avulla
- Tietosuoja tarkoittaa luonnollisen henkilön lakisääteisen yksityisyyden suojan turvaamista
  - Henkilötietoihin pääsyn rajaaminen ja valvominen
- Suojattavien kohteiden turvallisuus
    - Luottamuksellisuus
    - Eheys
    - **Saatavuus**
- Tietoturva on
    - Johdon vastuulla
    - Koko organisaation velvollisuus
    - Tietosuojan edellytys

Mitä tietosuoja-asetus m.m. edellyttää tietoturvalta?

- Art 5 (2): Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä **osoittamaan** se, että 1 kohtaa on noudatettu
- Art 24(1): Ottaen huomioon …**riskit** rekisterinpitäjän on **toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet**, joilla voidaan **varmistaa**…
- Art 24(3): …**hyväksytyn sertifiointimekanismin noudattamista** voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että rekisterinpitäjälle asetettuja velvollisuuksia noudatetaan
- Art 25(1):**Sisäänrakennettu ja oletusarvoinen tietosuoja**

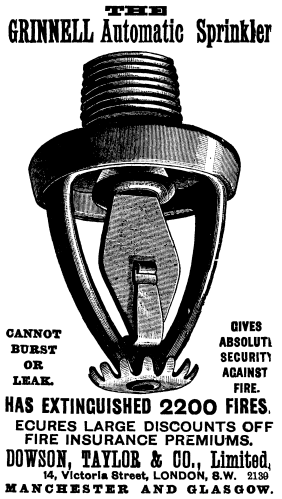
Mitä vielä tietosuoja-asetus edellyttää tietoturvalta?

- Art 32 (2): **Käsittelyn turvallisuus**
  - pseudonymisointi ja salaus
  - järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
  - Testataan.. ja arvioidaan säännöllisesti… tietojenkäsittelyn turvallisuuden varmistamiseksi
  - Riskeihin… vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi
- Art 33,34: **Henkilötietojen tietoturvaloukkauksesta ilmoittaminen**
- Art 35 (7d)**Tietosuojaa koskeva vaikutustenarviointi**
  - suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet

Miten saada tietoturva hallintaan?

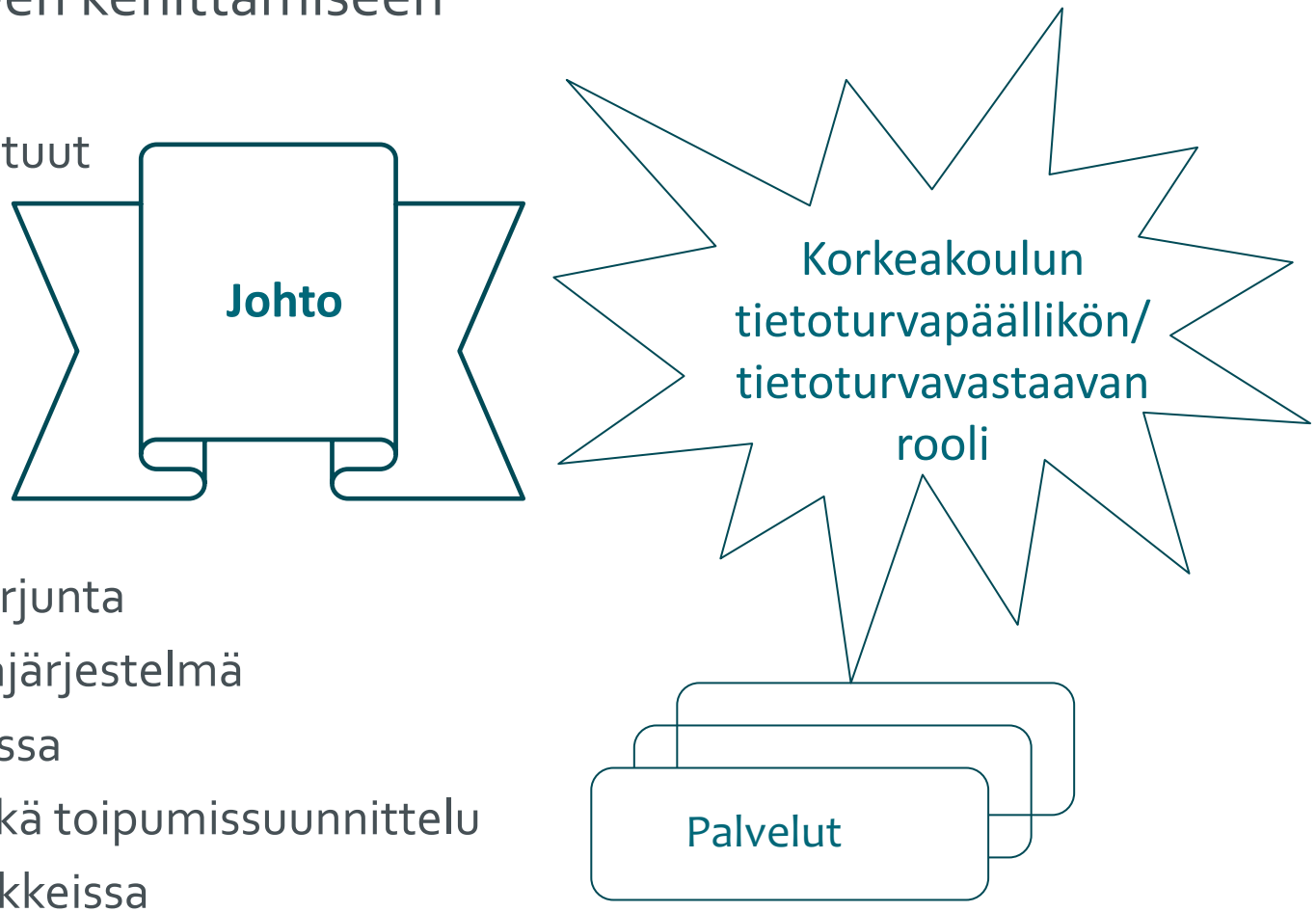
- Kun tilanne, esimerkiksi tietovuoto, on päällä tulee tilannetta hoitaa
  - Ole rauhallinen ja harkitse ennen kuin toimit
  - Toimi vastuullisesti
  - Viesti rakentavasti, älä syyllistä
  - Tee yhteistyötä
  - Palaudu normaaliin tilaan
  - Mieti ja kirjaa mitä voit poikkeamasta oppia vastaisuuden varalle

- Pidemmän päälle tulipalojen sammuttelu käy voimille
  - Miten poikkeamia voi estää ennalta
  - Miten voit havaita poikkeamat ajoissa
  - Miten poikkeamia voi vähentää sekä teknisin keinoin että johtamisella



Tietoturva hallintaan ja kestävälle pohjalle

- Tietoturva ei ole joukko satunnaisia toimenpiteitä vaan sen tulee perustua systemaattiseen ja pitkäjänteiseen kehittämiseen
  - Johdon tuki ja katselmukset
  - Turvallisuuteen liittyvät roolit ja vastuut
  - Politiikat ja ohjeet
  - Koulutus ja viestintä
  - Tilannekuva
  - Poikkeamien käsittely
  - Pääsynhallinta
  - Haittaohjelmien ja tietovuotojen torjunta
  - Muutoshallinta, vuosikellot, hallintajärjestelmä
  - Turvallisuusvaatimukset sopimuksissa
  - Elinkaarien hallinta ja jatkuvuus- sekä toipumissuunnittelu
  - Turvallisuusnäkökohdat kehityshankkeissa



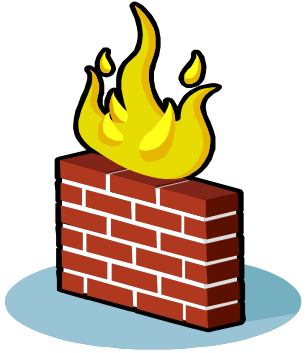
Tietosuojan hallintajärjestelmä

- Tietosuojaan liittyvät roolit ja vastuut
  - Johdon tuki ja katselmukset – vaikutusten arvioinnit
  - Tietosuojavastaava
  - Esimiehet
- Tietosuojapolitiikat ja -ohjeet
  - Käytännesäännöt
  - Käyttöehdot
  - Toimintaohjeet
- Koulutus ja viestintä
- Poikkeamien käsittely
- Tietosuoja sopimusehdoissa
  - Rekisterinpitäjän/Tietojen käsittelijänä
  - Kolmannet maat,…
- Tietovuotojen torjunta
- Tiedonhallintasuunnitelma
- Tietojen säilytys ja poisto
- Oletusarvoinen tietosuoja kehityshankkeissa

Miten saada tietoturva tietosuojaa palvelemaan?

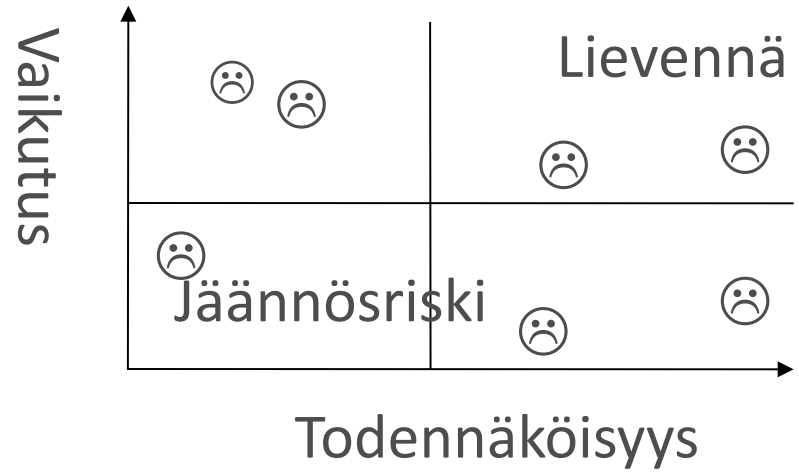
- Jatkuva operatiivinen yhteistyö
- Selkeät roolit ja työnjako
  - Tietoturvapäällikkö/tietoturvavastaava
  - Tietosuojavastaava
  - Yhteistyöryhmät
- Riskienhallinta/ vaikutusten arviointi
- Yhtenevät hallintajärjestelmät ja –käytännöt
  - Sopimusehdot vs. tietosuojan/turvallisuuden tekninen toteutus
- Pääsynhallinta ja valvonta
- Poikkeamien käsittely
- Neuvonta ja linjaukset, koulutus
- Kehityshankkeet – sisäänrakennettu ja oletusarvoinen tietosuoja

Minkälaisia riskejä kohtaamme?



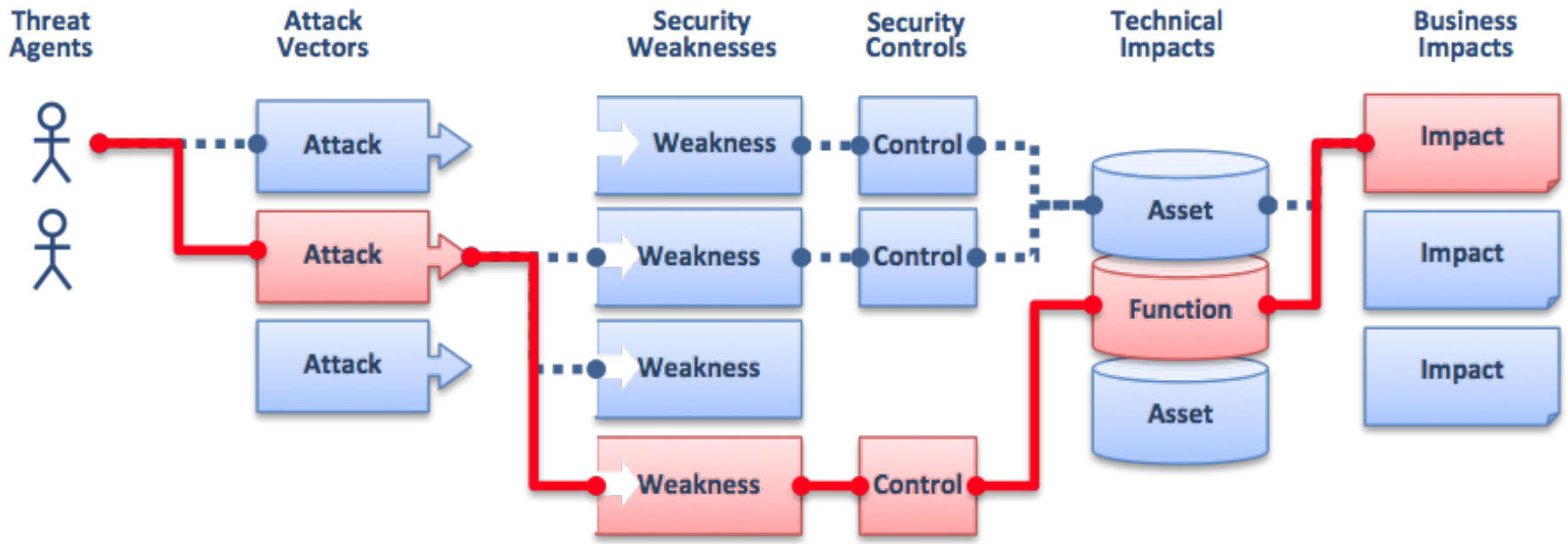
- Tunnuksen murto tai väärinkäyttö
- Tietovuoto
- Häiriöt infrastruktuurissa
- Vaikeasti toteutettavat turvallisuusvaatimukset
- Huono hankinta/harkinta, heikko ylläpito
- Palvelunestohyökkäykset
- Harkitsematon somen käyttö
- Varkaudet
- Haavoittuvuudet
- Takaportit
- *ja monta muuta…*

Sisäinen – Tuottamuksellinen
Sisäinen - Vahinko
Ulkoinen - Tuottamuksellinen
Ulkoinen - Vahinko



OWASPin* perinteinen (IT-)riskienhallinnan viitekehys

& Privacy/ impact



*OWASP CISO AppSec Guide: Criteria for Managing Application Security Risks

Tyypillisiä sisäisiä riskejä korkeakouluissa

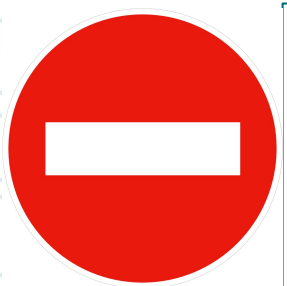
- Tunnuksen väärinkäyttö
- Konfigurointivirheet
- Suunnittelemattomat käyttökatkot
- Pula henkilöresurssista
- Ylläpidon laiminlyönti
- Henkilötietojen vuodot
- Luottamuksellisen tiedon vuoto
- Tiedon eheysongelmat
- Infrastruktuuriongelmat
- Taloudelliset väärinkäytökset

Ak14

- Tutkimuksen tai opinnäytteen plagiointi
- Päihdeongelmat
- Petokset ja muut rikokset
- Ylläpito-, esimies-, tai tutkinto-oikeuksien väärinkäyttö
- Ohjelmistohaavoitttuvuudet
- Hallitsematon toimintaympäristö
- Toimintakulttuurin merkittävät ongelmat
- Luottamuksellista tietoa ei luokiteltu tai merkitty

Riskien hallinnollisia lieventämiskeinoja

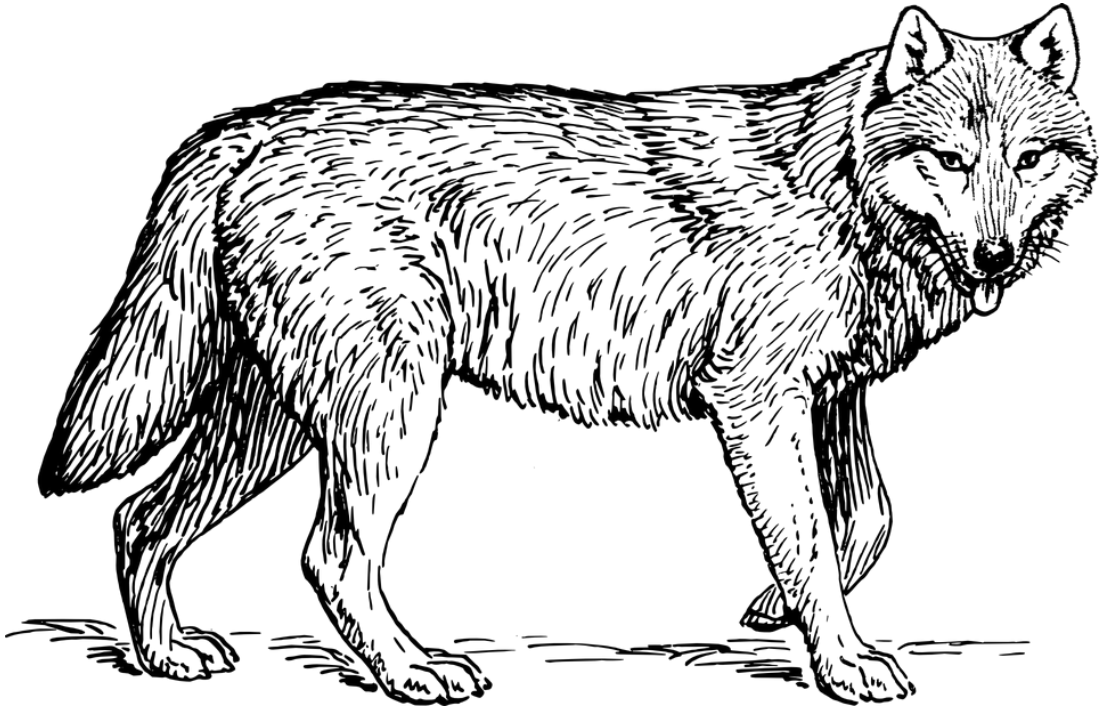
- Tunnusten hallinta
- Muutoshallinta
- Saatavuuden hallinta
- Henkilöstön resursointi
- Toimiva tietohallinto
- Tietojen luokittelu
- Eheysvarmistukset
- Toimiva tietohallinto
- Sisäinen tarkastus



- Tutkimuksen aitouden tarkistus
- Päihdepolitiikka, työterveyshuolto
- Sisäinen tarkastus, käyttöturvallisuus
- Hallintajärjestelmän ylläpito
- Konfiguraatioiden hallinta
- Muutoshallinta
- Hyvä johtamiskulttuuri ja johtamisjärjestelmä

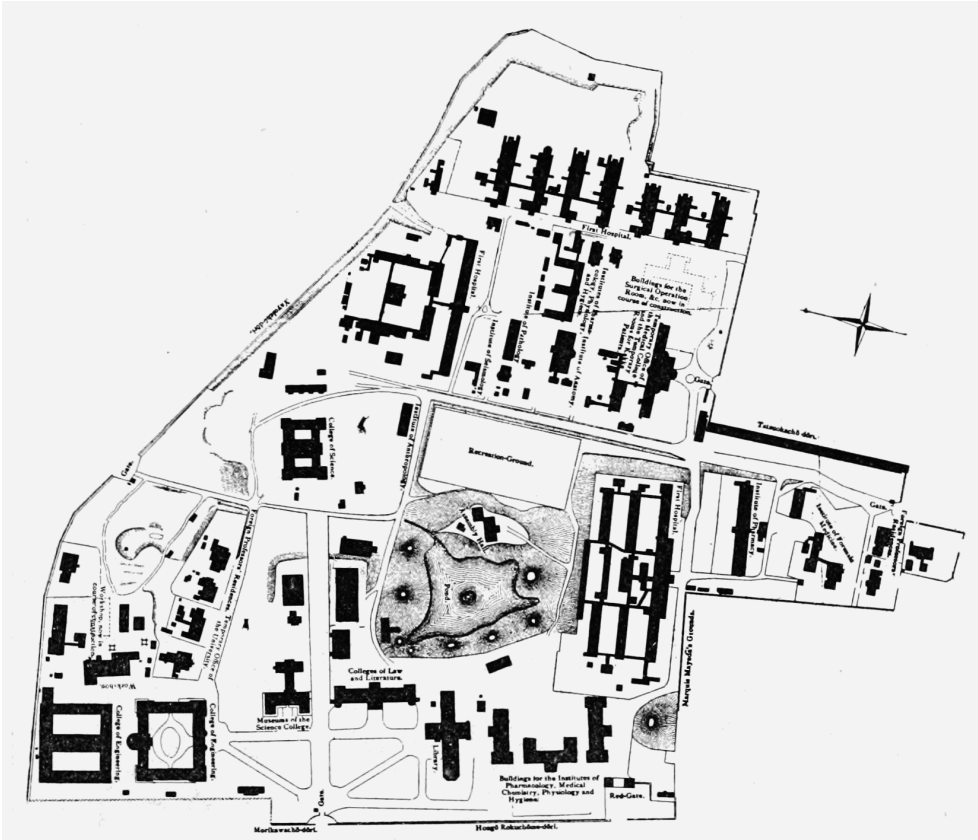
Miten riskit tulisi tunnistaa ja luokitella?

- Lähde tosiasioista, vältä tunnekuohuja ja vedätyksiä
  - Älä dramatisoi
  - Oma metriikka, skannaukset
- Aloita "matalalla roikkuvista hedelmistä"
  - Viime vuosina toteutuneet turvallisuuspoikkeamat
  - Havainnot sisäisissä arvioinnissa
  - Kokemuksia vertaisorganisaatioista
  - Tiedotteet luotettavilta tietoturvatoimijoilta
  - Haavoittuvuustilastot
  - Päivitystilanne
  - Saatavuustilastot
  - Pehmeä, esoteerinen tieto
- Yritä päätellä järkevästi
- Tee rajauksia, priorisoi
  - Voimme käsitellä vain rajallisen määrän riskejä



Yliopistot suojattavina kohteina

- Yliopiston tehtävät
  - Tieteellinen tutkimus
  - Tutkimukseen perustuva opetus
  - Yhteiskunnallinen vaikuttaminen
- Ei osa valtionhallintoa, ei yritys, ei yhdistys
- Tutkimuksen vapaus/ akateeminen kulttuuri
- Hajautettu päätöksenteko
- Osittain keskitetyt IT-palvelut
- Ulkoistukset/ pilvipalvelut
- Yhteistyöverkostot ja konsortiot
- Yhteiset infrastruktuurit
- Henkilökeskeisyys
- Ammattietiikka ja kriittinen ajattelu
- Merkittävä riippuvuus IT-palveluista



Riskienhallinnan kehittäminen korkeakouluissa

- Tunnista ja kuvaa suojattavat kohteesi
- Kirjaa tärkeimmät riskisi ja sekä turvallisuuskontrollisi
  - Johtaminen, turvallisuusvastaava tukee ja valvoo
  - Substanssiosaaminen, poikkeamat, ulkoiset lähteet
  - Sisäiset ja ulkoiset arvioinnit ovat erinomainen perusta
- Vastuuta turvallisuuteen liittyvät tehtävät
  - Turvallinen ylläpito
  - Politiikat ja ohjeet
  - Luo turvallisuuden ja tietosuojan hallintajärjestelmä
- Varmista osaaminen, ammattitaito ja asenne
  - Tekniset taidot, ymmärrys toiminnan vaatimuksista,
  - Ammattimainen asenne

Teknisten tietoturvariskit poikkeaman aikana

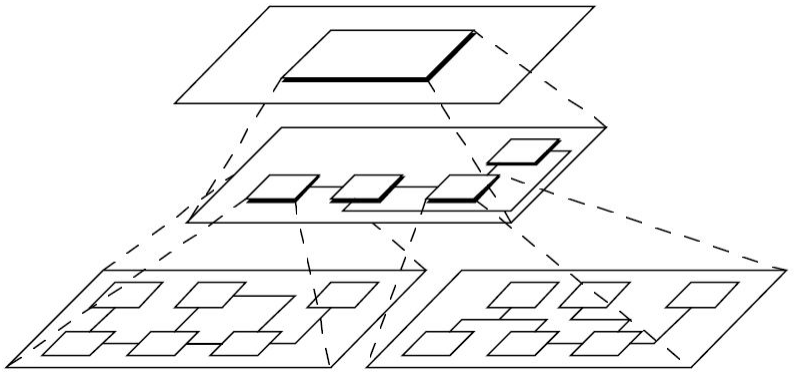
Tilanne päällä?

- Huolestuttava ja/tai kohuttu haavoittuvuus
- Tietomurto
- Hallitsematon katko/häiriö
- Ulkoinen tieto (esim. Funet CERT)tietoturvapoikkeamasta
- “Heikot signaalit”

•Älä panikoi
•Kokoa ja johda poikkeamaryhmää
•Hanki paras asiantuntijasi selvittämään vaikutukset
•Arvio liiketoiminnallinen riski johdon kanssa
•Viestintä (usein >50% työstä poikkeamien hallinnassa)
•Päätä välittömistä toimenpiteistä (palvelun sulkeminen) ja paikkauksista
•Johda toipuminen
•Raportoi johdolle – mitä opimme tästä, mitä pitää tehdä

Haasteena lisääntyvä kompleksisuus

- Porttikohtainen pääsynhallinta -> sovellusten turvallisuus
- Verkkoturvallisuuden tilannekuva
  - Liikennemäärä ja –tyypit
  - Heikkojen anomalioiden havaitseminen
  - Vanhana esimerkkinä Slowloris
- Välikerrosten turvallisuus (virtualisointi, kontit, federointi)
- Ulkoistetut palvelut
  - Toimittajien turvallisuus
- Pilvipalveluiden turvallisuus
  - Vaikeaa saada luotettavaa informaatiota
  - Paljon ”markkinointiviestintää”
- BYOD

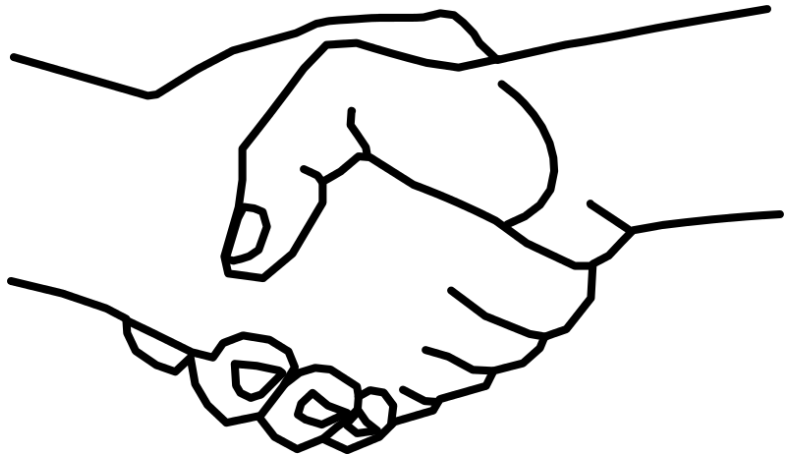


Priorisointi ja päätöksenteko

- Sekä reaktiivisessa että proaktiivisessa tietoturvallisuudessa priorisointi ja johtaminen ovat ratkaisemassa asemassa
- Usein käytettävissä oleva informaatio on epätäydellistä tai jopa vääristeltyä
- Päätöksenteon valtuudet usein ongelmallisia
- Organisaatiolla usein puutteelliset valmiudet kriisiviestintään
- Teknisen impaktin ja liiketoiminnallisen impaktin suhde vaikeaa määritellä
- Suosituksia:
  - Panosta kriisijohtamiseen etukäteen, kirjoita ohje- tai politiikka
  - Panosta tekniseen tietoturvan substanssi-osaamiseen ja hallintaan
  - Tee selkeitä päätöksiä ja viesti niistä olennaisille sidosryhmille
  - Opi poikkeamista, viesti asiasta myös johdolle

Turvallisuus perustuu yhteistyöhön

- Korkeakoulujen tietoturvaryhmä
  - Tietoturvapäälliköt/-vastaavat – yliopistot, ammattikorkeakoulut
  - Luottamuksellisen tiedon jakaminen
  - Yhteisten turvallisuusohjeiden ja –käytäntöjen kehittäminen
- Korkeakoulujen tietosuojaverkosto
  - Laaja-alainen yhteistyöverkosto
  - Keskustelu ajankohtaisista aiheista



- Yhteistapaaminen korkeakoulujen tietoturvapäivillä 2019 Seinäjoella
- Kansainvälinen yhteistyö
  - WISE https://wise-community.org/
  - GÉANT SIG-ISM https://wiki.geant.org/display/SIGISM/
  - NORDUnet https://www.nordu.net/
  - TF-CSIRT https://tf-csirt.org/…

Yliopistojen yhteiset tietoturvaohjeet – myös tietosuojan perusta

- Opiskelijan tietoturvaopas
  - http://www.oulu.fi/sites/default/files/content/opiskelijan-tietoturvaopas.pdf
- Henkilöstön tietoturvaopas
  - https://www.uef.fi/documents/11039/196003/henkiloston-tietoturvaopas.pdf
- Mobiiliturvaohje
  - https://www.ulapland.fi/loader.aspx?id=ba40652d-0bf0-4c69-966a-de4c4592727b
- Also available in English
- Tillgängliga även på svenska!

- *Tietosuojan käytännesäännöt*

Tietosuojan turvallisuushaasteita

- Ulkoistukset/Pilvipalvelut
- Henkilökohtaiset some-tunnukset
- Riippuvuudet
- Turvallisuuden valvonta
- Osaaminen
- Tietosuojavastaavan ja tietoturvavastaavan yhteistyö
- Ohjeistus
- Kyberuhat, tiedustelutoiminta
- Mittaaminen ja seuranta

Kiitos!

Kommentteja?
kysymyksiä?

urpo.kaila@csc.fi