Tieto- ja kyberturvallisuuden perusteet

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

TURKU AMK

Euroopan unionin rahoittama

NextGenerationEU

Rahoittaja

Jatkuvan oppimisen ja työllisyyden palvelukeskus

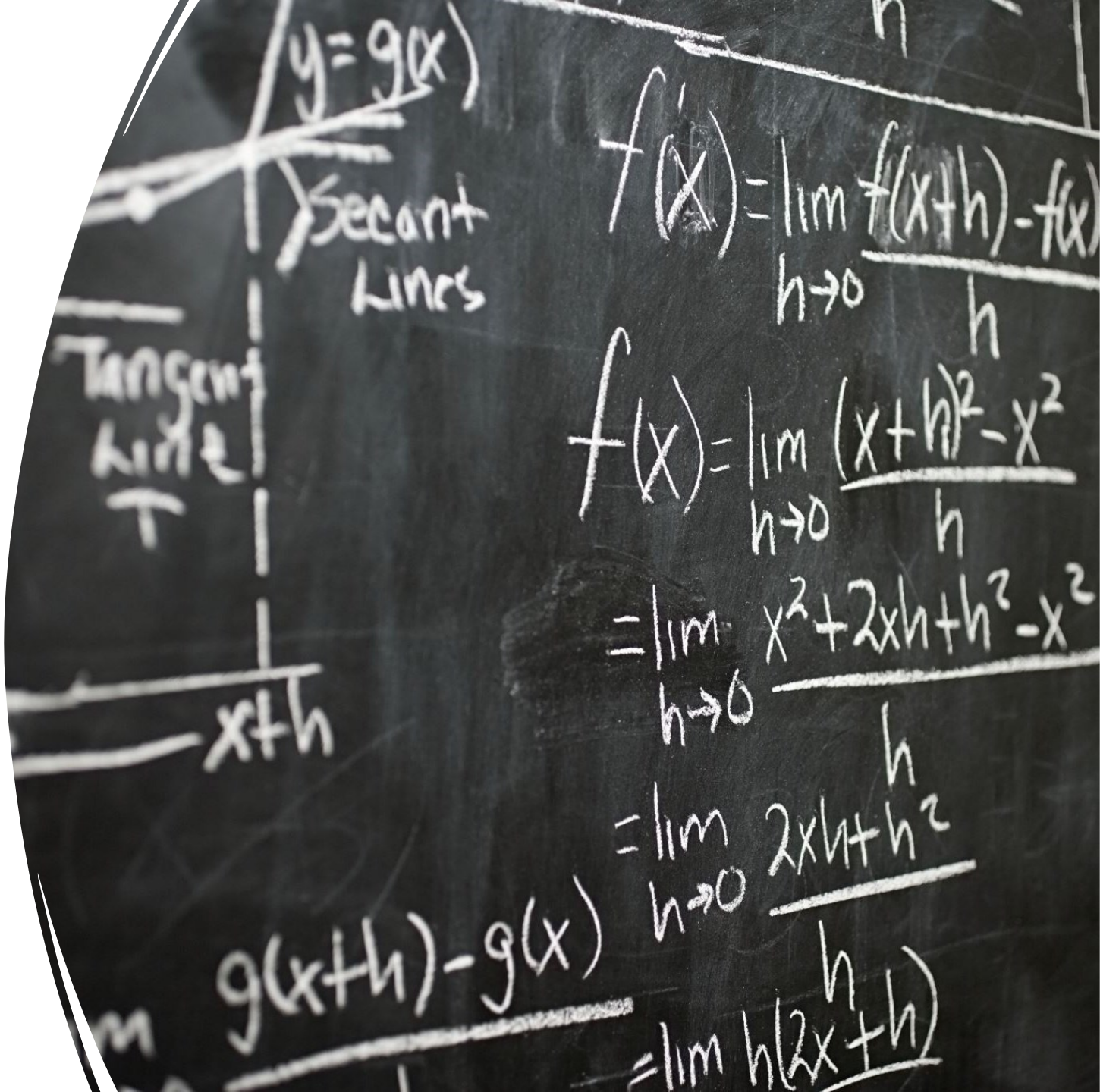
Koulutus on rahoitettu Euroopan unionin elpymis- ja palautumistukivälineellä (RRF), joka on EU:n elpymisvälineen (Next Generation EU) suurin ohjelma. Rahoituksen on myöntänyt Jatkuvan oppimisen ja työllisyyden palvelukeskus. Palvelukeskuksen tehtävänä on edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta sekä vastata nopealla toiminnalla työmarkkinoiden äkillisiin rakennemuutoksiin. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

Tavoitteet

- Opintojakson suoritettuaan opiskelija
  - Osaa nimetä ja selittää tieto-ja kyberturvallisuuden peruskäsitteet
  - Tunnistaa toiminta- ja uhkaympäristön ja osaa arvioida tieto-ja kyberturvallisuuden vaikutusta organisaation toimintaan
  - Osaa laatia organisaatiolle tietoturvapolitiikan ja ottaa sen käyttöön
  - Osaa luokitella tietoa ja tietojärjestelmiä
  - Ymmärtää osaamisen merkityksen tieto-ja kyberturvallisuuden toteutumisessa
  - Osaa laatia organisaatiolle koulutussuunnitelman ja arvioida sen vaikuttavuutta
  - Tunnistaa riskienhallinnan merkityksen tieto-ja kyberturvallisuuden toteutumisessa
  - Tunnistaa tekniset peruskäsitteet

Arviointi

- Palautetut tehtävät arvioidaan asteikolla 0-5
- Arvosana on tehtäväpalautusten keskiarvo
- Mediaseuranta ja tietoturvatapahtuma –etätehtävät arvioidaan hyväksytty/hylätty



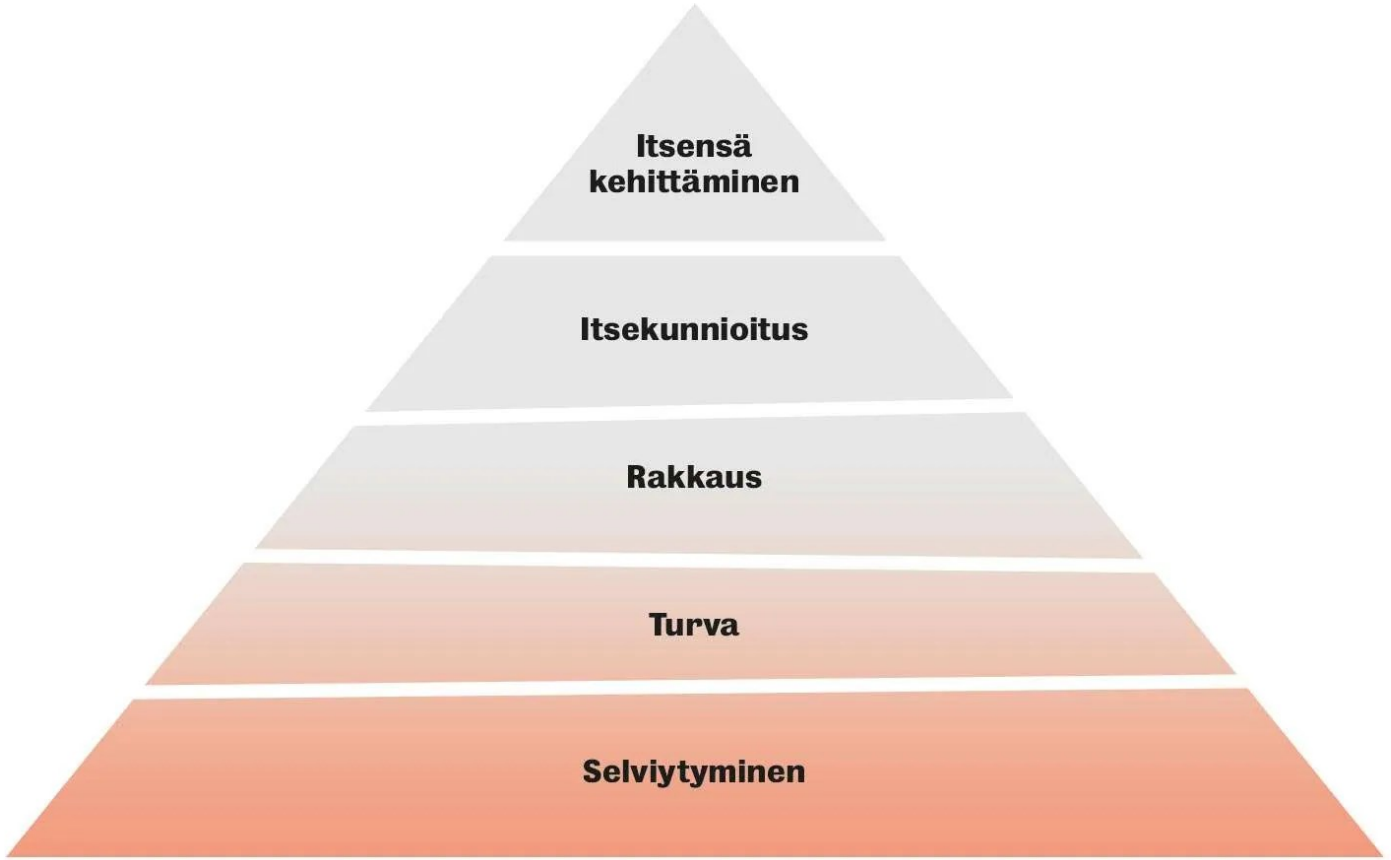
Käsitteet


tietojärjestelmä
kyberturvallisuus
tieto
tietoverkko
käytettävyys
resilienssi
saatavuus
kyberhyökkäys
hybridivaikuttaminen
kybervaikuttaminen
kyberpuolustus
tietoturva
eheys
kyberrikollisuus


INFORMATION
CYBER SECURTY

Turvallisuus – tietoturvallisuus - kyberturvallisuus

TURKU AMK

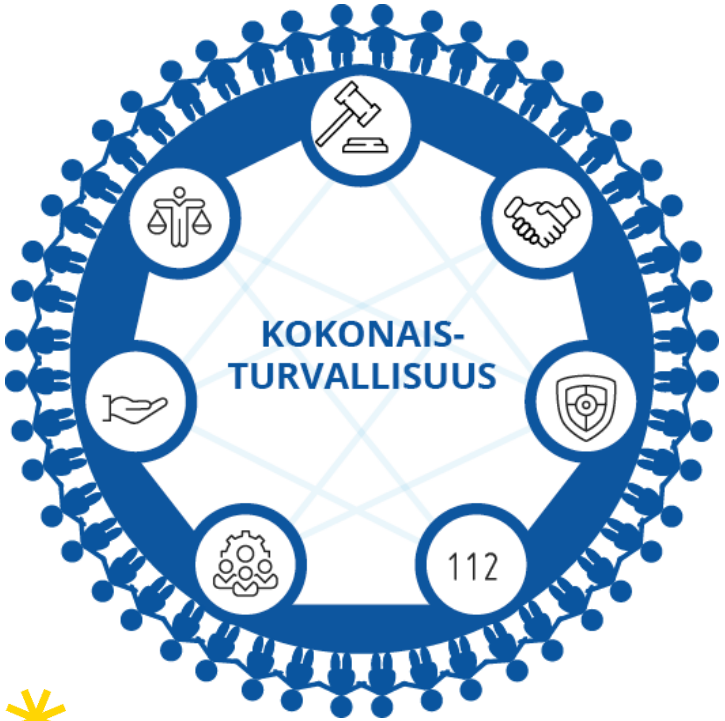


Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Mistä/miten turvallisuus syntyy?

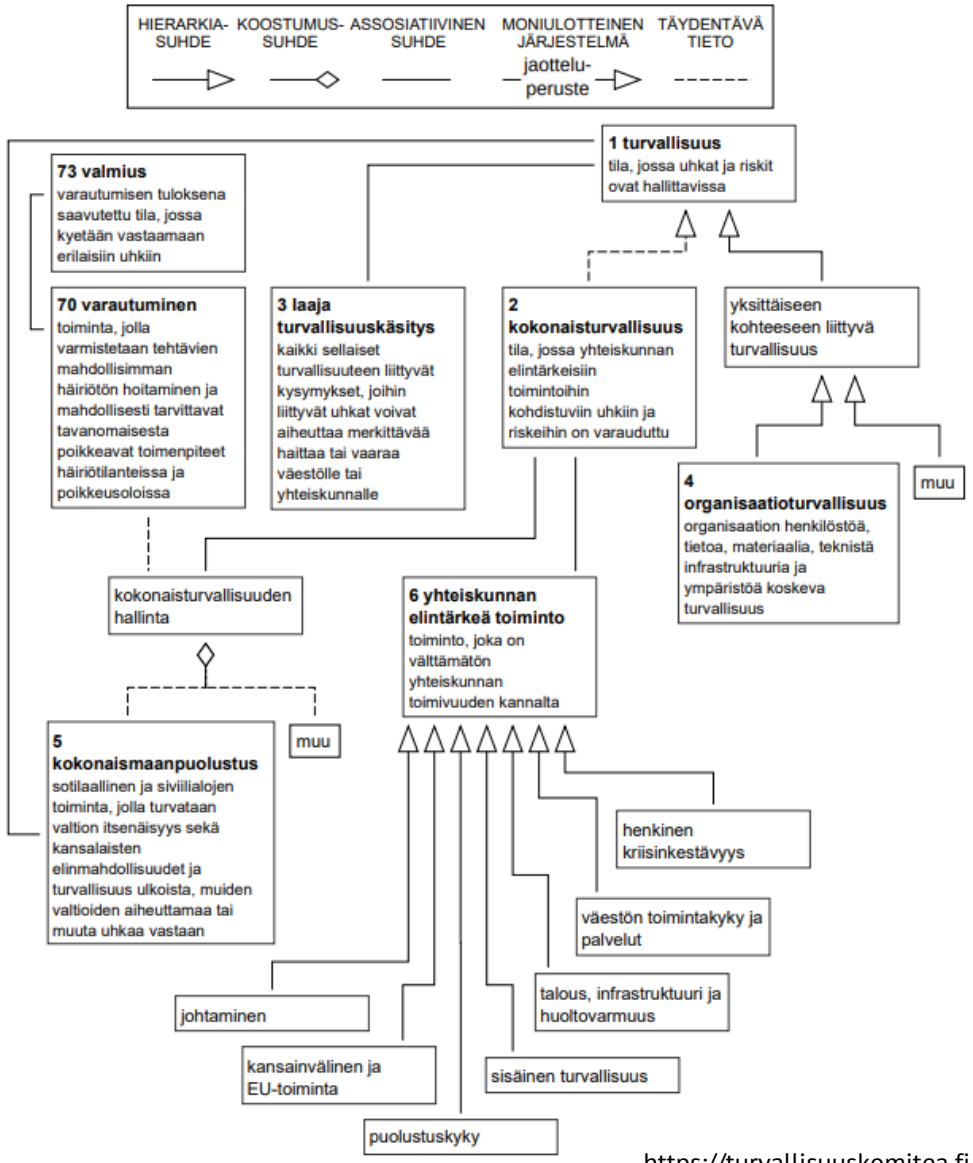
- Tunne
- Resilienssi
- Kulttturi
- Toimintaympäristö



TURKU AMK

1 KOKONAISTURVALLISUUS

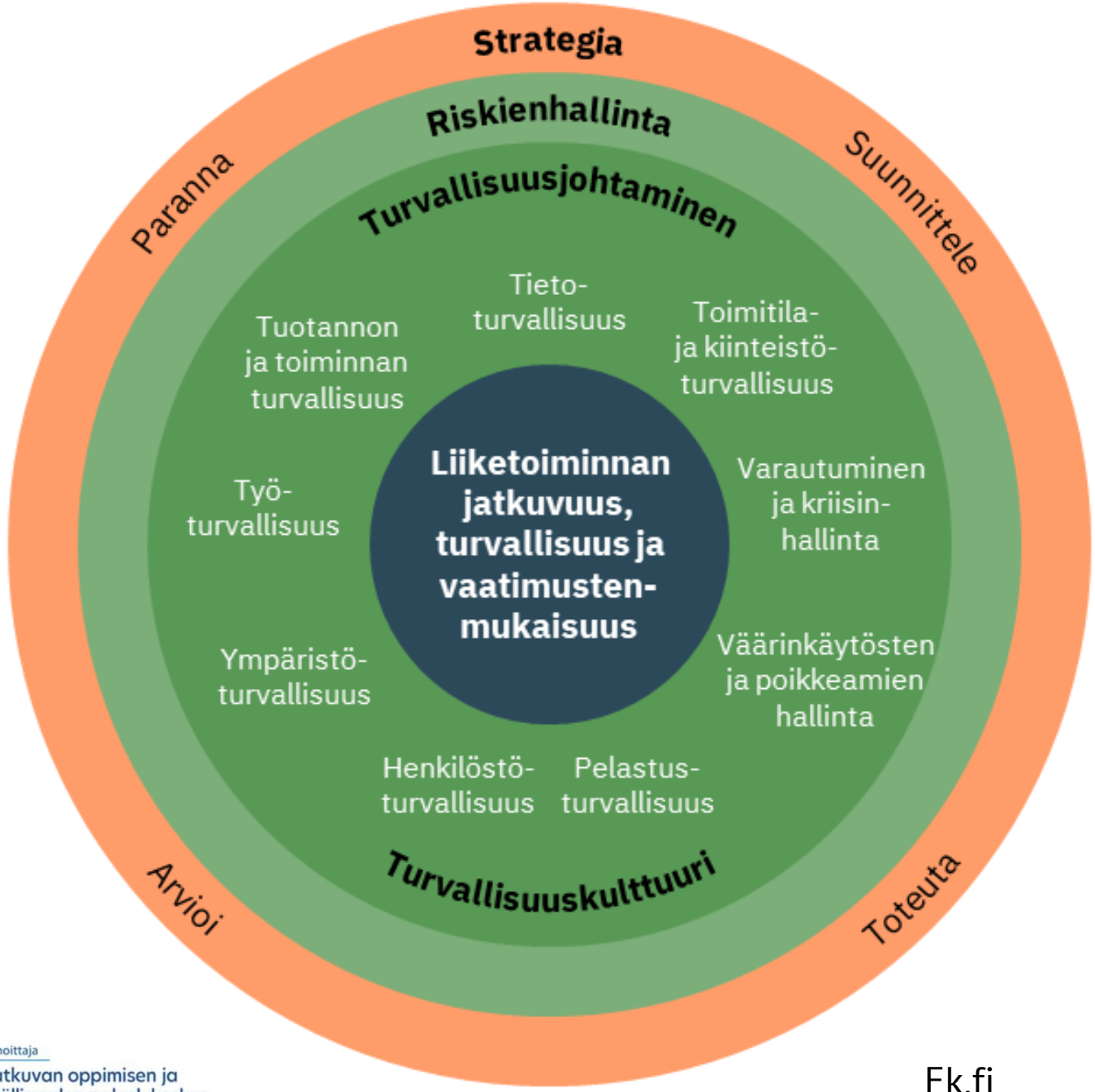
1.1 Yleisiä käsitteitä



Käsitekaavio 1. *Kokonaisturvallisuus.*

https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Turvallisuus kokonaisuutena



TURKU AMK

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Ek.fi

Tietoturvallisuus - perusperiaatteet

TURKU AMK

Saatavuus
- Tieto tai palvelu on käytettävissä silloin, kun sitä tarvitaan

Luottamuksellisuus
- Tietoja pääsevät näkemään vain ne, joilla on siihen oikeus

Eheys
- Sisällön oikudettoman muuttumattomuuden varmistamista
- Järjestelmät toimivat siten, kuin niiden on tarkoitettu toimivan

https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

IAAA –periaate (todentaminen ja kiistämättömyys)

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Access control is composed of

- The ***I*dentification** of the user
- The ***A*uthentication** of the user
- The ***A*uthorization** of the user
- The ***A*ccounting**

- **Käyttövaltuuksien todistaminen**
- **Tiedon kiistämättömyys**

Tätä ei odottaisi it-jätiltä: Käyttäjätunnus: admin, salasana: admin

21.10.2019 19:37 TIETOTURVA SALASANAT DIGITALOUS

Näinhän se olisi vielä vaivattomampaa.

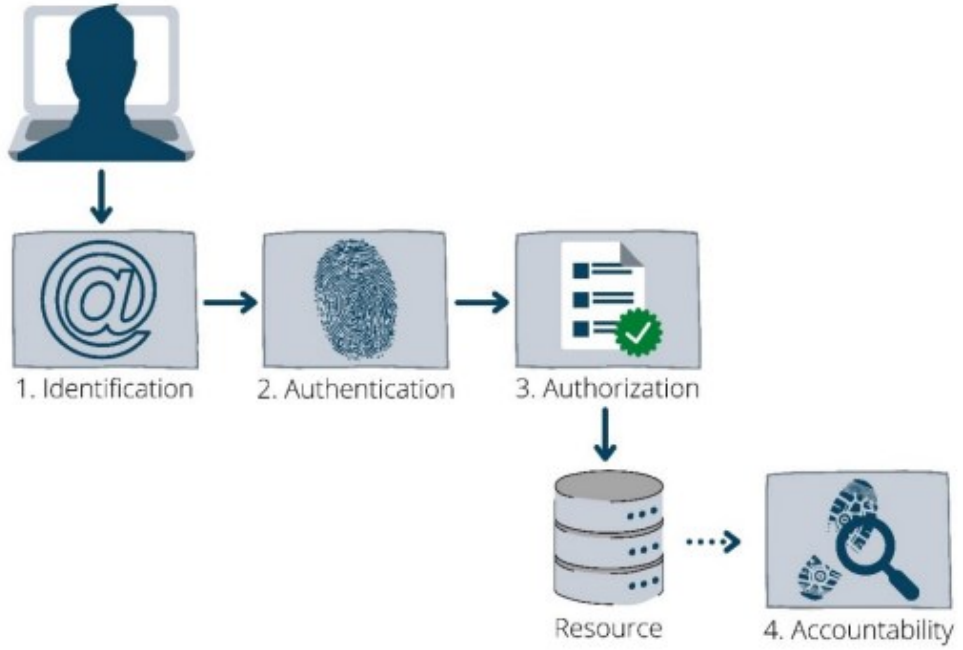
Yhdysvalloissa ja vähän muuallakin toimiva Equifax sai runsaasti julkisuutta pari vuotta sitten, kun sen järjestelmiin tehtiin järkyttäviin mittoihin paisunut tietomurto.

Rikokset

Vastaamon Malmin toimipisteessä luotiin vuonna 2012 työasemille salasana "malmi70" – sitten sitä käytettiin kaikkialla vuosien ajan

Keskusrikospoliisin esitutkinta paljastaa, että Vastaamon tietoturva oli olematonta. Salasanat olivat alkeellisia, ja eräällä käyttäjätunnuksella sellaista ei ollut lainkaan.

Psykoterapiakeskus Vastaamon entinen toimitusjohtaja Ville Tapio Helsingin käräjäoikeudessa 2.3. vierellään asianajaja Liina Kokko. Kuva: Jouni Immonen / Yle



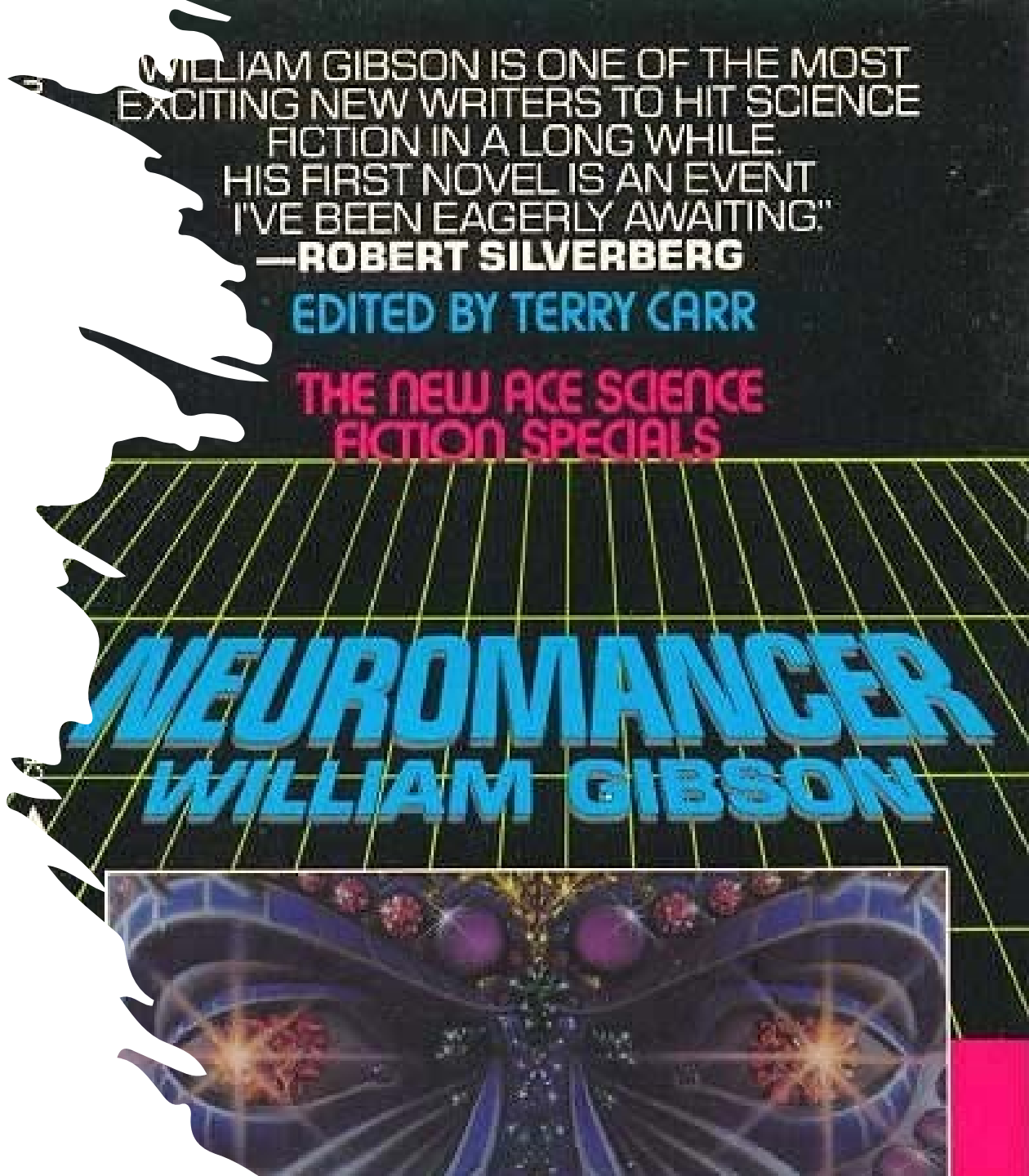
Kuva 2. IAAA-kehys.

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

”Cyber”

- Term cyberspace coined by William Gibson in 1984.
  - Sci-Fi genre called cyberpunk



Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Määritelmät

- **Kyberturvallisuus** keskittyy tiedon, tietojärjestelmien ja laitteiden turvallisuuden takaamiseen verkkoympäristössä.

- **Tietoturvallisuus** kattaa tiedon turvaamisen laajemmin. Tietoturvaan kuuluvat myös tiedon fyysinen tallentaminen ja tietoon pääsyn rajoittaminen digitaalisen ympäristön ulkopuolella.

- Kyberturvallisuuden ja tietoturvan uhat ovat osin erilaisia. Siinä missä kyberturvallisuus pyrkii estämään haitta-ohjelmien kaltaisten haittojen aiheuttamia vahinkoja, tieto-turvaan kuuluu myös kaikenlaisen **tiedon levittämisen sekä väärän tiedon torjunta**. (F-Secure)

Cyber security (NIST definition)

Cyber Security: The ability to protect or defend the use of cyberspace from cyber attacks.

Cyberspace: 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.

Cyber attack: 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.

"Kyberturvallisuus"

tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan

- Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä **tietoturva on keskeinen tekijä**.

- Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. [..] kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Keskeiset tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden, määritellään Suomen kyberturvallisuusstrategiassa (valtioneuvoston periaatepäätös 24.1.2013).

Euroopan unionin rahoittama
NextGenerationEU

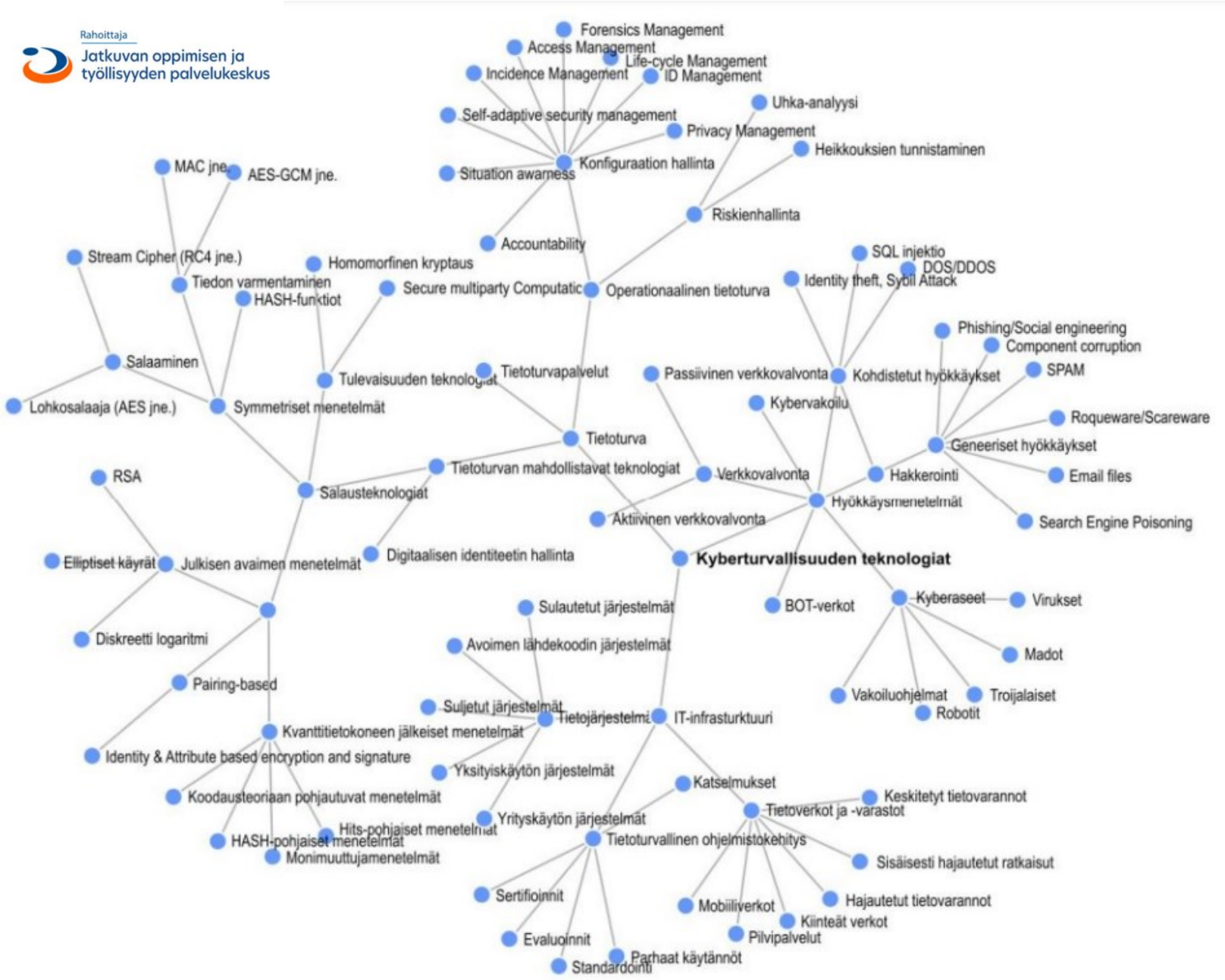
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

TURKU AMK

Kaavio 1 – Kyberturvallisuus liittyy tietoturvaan ja tietotekniikan turvallisuuteen

Lähde: Euroopan tilintarkastustuomioistuin.

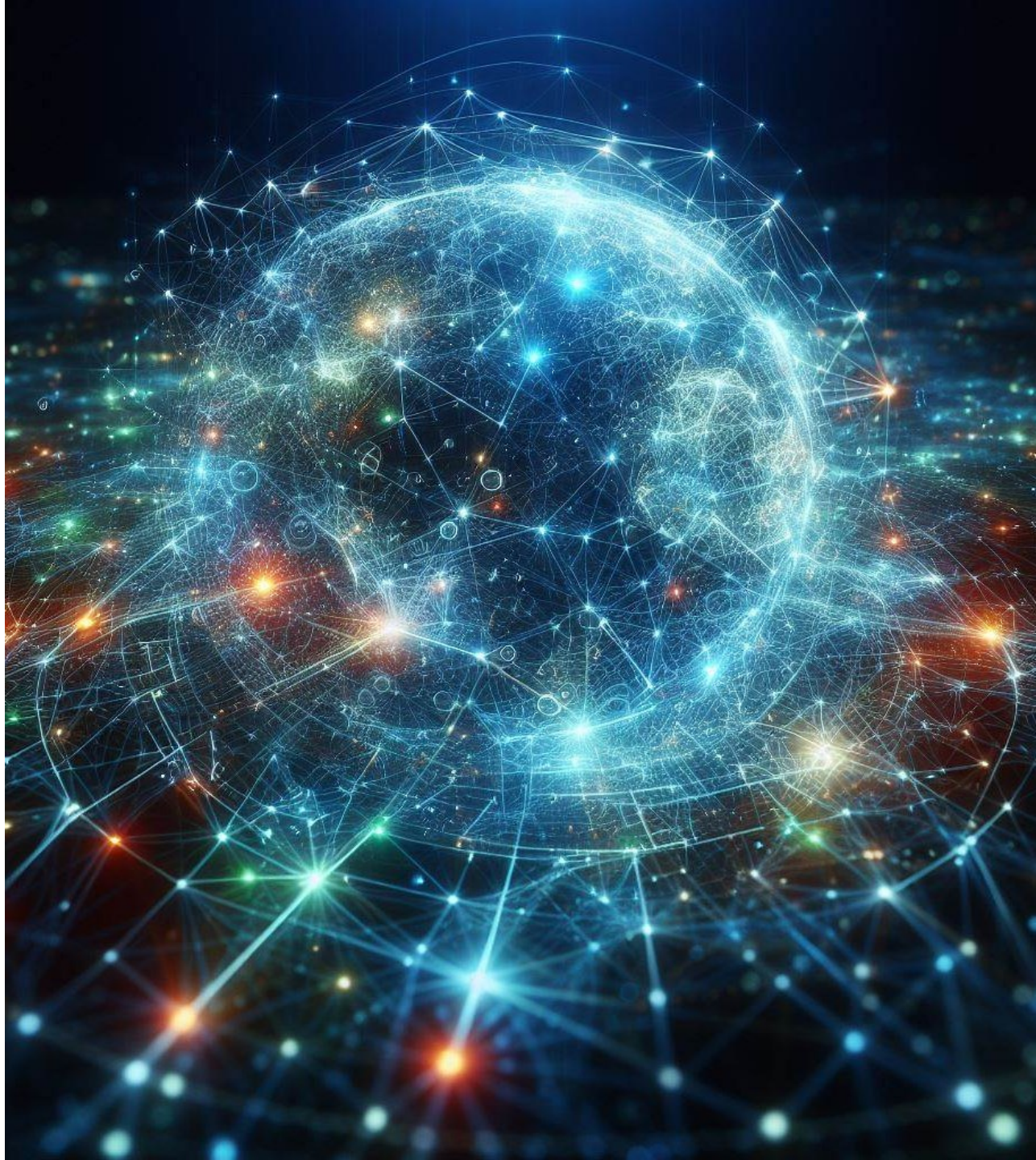
Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus



Kuva 1.2. Kyberturvallisuuden teknologiat, käsitekartta.

Kyberiä?

Toiminta- ja uhkaympäristö

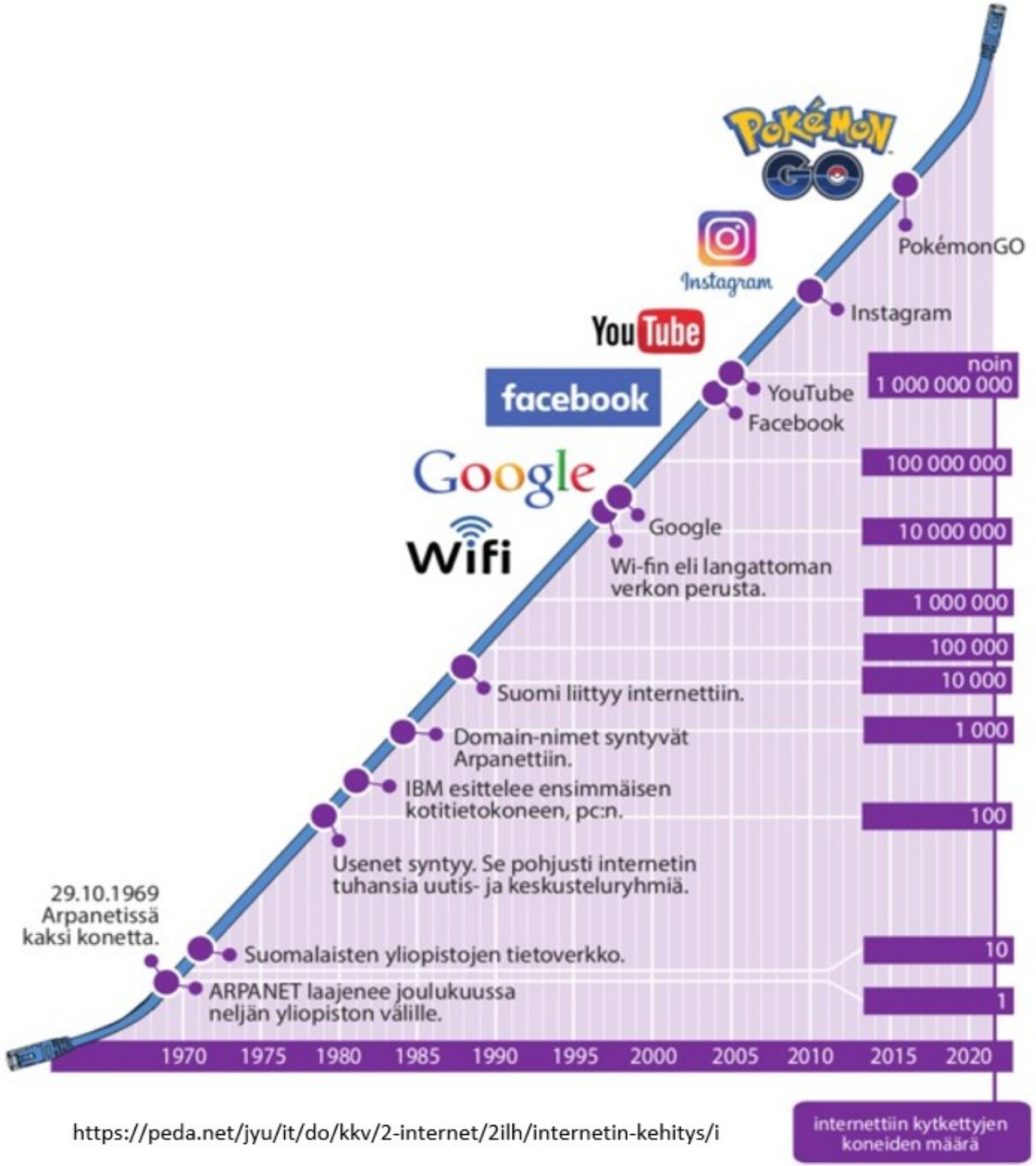


TURKU AMK

Maailmanlaajuinen toimintaympäristö

Toimintaympäristö

- Vuonna 2023 oli noin 13,1 miljardia Internetiin kytkettyä laitetta, joista suurin osa oli IoT-laitteita eli esineiden internetin laitteita, kuten älykelloja, termostaatteja, turvakameroita muita älykkäitä laitteita



https://peda.net/jyu/it/do/kkv/2-internet/2ilh/internetin-kehitys/i

Euroopan unionin rahoittama
NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Kyberuhka - peruskäsitteet

ULKOMAAT

Vaihto-opiskelijan kohtalo USA:ssa paljasti järkyttävän rikostrendin: "Voi tapahtua kenelle vain"

Asiantuntijat huolestuivat yleistyvästä rikostrendistä.

Kybersieppauksia on tapahtunut ainakin Yhdysvalloissa, Kanadassa ja Australiassa. Kuvituskuva. MOSTPHOTOS

Käsite	Selite
Kybertoimintaympäristö, kyberympäristö (Cyber environment)	Kybertoimintaympäristö on monimutkainen ja monikerroksinen maailmanlaajuinen informaatioverkosto. Kybertoimintaympäristössä on monenlaisia toimijoita; kansallisia turvallisuusviranomaisia, yritysten ja julkishallinnon kommunikaatioverkkoja sekä teollisuuden ja kriittisen infrastruktuurin valvontajärjestelmiä.
Kyberuhkien aiheuttaja (Cyber attacker)	Kyberuhkien aiheuttajia ovat kaikki ne toimijat, jotka voivat toimissaan onnistuessaan aiheuttaa riskin arjen toimintojen ja palveluiden käytettävyydelle, toimivuudelle, eheydelle, saatavuudelle, luotettavuudelle, tunnistettavuudelle ja varmennettavuudelle. Kyberuhkien aiheuttajat luokitellaan tyypillisesti toimintamotiivien perusteella.
Kybermaailma (Cyber world)	Kybermaailmalla tarkoitetaan toisiinsa kytkettyjen tietokoneiden kommunikaation maailmaa.
Kyberuhka (Cyber threat)	Kyberuhka on sellainen uhka, joka toteutuessaan vaarantaa yhteiskunnan elintärkeän toiminnon tai muun kybertoimintaympäristöstä riippuvaisen toiminnon.
Kyberturvallisuus (Cyber security)	Kyberturvallisuus on tila, jossa kybertoimintaympäristöstä koituvat uhkat ja riskit ovat hallinnassa
Kyberisku (Cyber attack)	Kyberiskulla tarkoitetaan sellaista hyökkäystä, joka kohdistuu kybertoimintaympäristöön ja sen mahdollisesti ohjaamiin fyysisen maailman toimintoihin. Kyberhyökkäys voi kohdistua esimerkiksi ydinvoimalan ohjausjärjestelmään, elintarvikkeiden kuljetus- ja logistiikkajärjestelmään, liikenteen ohjausjärjestelmään tai pankki- ja maksujärjestelmään.

https://peda.net/jyu/it/do/kkv/4kjna

Onko tieto- ja kyberturvallisuuden asema tai kulttuuri organisaatioissanne muuttunut viimeisen vuoden aikana?

Entä julkisessa puheessa?

Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Kyberuhkien jaottelu

Digitaaliset, fyysiset, taloudelliset:

- julkiseen hallintoon
- logistiikkajärjestelmiin
- raha- ja maksujärjestelmiin
- tietoliikenne- ja tietojärjestelmiin
- elintarvikehuoltoon
- terveydenhuoltoon

- yhdyskuntatekniikan palveluihin
- rajaturvallisuuteen
- yleiseen järjestykseen ja turvallisuuteen
- vesi-, energia- ja voimahuoltoon tai
- sisäiseen turvallisuuteen pelastusviranomaisten ja sotilaskohteiden ja -toimintojen kautta

https://peda.net/jyu/it/do/kkv/4kjna/4kj

Informaatio- ja hybridivaikuttaminen

- Propaganda
- Disinformaatio
- Manipulointi
- Valeuutiset

Turvapaikanhakijoita saapui Venäjältä raja-asemille marraskuussa. Tällä hetkellä itäraja on kiinni.
KUVA: KALLE KOPONEN / HS

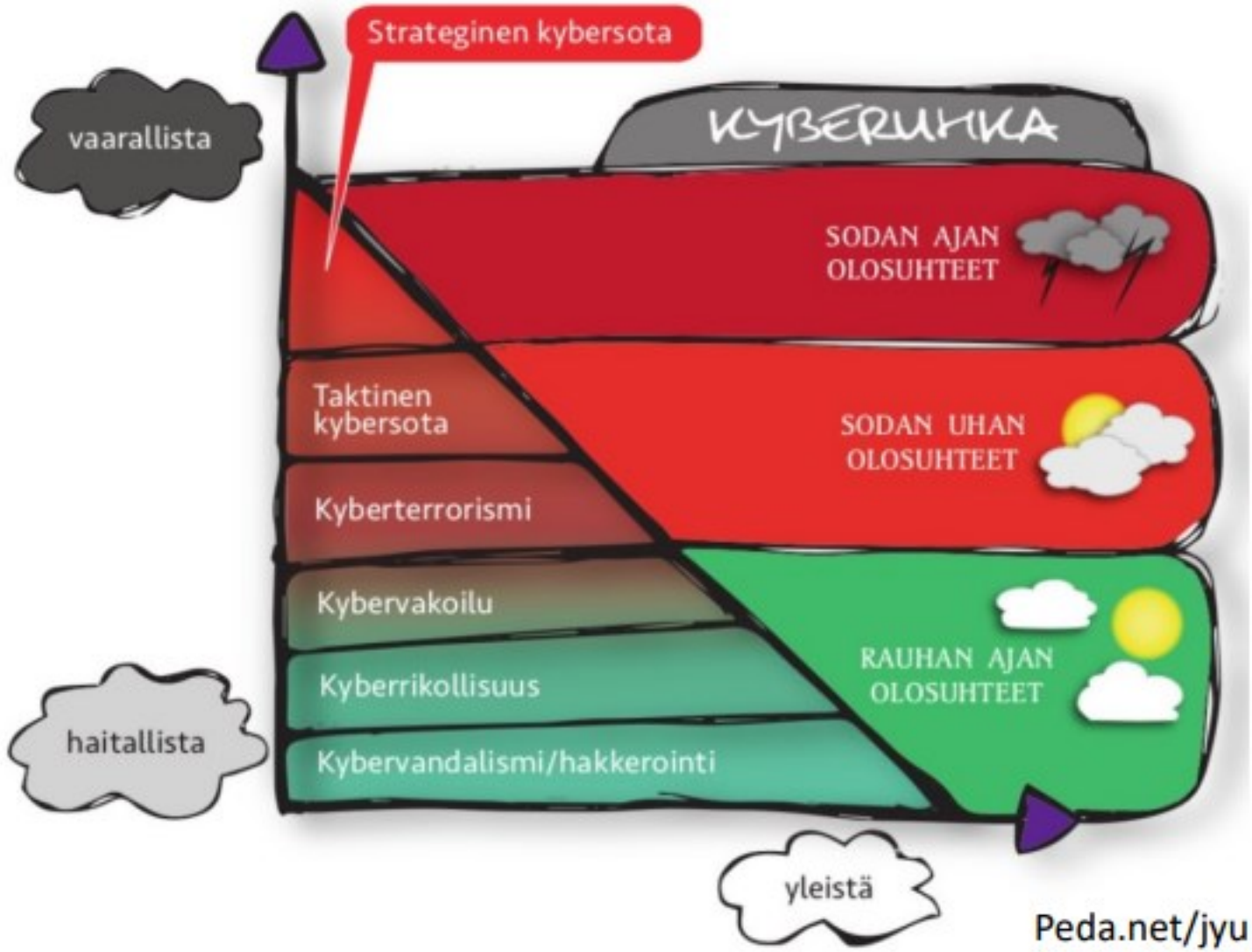
- Taloudellinen painostus
- Kyberhyökkäys
- Operaatiot
- Diplomaattiset toimet

”Disinformaatio-operaatiot eivät ole käärmeitä, jotka tapetaan katkaisemalla pää, vaan myrkkysienirihmastoja. Paras tapa torjua niitä on muovata maaperä sellaiseksi, ettei se houkuttele myrkkysieniä”

Sofi Oksanen, HS 31.12.2023

Kyberuhkien tasot, motiivit ja kohteet

- **Valtiot: Venäjä, Kiina, Turkki, ym.**
  - Valtiollisen tason tiedon kerääminen
  - Päätöksentekoon vaikuttaminen
  - → Viranomaiset, kansa, yksilöt
  - → Sotilaallinen toimintakyky
- **Valtioiden tukemat rikollisryhmät**
  - Yhteiskunnan epävakaus
  - Valtion agendan tukeminen
  - → Kriittinen infra
  - → Teollisuus-/yritysvakoilu → Toimitusketjut
- **Rikolliset hakkerit ja haktivistit**
  - Raha
  - Ideologiat
  - → Yksityinen sektori
  - → Ideologioiden mukaiset kohteet
  - → Haavoittuvuudet



Peda.net/jyu

Uhkaympäristö

Toimitusketjuhyökkäyksissä yritykseen tai julkiseen organisaatioon yritetään tunkeutua yhteistyökumppanin tai alihankkijan kautta. Suomalaistenkin organisaatioiden kannattaa varautua tähän kasvavaan kyberuhkaan, kirjoittaa Supon ylitarkastaja Sari Sarani.

Toimitusketjuhyökkäys voi kuulostaa etäiseltä ja hankalalta asialta. Se on kuitenkin hyvin konkreettinen nykypäivän kyberuhka, johon suomalaistenkin yritysten ja julkisten organisaatioiden on syytä varautua. Jos toimitusketjuhyökkäys kohdistuu kriittiseen toimijaan, sillä voi olla vaikutuksia isojenkin ihmisjoukkojen elämään myös Suomessa.

TIETOTURVA

KSML: Kyberhyökkäys keskeytti traktorien valmistuksen Ääne-koskella

Valtran emoyhtiö vahvistaa kyberhyökkäyksen, joka Keskisuomalaisen mukaan sulki traktorien tuotannon Äänekoskella.

JAA

Traktorien tuotantoa Suolahdella. KUVA: ESKO SIEKKINEN

Nordeaan kohdistunut kyberhyökkäys oli "poikkeuksellisen hyvin toteutettu", sanoo asiantuntija – hyökkääjän taustoista ei tietoa

Nordean mobiili- ja verkkopankeissa oli tiistaina häiriöitä poikkeuksellisen pitkään. F-securen Mikko Hyppönen suosittelee mobiilivarmenteen käyttöä, jotta tunnistautuminen ei riippuisi pankeista.

Kyberuhka

Verkkohyökkäys voi lamaannuttaa sairaalan – esimerkkejä löytyy jo Suomestakin

Tietojärjestelmään ujutettu haittaohjelma, palvelunestohyökkäys, hakkerointi. Siinä muutamia ulkopuolelta tulevia uhkia, joihin myös sairaaloiden pitää varautua.

Kuva: Jarmo Honkanen / Yle

Tietojen kalastelu

AKA: Email spoofing, Social engineering, Identity theft

Uhkataso: Hyvin korkea / Kriittinen

Tietojen kalastelu (engl. phishing) on vilpillinen yritys hankkia arkaluontoisia tietoja, kuten salasanoja, esittämällä hyvämaineista toimijaa.

Salasana-hyökkäykset

AKA: Compromised credentials, Password cracking

Uhkataso: Korkea / Kohonnut

Tunnuksia on niin moneen paikkaan, että samoja käyttöoikeustietoja käytetään uudelleen ja uudelleen. Tämä on tosiasia, jota hyökkääjät hyödyntävät.

Työntekijöiden huolimattomuus

AKA: Human error, Bad security behaviour

Uhkataso: Normaali / Varautunut

Usein tietovuodot syntyvät vahingoista, esimerkiksi työntekijän kadottaessa mobiililaitteen tai työskennellessä suojaamattomassa Wi-Fi-yhteydessä.

Haittaohjelmat

AKA: Viruses, Trojan Horses, Spyware, Worms

Uhkataso: Korkea / Kohonnut

Haittaohjelma (engl. malware) on yleisnimitys ei-toivotuille ohjelmille. Virukset, botit, troijalaiset, rootkitit ja madot ovat eri tyyppisiä haittaohjelmia.

Business-email-compromise

AKA: Email fraud, CEO scams, Invoice scams

Uhkataso: Hyvin korkea / Kriittinen

Työntekijän sähköposti pyritään joko saamaan haltuun tai sitä esitetään pyytääkseen kollegoja tai kumppaneita tekemään tekaistuja pankkisiirtoja.

Sisäpiiri-hyökkäykset

AKA: Malicious employees, Internal cyber attacks

Uhkataso: Korkea / Kohonnut

Työntekijät (ex-työntekijät, toimittajat, jne.) voivat olla merkittävä uhka ajatellessaan hyötyvänsä meihin kohdistuvista haitallisista toimistaan.

Kiristyshaitta-ohjelmat

AKA: Encryption ransoms, CryptoWalls

Uhkataso: Hyvin korkea / Kriittinen

Kiristyshaittaohjelma (engl. ransomware) on haittaohjelma, joka salaa uhrin tiedostot ja tarjoaa pääsyä tiedostoihin ainoastaan lunnasmaksua vastaan.

Väärät pääsyoikeudet

AKA: Wrong priviliges, Poor identity governance

Uhkataso: Normaali / Varautunut

Pääsy- ja käyttöoikeuksien hallinta luo työntekijöille digitaalisen identiteetin. Vanhentuneet tai väärät pääsyoikeudet ovat kuin lahja hakkereille.

Väärinkonfiguroitu pilvitallennustila

AKA: Default credentials or conf, Missing access control

Uhkataso: Korkea / Kohonnut

Väärin konfiguroidut pilvipalvelimet voivat paljastaa arkaluontoisia tietoja. Tämä on yleinen virhe, joka on hakkereille kuin avoin kutsu satuttaa organisaatiota.

Paikkaamattomat haavoittuvuudet

AKA: Security patches, Software updates

Uhkataso: Hyvin korkea / Kriittinen

Korjaustiedostoilla paikataan koodin teknisiä haavoittuvuuksia. Julkaistut, mutta korjaamattomat haavoittuvuudet ovat erityisen vaarallisia.

Man-in-the-Middle -hyökkäykset

AKA: Wi-Fi spoofing, IP spoofing, eavesdropping

Uhkataso: Normaali / Varautunut

Man-in-the-Middle (MitM) -hyökkäys tapahtuu, kun hyökkääjä sujauttaa itsensä mukaan tietojenvaihtoon esim. tietokoneen ja palvelimen välillä.

Denial-of-service -hyökkäykset

AKA: Botnet attacks, Traffic floods, Zombie network attacks

Uhkataso: Korkea / Kohonnut

Denial-of-service (DoS) -hyökkäyksessä verkkosivustolle sysätään enemmän liikennettä kuin se pystyy käsittelemään.

Euroopan unionin rahoittama
NextGenerationEU
Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Toimitusketju-hyökkäykset

AKA: Third-party attacks, Watering hole attacks

Uhkataso: Korkea / Kohonnut

Toimitusketjuhyökkäyksessä pyritään vahingoittamaan organisaatiota kohdistamalla hyökkäys toimitusketjun heikompiin osiin.

Hyödyllisiä linkkejä

- Traficom – Kyberturvallisuuskeskus: Etusivu | Traficom (kyberturvallisuuskeskus.fi)
- ENISA – European Union Agency for Cybersecurity: ENISA (europa.eu)
- NIST – National Institute of Standards and Technology: Cybersecurity | NIST
- Sisäministeriö: https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyber-ja-informaatiovaikuttaminen-saman-kolikon-kaksi-puolta
- https://julkaisut.valtioneuvosto.fi/handle/10024/161512