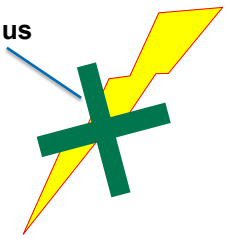
Tieto- ja kyberturvallisuus

Käsitteet ja perusteet

Mitä on kyberturvallisuus (2010)

Kyberturvallisuus



Kyberhyökkäykset

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

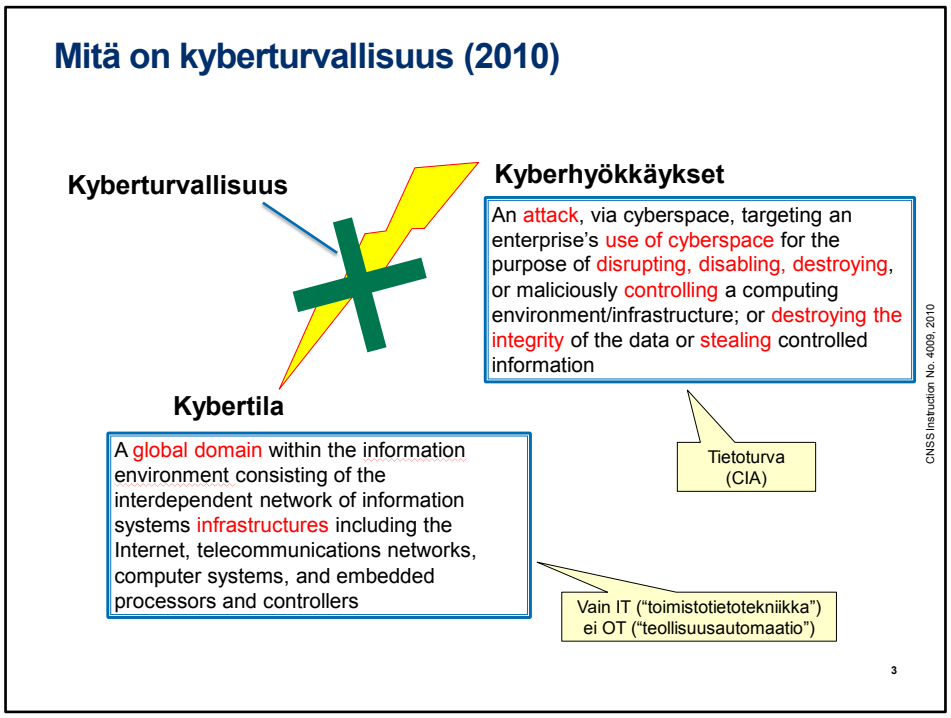
Kybertila

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

CNSS Instruction No. 4009, 2010

2

USA:n kansallisen turvallisuusjärjestelmien komitean (CNSS) vuoden 2010 määritelmän mukaan kyberturvallisuus on kybertilan suojaamista kyberhyökkäyksiltä.



Olennaista vanhassa määritelmässä oli se, että hyökkäys sidottiin perinteiseen IT-infraan (työasemiin, palvelimiin, tietoverkkoihin ym.) sekä näiden sisältämän datan turvaamiseen (luottamuksellisuuteen, eheyteen ja saatavuuteen). Näissä määritelmissä on muutamia haasteita, kuten esimerkiksi teollisuusautomaatiota vastaan hyökkääminen, hyökkäyksen seuraukset ja niiden laajuus sekä tapahtuneen seurauksen tahallisuus.

Kyberturvallisuuden määritelmä tänään?

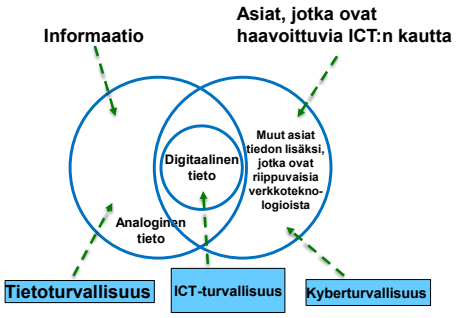
- **Fyysisten uhkien torjunta kyberturvalla**
  - Esim. palveluiden siirtäminen pilveen
- **Kyberuhkien torjunta fyysisin keinoin**
  - Esim. palvelininfran takavarikointi
- **Uhkat laajempia kuin vain ICT ja data**
  - Kriittinen infrastruktuuri
- **Mikä on tarkoituksellista?**
  - Miten tunnistetaan inhimillinen erehdys?
- **Entä tekoäly?**
- **Miten vahinkoihin tulee varautua?**
- **Tietoturvallisuus vs. käyttöturvallisuus**
  - Security vs. safety

4

Fyysinen maailma ja kybermaailma kietoutuvat tiukemmin ja tiukemmin yhteen.
Pelkästään vahinkoja tulkitsemalla on nykyisin entistä vaikeampaa erottaa inhimilliset erehdykset tahallisesta toiminnasta; saati sitten kohdennettu hyökkäys esimerkiksi yleisestä haittaohjelmakampanjasta: Floridan vedenpuhdistamossa käynyt tapaus sisälsi kaikki kyberhyökkäyksen tunnusmerkit, mutta oli lopulta työntekijän virhe.
Perinteiset tietoturvallisuuden suojauksen määritelmät eivät lisäksi ole enää riittäviä tekoälyn kanssa, uhkamallit ovat paljon laajempia.

Kyberturvallisuuden määritelmä tänään?

- **Kyse ei ole vain datasta**
  - … mutta data on kybertoimintaympäristön ja –turvallisuuden ytimessä
- **Tässä käytettävä määritelmä:**
  - Kyberturvallisuus on datan ja datasta riippuvien järjestelmien suojaamista haitallisilta vaikutuksilta, ja muiden järjestelmien suojaamista datan ja datasta riippuvien järjestelmien aiheuttamilta uhilta ja niiden väärinkäytöltä
- **Huom.**
  - Kyberturvallisuus ei aina ole paras suojauskeino → kokonaisriskienhallinta

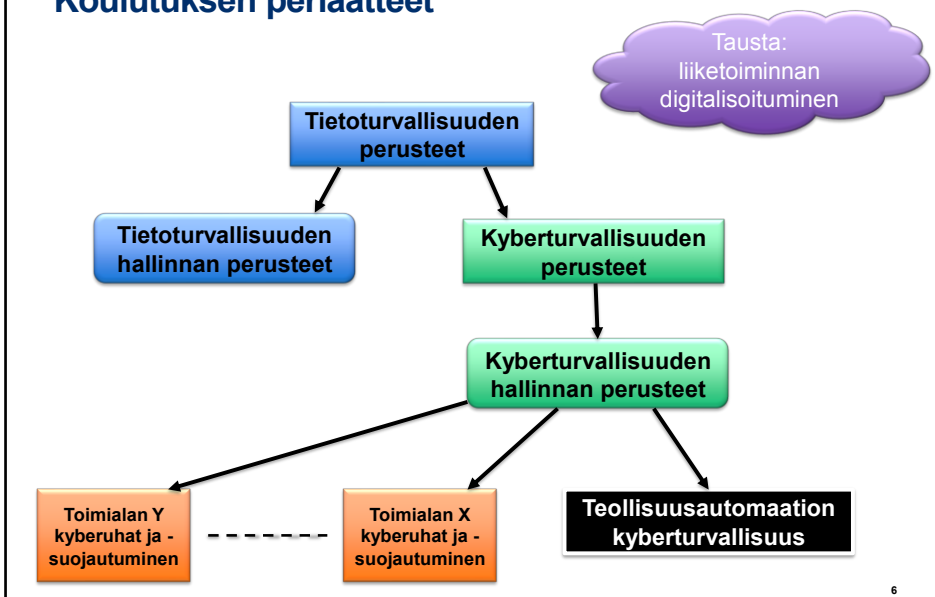


5

Tietoturvallisuus käsittää myös analogisen tiedon, ja toisaalta jättää huomiotta tai ainakin tulkinnanvaraiseksi sen, miten esimerkiksi teollisuusautomaatiota tulisi käsitellä. Data on kyberturvallisuuden ytimessä, mutta se ei ole sen koko kuva.

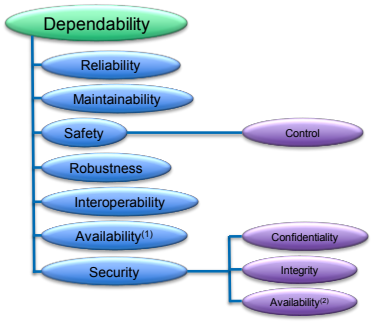
On hyvä huomata, että kyberturvallisuus pitää hallinnollisesti nähdä osana muuta organisaation riskienhallintaa. Kaikkiin kyberuhkiin ei ole kustannustehokasta varautua kybertekniikoilla, vaan esimerkiksi ulkoistamalla riski (vakuutus) tai hallinnollisin sanktioin.

Koulutuksen periaatteet



Datan ja järjestelmien suojaamisen käsitteitä

- **Lähestymistavasta riippuen**
  - Puhdas tietoturva
  - Systeemitieteet
  - Teollisuusautomaatio
  - Tekoäly
- **Suojaamisen käsitteillä sovelluskohtaista priorisointia**



Trustworthy AI goals
(NIST AI-100-1)

7

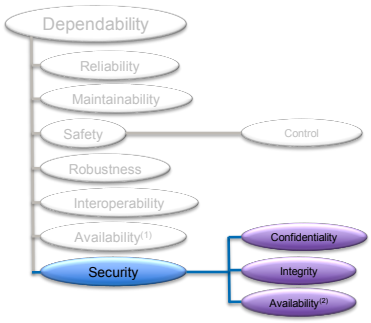
Niinkutsutut CIA-attribuutit ovat kuitenkin melko uusi käsite. Nk. Toimintavarmuus nousi esille jo 1830-luvulla, ja erityisesti ensimmäiset analogiset tietokoneet 1940- ja 50-luvuilla käyttivät epäluotettavia komponentteja ja tärkeintä oli ylipäätään laskennan saaminen päätökseen. Monet toimintavarmuuden käsitteet ovatkin ymmärrettävissä tätä kautta.

Toimintavarmuuden käsitteitä ovat mm.
- Toiminnan luotettavuus ympäristön olosuhteiden heiketessä. RRR-mallissa (reliability, resiliency, robustness) luotettava (resilient) järjestelmä toimii oikein normaaleissa olosuhteissa; vikasietoinen (resilient) järjestelmä toimii, vaikkakin heikommin, myös epänormaaleissa olosuhteissa ja kestävä (robust) järjestelmä toimii normaalisti myös (tiettyjen rajojen sisällä olevissa) epänormaaleissa olosuhteissa.
- Huollettavuus (maintainability), tarkoittaa, että järjestelmää on fyysisesti, teknisesti ja organisaation prosessien kannalta ylipäätään mahdollista huoltaa
- Fyysinen turvallisuus (safety) tarkoittaa sitä, että ihmiset ja järjestelmät säilyvät vahingoittumattomina
- Saatavuutta on kahta lajia: järjestelmän “pysyminen pystyssä” ja tietoturvallisuuden saatavuus vain luvitetuille käyttäjille.

Tekoälyn turvallisuusominaisuuksien katsotaan ulottuvan laajemmalle, ja mukana on tekoälyn luotettavan toiminnan lisäksi myös yhteiskunnallisia ulottuvuuksia, kuten vähemmistöjen suoja.

Datan suojaamisen käsitteitä

- **Tietoturvallisuus**
- **= Datan turvallisuus**
- **Perinteisellä priorisoinnilla:**
  - Luottamuksellisuus (Confidentiality)
  - Eheys (Integrity)
  - Saatavuus (Availability)
- **= C + I + A**



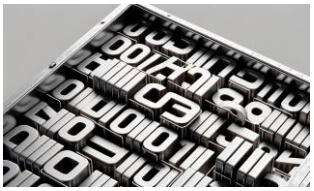
8

Tietoturvan peruskäsitteet ovat
- Luottamuksellisuus (C)
- Eheys (I)
- Saatavuus (A)

Lyhyesti: tiedon pitää olla luotettavaa ja saatavissa vain sen tarvitsijoille

Data and tietoturva nykyisin

- **Datan “liiketilat”**
  - Tietoliikenne (Data-in-transit, perinteinen)
  - Säilöttävä tieto (Data-at-rest, perinteinen)
  - Laskennassa oleva tieto (Data-in-computation/use, uusi)



9

Liikkeessä olevaa tietoa (data-in-transit, esimerkiksi Internetissä kulkeva data tai Netflixistä TV:hen tuleva stream) on suojattava pääosin eri mekanismein kuin paikallaan olevaa, esimerkiksi tietokantoja ja tiedostoja. Tärkein ero suojausmekanismeissa on, että liikkeessä olevaa tietoa suojattaessa suojausmekanismi on helpompi irrottaa itse datasta: data voidaan antaa suojatun siirtomekanismi käyttöön ja poistaa sieltä, kun siirto on tapahtunut. Säilöttävän data suojausprosessi ei ole useinkaan yhtä suoraviivainen.

Laskennassa olevan datan suojaaminen on vielä uutta tiedettä: on vaikeaa tehdä operaatioita datalle, jos datasta ei voi tietää mitään. Tämä on haaste erityisesti tekoälyssä.

Perusattribuuteista johdettuja tavoitteita

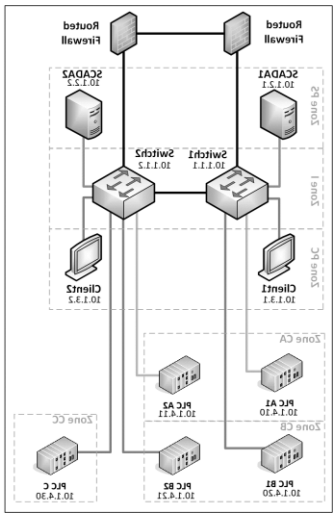
- **Luottamuksellisuudesta johdettuja**
  - Yksityisyys = Tiettyjen henkilöön sidottujen tietojen luottamuksellisuus
  - Yksityinen laskenta = Laskennassa olevan datan luottamuksellisuus

- **Eheydestä johdettuja**
  - Autenttisuus = Esim. lähettäjän identiteetin eheys
  - = Myös: datan alkuperätiedon eheys
  - Kiistämättömyys = Datan luojan/käsittelijän identiteetin eheys
  - IoT-laitteen attestaatio = Koodin tai metatietojen eheys
  - Tietokannan yhtäpitävyys = Tietokantataulujen yhtenevyyden eheys
  - Lohkoketjun konsensus = Tapahtumaketjun järjestyksen eheys

10

Yleisiä tietoturvan periaatteita: eristäminen

- **Idea:**
  - Monimutkaisuuden vähentäminen
  - Hallittavissa oleva määrä tarkastuspisteitä
- **Eri periaatteita eristämiseen:**
  - Politiikkataso: roolinhallinta
  - Politiikkataso: tiedon herkkyysluokat
  - Tekninen taso: verkon segmentointi
  - Fyysinen taso: fyysinen erottelu (“airgap”)



11

Roolinhallinta viittaa auktorisoinnin ts. pääsynhallinnan sitomiseen rooleihin (/tehtäviin) pikemmin kuin henkilöihin. Henkilön yhtäaikaa hyödynnettävissä olevien roolien tyyppeihin asetetaan rajoituksia (nk. Vaaralliset työyhdistelmät). Sama henkilö ei esimerkiksi voi olla laskun tekijän ja laskun hyväksyjän roolissa, ainakaan saman laskun osalta.

Politiikkatasolla voidaan myös luokitella tieto sen herkkyyden perusteella ja perustaa käsittelymenetelmiä luokituksen (esim. “YRITYSLUOTTAMUKSELLINEN”) perusteella.

“Air gap” tarkoittaa, että järjestelmät erotellaan fyysisesti riittävän kauas toisistaan. Tästä ei kuitenkaan välttämättä seuraa turvallisuutta, koska fyysisesti eriytetytkin järjestelmät ovat tekemisissä muiden kanssa esim. USB-median avulla.

Yleisiä tietoturvan periaatteita: virhetilanteiden käsittely

- **Järjestelmän logiikan pettäminen → kyberhyökkäykset**
- **Entä jos…?**
  - Syötteen rajoitukset
  - Järjestelmän käyttöpolitiikan muutokset
  - Rajapintojen muutokset
- **Määrittelemätön toiminto**
- **Määritelty toiminto (mutta tunnistettu)**
- **Määritelty ja käsitelty toiminto**

- **Testaus, validointi, verifiointi ja harjoittelu**

12

Kyberhyökkäykset pääsevät lävitse järjestelmiin kohdista missä järjestelmän toimintalogiikka pettää. Useimmiten tämä pettää juuri kohdissa, joissa toiminnallisuutta ei ole tarkkaan määritelty ja tiedostettu, erityisesti tämä koskee järjestelmän virhetilanteiden käsittelyä.

Entä jos…?

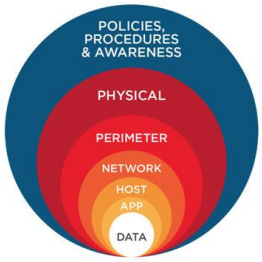
- Järjestelmä saakin “Kyllä/ei”-vastauksen sijasta 2G karttakuvan?
- Henkilön vaihtaessa tehtävää organisaation sisällä vanhat roolit jäävätkin voimaan ja johtavat vaarallisiin työyhdistelmiin (esim. Pääsee hyväksymään omat laskunsa)
- Maksujärjestelmä noudattaakin hieman vanhaa yhteysstandardia

Vaikeampia asioita on ylipäätään tunnistaa erilaiset virhetilanteet. Näitä on kaikilla abstraktiotasoilla koodin kirjoittamisesta käyttövaltuuspolitiikkoihin. Jo se, että virhetilanteet ja muut toiminnot on tunnistettu ja määritelty auttaa hyökkäyksen sattuessa vähintään tekemään korjaavia toimenpiteitä. Parhaassa tapauksessa epäsuotuisasti vaikuttava toiminto on myös korjattu tai vähintään mitigoitu.

Koska kaikkiin järjestelmiin koodista organisaation riskienhallintaan jää virheitä, ainoa ratkaisu on testata ja uudelleenarvioida niitä säännöllisesti ja erityisesti muutospisteissä.

Yleisiä tietoturvan periaatteita: syväpuolustus

- **Syväpuolustus = Defence in Depth (DiD)**
- **DiD = "***Useiden eri vastakeinojen soveltamista kerroksellisesti tai peräkkäisin askelin turvatavoitteiden saavuttamiseksi. Metodologia sisältää heterogeenisten turvateknologioiden käyttöä kerrostamalla niitä yhteisten uhkavektorien suunnassa niin, että yhden teknologian pettäessä uhan estää toinen teknologia eri kerroksella***." (IEC 62443)**
- **Tämänhetkinen jaottelu:**
  - *Politiikat*: luo hyvät säännöt, sitouta ihmiset niihin
  - *Tilaturva:* tuki loogisen suojauksen kiertomahdollisuudet
  - *Verkko/reuna:* suojaa virtuaalisen tason pääsyä usealla organisaation rajoilla (ulkoisilla ja sisäisillä)
  - *Työsema/palvelin:* suojaa loppukäyttäjän laite erikseen
  - *Sovellus:* luotettu sovelluksen asennus, päivityksen, käyttäjäntunnistus,…
  - *Data*: CIA, esim. Salaa tiedot luottamuksellisuuden takaamiseksi



13

DiD-periaate on datakeskeistä, mutta käyttäjääkään ei voi unohtaa: myös käyttäjänhallinnan ja todentamisen on oltava monikerroksista. On kuitenkin huomioitava, että monikerroksinen käyttäjän todentaminen EI tarkoita salasanan kysymistä joka viides minuutti, VAAN tietoturvapalveluiden integrointia esimerkiksi SSO:n kautta.

Politiikat: sääntöjen tulisi noudattaa yrityksen prosesseja ja soveltuvaa viranomaissääntelyä. Sääntöjä, eli "hallinnollisia kontrolleja" ei tule keksiä helpottamaan hallintohenkilöstön töitä, koska turhat säännöt johtavat pelkästään niiden kiertämiseen ja tärkeidenkin sääntöjen noudattamatta jättämiseen.
Tilaturvallisuus on kyberturvallisuuden kannalta olennaista, koska esimerkiksi palomuuri (joka on loogisen tason kontrolli) ei suojaa siltä, että joku kävelee ovesta sisään, ja asentaa hakkerityöaseman konttorin sisäverkkoon.

"Reuna" (perimeter) on tietyntyyppisen turvallisuusajattelun käsite, jossa luodaan samaa turvatasoa olevien fyysisen tilan, tietoverkkojen ja tietojärjestelmien kokonaisuuksia, turva-alueita. Tarkastaminen ja toiminnan rajoittaminen tehdään nimenomaan turva-alueiden rajalla tai reunalla. Turva-alueet on luonnollista asettaa organisaation hierarkian mukaisesti, koska

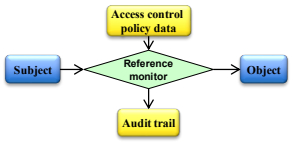
hierarkia *yleensä* noudattelee liiketoimintaprosesseja ja niiden perusteella tehtyjä turva-aluerajoja.

Nykyisissä dynaamisissa organisaatioissa ja projektiluontoisessa työssä joudutaan toimimaan organisaatiorajojen ylitse, ja tietojärjestelmätkin ovat pilvessä. Tämä ei kuitenkaan tarkoita sitä, että syväpuolustus unohdetaan, vaan että pilvipalvelun tarjoaja hoitaa osan esimerkiksi fyysisestä, ja reuna-alueen turvallisuudesta. Tällaisessa toiminnassa turva-alueet ovat dynaamisempia ja muodostavat lisäkerroksia aiempien virtuaalisten turva-alueiden sisälle, esimerkiksi Teams-palvelun pääsynhallintalistojen tai VPN:n avulla.

Tietoliikenneprotokollat ovat nykyisin jo hyvin mietittyjä sitä uhkamallia varten, että hyökkääjä salakuuntelee tai yrittää vaikuttaa itse protokollaan verkon ylitse. Sen sijaan päätelaitteissa on lukuisia muita sovelluksia, jotka eivät ole yhtä hyvin suojattuja. Useimmiten hyökkääjä pyrkiikin murtamaan päätelaitteesta jonkin heikomman sovelluksen, jota kautta saadaan koko päätelaite haltuun. Tämän jälkeen tietoliikennettä voidaan “kuunnella” pelkästään urkkimalla vaikkapa puhelimen mikrofonia tai ottamalla näyttökuvia. Tämän vuoksi myös päätelaitteen suojaaminen on olennaista.

Yleisiä tietoturvan periaatteita: kuristuspisteet

- **Idea: jokaisen tapahtuman tarkastaminen joka paikassa on liian kallista**
  - Vähennä tapahtumia → järjestelmän käytettävyys kärsii
  - Vähennä tarkastuksia → jotkin tapahtumat jäävät tarkastamatta, ja turvallisuus kärsii
- **Pakotetaan suurin osa tapahtumista muutamien kanavien lävitse (kuristuspisteet)**
  - Epäilyttävien tapahtumien tarkastaminen (+karsiminen)
  - Suorituskyky voi kärsiä (esim. IoT)
- **Esimerkkejä: palomuuri, IDS**
- **Toimii turva-alueajattelun kanssa**
  - Turva-alueiden välinen liikenne ainoastaan kuristuspisteiden kautta
- **Tarvitsee tietoturvapolitiikan toimiakseen**
- **Tulee jättää lokitiedot siitä, mitä tapahtui ja millä perusteella**



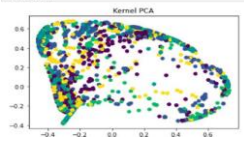
14

Yleisiä tietoturvan periaatteita: poikkeamien havaitseminen

- **Tietojärjestelmien monimutkaisuus → monipuoliset käyttötavat**
- **Luvaton käyttötapa → poikkeava jalanjälki**
  - … kuten myös jotkin käyttäjät ja erikoiset käyttötavat
- **Poikkeava jalanjälki vahva tunnistustapa**
- **Mikä onkaan "normaalikäyttöä"?**
  - Voi vaatia operatiivisessa käytössä olevan järjestelmän seurantaa ja analysointia jonkin aikaa
- **Kuinka poikkeavuudet huomataan?**
  - Määriteltävä metriikat, tilastot ja ulottuvuudet
  - Yleensä valmiiden tuotteiden osana
- **Käyttö niin verkko- kuin päätelaiteturvallisuudessa**
  - IDS/IPS
- **Tekoälyratkaisut tässä hyvin toimivia ja helppokäyttöisiä**

```
#Kernel PCA
kpca = KernelPCA(kernel='rbf', gamma=1)
X_kpca = kpca.fit_transform(X_train)

plt.title("Kernel PCA")
plt.scatter(X_kpca[:,0], X_kpca[:,1], c=y_train)
plt.show()
```



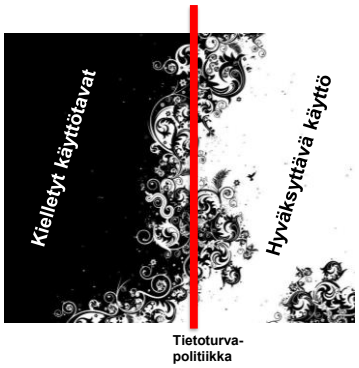
15

Nykyiaikainen organisaatio tarvitsee hyvin monenlaisia tapoja käyttää tietojärjestelmiä. Luvaton käyttö, mikäli tietoturvapolitiikka on asetettu järkeväksi, aiheuttaa jo määritelmän mukaankin poikkeavaa käyttäytymistä tietojärjestelmissä. Tämä on sinänsä hyvin toimiva periaate vahingollisen kybertoiminnan havaitsemiseen (ei siis vielä torjuntaan). On kuitenkin oltava realistinen kuva siitä, mikä on aidosti normaalikäyttöä: pelkkien asetettujen käytänteiden perusteella sitä ei voi päätellä, koska organisaatiossa muodostuu monia hyödyllisiä tapoja virallisten sääntöjen huomioimatta jääneille alueille. On siis kyettävä jollakin tavalla jalkautumaan organisaation jokapäiväiseen toimintaan, nimenomaan tietoliikenteen ja järjestelmien käytön tasolla.

Erilaiset tekoälyratkaisut ovat tällaisessa tarkoituksessa tehokkaita, koska ne kykenevät oppimaan myös tunnistamattomia tapoja käyttää tietojärjestelmiä pelkästään lokitietojen tai tietoliikenneprofiilien perusteella, ja analysoimaan niitä useammassa ulottuvuudessa.

Yleisiä tietoturvan periaatteita: hienojakoinen pääsynhallinta

- **Turvallisuus vs. käytettävyys**
- **Linja hyväksyttävän (ja/tai välttämättömän) ja kielletyn käytön välillä kompleksinen**
- **Lyhyt ja karkeajakoinen tietoturvapolitiikka johtaa sääntöjen kiertämiseen**
- **Ratkaisu: hienojakoinen kontrolli**
  - Esim. RBAC- tai ABAC-säännöstö
  - Vaatii luotettavan käyttäjän tunnistamisen ja todentamisen (/autentikoinnin)
  - Ylläpidettävyys → automatisointi
- **Erilliset toimintoalueet:**
  - Identity- and Access Management
  - Role-/Attribute-based Access Control



16

Turvallisuus ja käytettävyys ovat yleisesti ottaen saman asteikon eri päissä, koska helppokäyttöistä järjestelmää on myös helppo väärinkäyttää. Tämä ei kuitenkaan ole koko totuus: jos järjestelmän turvallisuuden ja käytettävyyden suunnitteluun käytetään riittävästi resursseja, päästään varsin hyviin kompromisseihin.

Jos tietoturvapolitiikka on liian yksinkertainen käyttötapauksiin nähden, normaalikäyttäjät alkavat kiertämään sääntöjä saadakseen hommansa tehdyksi. Tämä johtaa siihen, että sisäiset, auktorisoidut käyttäjät ohittelevat tietoturvakontrolleja.

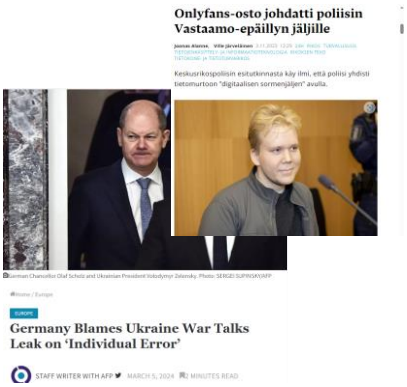
Tietoturvapolitiikka on hyvä rakentaa roolipohjaisuuden ja attribuuttipohjaisuuden varaan. Roolipohjaisessa pääsynhallinnassa (RBAC) käyttäjille annetaan työtehtävän perusteella rooleja, ja luvitus järjestelmiin tehdään roolien perusteella. Attribuuttipohjainen pääsynhallinta antaa luvituksen työtehtävän lisäksi järjestelmän ja ympäristön muiden ominaisuuksien perusteella, esimerkiksi sijainnin, kellonajan ja tietojärjestelmän senhetkisen liiketoimintaprosessin liitynnän kautta.

Automatisointi tarkoittaa tässä sitä, että esimerkiksi uuden käyttäjän

lisääminen järjestelmiin menee HR:n ja esimiehen antamien työtehtävien perusteella automaattisesti HR- ja ERP-järjestelmistä operatiivisten järjestelmien pääsynhallintaan, tai että uudessa projektissa tarvittavat pääsyoikeudet Sharepointiin tulevat automaattisesti projektinhallinnan toimin. Nämä kaikki vaativat järjestelmien välistä identiteettienhallinnan ja todentamisen menetelmien yhteentoimivuutta, esim. SSO.

Yleisiä tietoturvan periaatteita: OPSEC

- **Joka tason 360 astetta turvallisuus →**
- **OPSEC = Operations security**
  - Nimi USA:lta Vietnamin sodan aikana
  - "*järjestelmällisiä ja koestettuja turvallisuus-käytäntöjä, joiden avulla vastustajalta estetään kyky kerätä, analysoida ja käyttää hyväkseen tietoja, mm. puolustajan kyvyistä ja tavoitteista*"
- **Turvaa myös prosessit**
  - Käyttäjän tietoisuus uhista ja koulutus poikkeustilanteissa toimimiseen
  - Vain välttämättömät säännöt
  - … mutta tarkoin toteutetut
  - Hyvin määritellyt poikkeukset (prosesseihin ja sääntöihin)



17

OPSEC-termi on peräisin USA:n sotilaspuolelta, kun he huomasivat että vihollinen kokosi yhteen yksittäisiä sinänsä viattomia (ja suojaamattomia) tiedonpalasia päätelläkseen etukäteen USA:n operaatioiden toimeenpanoa. Tällaisia olivat esimerkiksi ennustettavat (ja helposti havainnoitavat) joukkojen rutiinit, hallinnollisen tietoliikenteen salaamattomuus, a turha tiedonjako.

Mitä kuuluu kyberturvallisuuteen?

- **Eri näkökulmia**
- **Tekninen**
  - Fyysinen turvallisuus
  - Verkkoturvallisuus
  - Sovellusturvallisuus
- **Järjestelmä**
  - Tietokantaturvallisuus
  - Mobiililaitteiden turvallisuus
  - Pilven turvallisuus
- **Suojattavat kohteet**
  - Liiketoimintatietojen luottamuksellisuus
  - Kriittisten järjestelmien suojaaminen
- **Prosessi**
  - Hyökkäämisen ja suojaamisen vaiheistus
- **Hallintanäkökulma**
  - Turvallisuushallintaohjelma
  - Riskienhallinta
  - Compliance

18

Kyberturvallisuutta voidaan käsitellä monesta eri näkökulmasta, riippuen optimoitavasta asiasta.

Ohessa esimerkkeinä sitä, mitä näkökulmia on ylipäätään olemassa: koska tämä kurssi keskittyy johtamiseen, niin näkökulmaksi valitaan hallinta ja prosessit. On hyvä kuitenkin tietää perusteet eri näkökulmien käsitteistä.

Mitä kuuluu kyberturvallisuuteen 2024?

CISSP	CompTIA Security+	CISO Mindmap 2024	NIST CSF	ISO 27001/2
Turvallisuus ja riskienhallinta	Hallinta, riski ja compliance	Hallinta (govn.)	Uhkan ja kohteiden *tunnistaminen*	Turvallisuus*johtaminen*
Suojattavien kohteiden turvallisuus	Uhkat, hyökkäykset ja haavoittuvuudet	Riskienhallinta	Kohteiden *suojaaminen*	Turvallisuusohjelman (ISMS) *suunnittelu*
Turva-arkkitehtuuri	Arkkitehtuuri ja suunnittelu	Turva-arkkitehtuuri	Toteutuvien uhkien *havaitseminen*	ISMS *liitynnät* organisaatiossa
Turvallisuuden arviointi ja testaus	Operaatiot ja hälytysvaste	Auditointi ja compliance	Hyökkäyksiin *vastaaminen*	ISMS *operointi*
Tietoliikenneturvallisuus	Toteutukset	Automatisointi ja analytiikka	Hyökkäyksistä *toipuminen*	ISMS *arviointi*
Identiteetinhallinta (IAM)		Identiteetinhallinta		ISMS *parantaminen*
SecOps		SecOps		*Organisaation* kontrollit
Turvallinen ohjelmistonkehitys		Tuotekehityksen turvallisuus		*Henkilöön* kohdistuvat kontrollit
		Etätyö		*Fyysiset* kontrollit
		Tekoäly		
		Liiketoimintasov.		
		Kybertiimin hallinta ja brändi		
		HR ja laki		

19

Käytännössä eri näkökulmat kuitenkin suodattuvat eri rooleihin eri tavalla eri aikoina. Tässä taulukossa näkyy jaottelu kolmentyyppisestä näkökulmasta: CISSP ja Security+ ovat yleisiä kyber-/tietoturvallisuuden sertifiointeja; CISO Mindmap on kooste tyypillisen organisaation informaatio-(/kyber-)turvallisuusjohtajan tehtäväkentästä (tarkemmin edempänä) ja kolmantena sääntelijän ohjeistus siitä, millä tavalla kyberturvallisuutta tulisi lähestyä. NIST CSF ja ISO 27k ovat nimenomaan hallinnan standardeja, ja käyn niitä lävitse tarkemmin jäljempänä.

Verrattuna n. 10 vuoden takaiseen, yksittäiset teknologiat tai jopa teknologiaryhmät ovat piiloutuneet toimintojen alle, joita taas nykyisin jaotellaan nk. Kill-chainin mukaisesti (eli tyypillisen hyökkäyksen kulkemisen perusteella) tai turvallisuusfunktioiden perusteella: esimerkiksi kontrollien jaottelu, tai yleinen prosessin kypsyysmallin mukainen jaottelu.

Uusimmat teknologiat kulkevat näissä kehyksissä mukana yleensä itsenäisinä, kunnes on selvää, mikä on ko. Teknologian pääasiallinen merkitys turvallisuusfunktioiden kannalta. Näitä teknologioita ovat toistaiseksi tekoäly, pilviteknologiat ja IAM.

CISO Mind map 2024

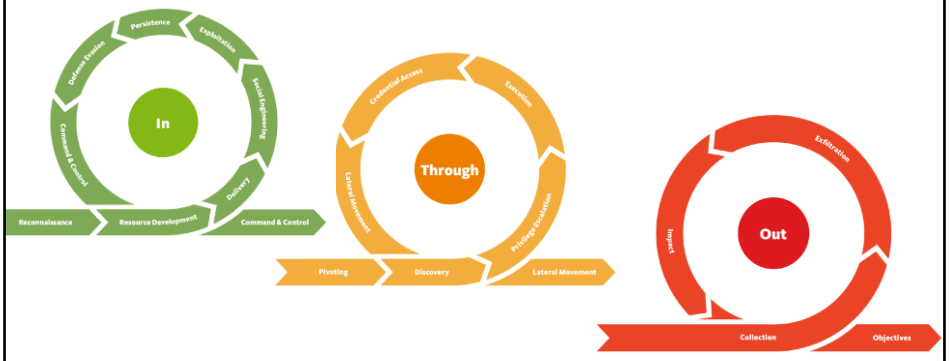
https://rafeeqrehman.com/ciso-mindmap/

(ladatkaa itsellenne kopio, ja tutustukaa alueisiin)

20

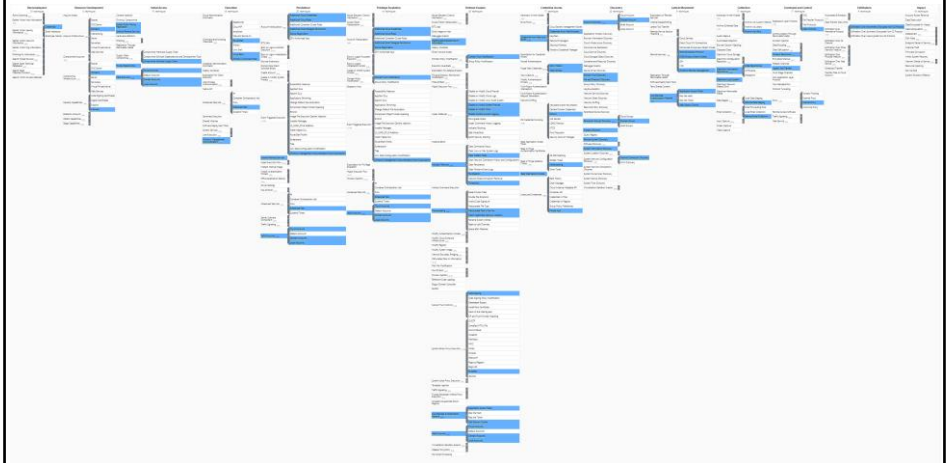
Seuraavissa kalvoissa käyn lävitse kyberjohtamisen osa-alueita kursorisesti. On hyvä tiedostaa, että kovin monet osa-alueet vaativat erityisosaamista, esimerkiksi kryptografia.

Miltä näyttää monivaiheinen kyberhyökkäys?



21

Esimerkki toimitusketjuhyökkäyksestä: Solarwinds



22

Tämä on MITRE ATT&CK-kehikon mukainen näkymä erääseen ohjelmistojen toimitusketjuja vastaan kohdistuneeseen kyberhyökkäykseen (Solarwinds). Solarwinds-hyökkäyksessä. SolarWinds on yritys joka tekee erilaisia verkonhallintatyökaluja organisaation IT-ylläpitäjille. Hyökkääjä oli murtanut ohjelmiston toimitusketjussa useamman organisaation tuotekehityspalvelimia ja saanut ujutettua takaportitettuja ohjelmia kymmeniin tuhansiin organisaatioihin, mukaan lukien USA:n valtionhallinto. Hyökkäyksen tekijä oli todennäköisesti Venäjän SVR:n (ulkomaantiedustelu) rahoittama ja ohjaama uhkatoimija nimeltään Cozy Bear (/ APT29 / Midnight Blizzard).