

Liiketoiminnan riskihallittuun kehittämisen ratkaisukuvauksia pohjautuen “DigiTurvaMatriisiin”

Riski-Digi –hanke 2021

Juha Arrasvuori
Matti Pyykkönen



Vipuvoimaa
EU:lta
2014–2020



Teknologian riskejä

DIGIRISKIT

TEKNISET HÄIRIÖT

Käyttökeskeytys,
yhteyshäiriöt

TIETOTURVA

Tietovarkaudet,
teollisuusvakoilu,
tietovuodot

PALVELUNESTO

Estohyökkäykset,
tietoliikenne-häirintä

TALOUS- RIKOLLISUUS

Kiristys, Petos,
Identiteetti-
varkaudet

KYBER- RIKOLLISUUS

Virukset ja
Hakkerointi

- ✓ **Tekniset häiriöt:** Käyttökeskeytys, yhteyshäiriöt
- ✓ **Tietoturva:** Tietovarkaudet, teollisuusvakoilu, tietovuodot
- ✓ **Palvelunesto:** Estohyökkäykset, tietoliikennehäirintä
- ✓ **Talousrikollisuus:** Kiristys, Petos, Identiteettivarkaudet
- ✓ **Kyberrikollisuus:** Hakkerointi ja virukset

DigiTurvaMatriisi

TEKNOLOGIAT DIGI RISKIT	VERKKO Tietoliikennetekniikka, verkkoyhteydet , viestintä, kommunikaatio ja telepresens	TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot	KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly	AUTOMAAATIO IoT, Sensorit, robotiikka, etäkäyttö ja etävalvonta	VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnaolo (metaversumi)
TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyshäiriöt					
TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot					
PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä					
TALOUS- RIKOLLISUUS Kirstytys, petos, Identiteetti- varkaudet					
KYBER- RIKOLLISUUS Virukset ja Hakkerointi					

DigiTurvaMatriisi

TEKNOLOGIAT DIGI RISKIT	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio ja telepresens	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly	4. AUTOMAAATIO IoT, Sensorit, etäkäyttö ja etävalvonta	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi)
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyshäiriöt	#1a	#2a	#3a	#4a	#5a
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot	#1b	#2b	#3b	#4b	#5b
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä	#1c	#2c	#3c	#4c	#5c
d. TALOUS- RIKOLLISUUS Kirstitys, Petos, Identiteetti- varkaudet	#1d	#2d	#3d	#4d	#5d
e. KYBER- RIKOLLISUUS Virukset ja Hakkerointi	#1e	#2e	#3e	#4e	#5e

DigiTurvaMatriisi

TEKNOLOGIAT DIGI RISKIT	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio ja telepresens ★	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot ★	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly ★	4. AUTOMAAATIO IoT, Sensorit, robotiikka, etäkäyttö ja etävalvonta ★	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi)
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyskatkokset	Vaihe 1: Valitaan teknologia-alue matriisin vaakatasolta				
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot					
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä					
d. TALOUS-RIKOLLISUUS Kirstys, petos, Identiteetti- varkaudet					
e. KYBER-RIKOLLISUUS Virukset ja Hakkerointi					








HUOM!

Uusi hyödynnettävä teknologia liittyy yleensä useampaan teknologia-alueeseen (**merkitty tähdellä**).







Esim. **IoT ja robotiikka ratkaisu etävalvonnalla:**
(4)automaatio, (1)verkko, (3)käsittely, (2)tietovarannot.

Tällöin on riskit selvitettävä kaikkien teknolgian osa-alueiden (a-e) näkökulmista

DigiTurvaMatriisi

TEKNOLOGIAT DIGI RISKIT	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio ja telepresens 	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot 	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly 	4. AUTOMAAATIO IoT, Sensorit, robotiikka, etäkäyttö ja etävalvonta 	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi)
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyshäiriöt					
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot 	Vaihe 2: Valitaan riski-alue matriisin pystytasolta				
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä					
d. TALOUS- RIKOLLISUUS Kiristys, petos, Identiteetti- varkaudet 	HUOM! Uusi teknologia-alue, yksi tai useampi, sisältää useita riskitekijöitä (merkitty kolmiolla). Kartoitettavan teknologian osalta on tunnistettava kaikki mahdolliset riskitekijät ja arvioitava niiden todennäköisyyttä. Yhden riskitekijän realisoituminen aktivoi myös muita. Esim. hakkeroidussa järjestelmässä on henkilötietoja ja yritykselle tärkeitä tietoja. Salaamaton tietoliikenne avaa luettavaksi kaiken viestinnän.				
e. KYBER- RIKOLLISUUS Virukset ja Hakkerointi 					

Esimerkki #1 : Herätetietojen keruu asiakkaalta tuotekehitykseen

TEKNOLOGIAT DIGI RISKIT	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio ja telepresens 	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot 	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly 	4. AUTOMAAATIO IoT, Sensorit, etäkäyttö ja etävalvonta	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi)
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyskatkokset	#1a	#2a	#3a	#4a	#5a
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu , tietovuodot 	#1b	#2b	#3b	#4b	#5b
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä	#1c	#2c	#3c	#4c	#5c
d. TALOUS-RIKOLLISUUS Kiristys, Petos, Identiteetti- varkaudet 	#1d	#2d	#3d	#4d	#5d
e. KYBER-RIKOLLISUUS Virukset ja Hakkerointi 	#1e	#2e	#3e	#4e	#5e

Ratkaisukuvaus #1

Mahdollinen uusi liiketoiminta: Herätetietojen keruu asiakkaalta tuotekehitykseen

Teknologia: Herätejärjestelmä, CRM-asiakkuuksien hallinta, tietovarasto palvelimella

Koostuu useista tekniikoista:

Verkkoyhteys, tuotetiedot, asiakastiedot ja käyttöohjelmisto

Teknologia-alueet DigiTurva -matriisissa:

(1)verkko, (3)käsittely, (2)tietovarannot

Digiriskit:

- e. **kyberrikollisuus/hakkerointi:** tunkeutuminen verkkoon käyttäjätilin kautta, rikollinen pääsee asiakastietoihin
- b. **tietoturva/tietovarkaus:** tietoliikenteen seuranta/vakoilu, yritykselle tärkeät tiedot vieraissa käsissä
- d. **talousrikollisuus/identiteettivarkaus:** käyttäjän identiteettivarkaus, rikollinen pääsee esiintymään käyttäjänä

Ratkaisukuvaus: Tietoturvaohjeisto ja henkilöstön koulutus; Palvelinten, ohjelmistojen ja palvelujen suojaus (https/SSL salaus ja käyttäjän vahva tunnistautuminen); Virussuojaohjelmat ja palomuurit verkkorajapintoihin; Salatut ja suojatut yhteydet (VPN); Käytön valvonta ja raportointi häiriöistä.

Esimerkki #2 : Kumppanuusverkoston yhteisöjärjestelmä

TEKNOLOGIAT DIGI RISKIT	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio ja telepresens ★	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot ★	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly ★	4. AUTOMAAATIO IoT, Sensorit, etäkäyttö ja etävalvonta	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi)
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyshäiriöt	#1a	#2a	#3a	#4a	#5a
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu , tietovuodot ▲	#1b	#2b	#3b	#4b	#5b
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä ▲	#1c	#2c	#3c	#4c	#5c
d. TALOUS-RIKOLLISUUS Kirstytys, Petos, Identiteetti- varkaudet ▲	#1d	#2d	#3d	#4d	#5d
e. KYBER-RIKOLLISUUS Virukset ja Hakkerointi ▲	#1e	#2e	#3e	#4e	#5e

Ratkaisukuvaus #2

Mahdollinen uusi liiketoiminta: Kumppanuusverkoston yhteisöjärjestelmä

Teknologia: Kumppanuusverkoston tieto- ja viestintäjärjestelmä, extranet

Koostuu useista tekniikoista:

Yhteisöalusta (esim. mediawiki/Tiki); Kumppanuustietorekisteri; Tiedostoina tuote- ja palvelutiedot, tuotemallit, ohjeistot; Käyttöohjelmisto; Kommunikointi ja viestitysohjelmisto (esim. zoom).; Verkkoyhteydet

Teknologia-alueet DigiTurva -matriisissa:

(1)verkko, (3)käsittely, (2)tietovarannot

Digiriskit:

- e. **kyberrikollisuus/hakkerointi:** tunkeutuminen verkkoon käyttäjätilin kautta, rikollinen pääsee kumppanuustietoihin
- b. **tietoturva/tietovarkaus:** tietoliikenteen seuranta/vakoilu, yritykselle tärkeät tiedot vieraisa käsissä
- d. **talousrikollisuus/identiteettivarkaus:** identiteettivarkaus, rikollinen pääsee esiintymään käyttäjänä
- c. **palvelunestohyökkäys /WEB:** Kumppani ei saa verkkoyhteyttä palveluun

Ratkaisukuvaus: Tietoturvaohjeisto ja henkilöstön koulutus; Palvelinten, ohjelmistojen ja palvelujen suojaus (https/SSL salaus ja käyttäjän vahva tunnistautuminen); Virussuojaohjelmat ja palomuurit verkkorajapintoihin ja palvelimelle; Salatut ja suojatut yhteydet (VPN); Turvalliset kommunikointi- ja viestiohjelmat; Käytön valvonta ja raportointi häiriöistä.

Esimerkki #3 : Käytön koulutus - oppimisalusta

TEKNOLOGIAT DIGI RISKIT	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio ja telepresens ★	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot ★	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly ★	4. AUTOMAAATIO IoT, Sensorit, etäkäyttö ja etävalvonta	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi) ★
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyshäiriöt	#1a	#2a	#3a	#4a	#5a
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot ▲	#1b	#2b	#3b	#4b	#5b
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä ▲	#1c	#2c	#3c	#4c	#5c
d. TALOUS-RIKOLLISUUS Kirstytys, Petos, Identiteetti- varkaudet ▲	#1d	#2d	#3d	#4d	#5d
e. KYBER-RIKOLLISUUS Virukset ja Hakkerointi ▲	#1e	#2e	#3e	#4e	#5e

Ratkaisukuvaus #3

Mahdollinen uusi liiketoiminta: Käytön koulutus - oppimisalusta

Teknologia: Selainohjelmisto, oppialusta (esim. Moodle), opetussisältö, virtuaalimallit ja simulaatio

Koostuu useista tekniikoista:

Palvelimella oleva alustasovellus ja käyttöohjelmisto; oppisisältö ja oheismateriaali tiedostot; Opetettavan kohteen virtuaalimalli ja simulaatio-ohjelmisto; Kommunikointi ja viestitysohjelmisto (esim. zoom).

Teknologia-alueet DigiTurva -matriisissa:

(1)verkko, (3)käsitteily, (2)tietovarannot, (5)virtuaalisuus

Digiriskit:

- e. **kyberrikollisuus/hakkerointi:** tunkeutuminen verkkoon käyttäjätilin kautta, rikollinen pääsee järjestelmiin
- b. **tietoturva/tietovarkaus:** tietoliikenteen seuranta/vakoilu, yritykselle tärkeät tiedot vieraisa käsissä
- d. **talousrikollisuus/identiteettivarkaus:** käyttäjän identiteettivarkaus, rikollinen pääsee esiintymään käyttäjänä
- c. **palvelunestohyökkäys /WEB:** ei saada verkkoyhteyttä palvelukohteeseen

Ratkaisukuvaus: Tietoturvaohjeisto ja henkilöstön koulutus; Palvelinten, ohjelmistojen ja palvelujen suojaus (https/SSL salaus ja käyttäjän vahva tunnistautuminen); Virussuojaohjelmat ja palomuurit verkkorajapintoihin ja palvelimille; Salatut ja suojatut yhteydet (VPN); Rajattu pääsy oppialustaan, virtuaalimalleihin ja simulaatioon; Turvallinen kommunikoiti- ja viestitysohjelmisto, käytön valvonta ja raportointi häiriöistä.

Esimerkki #4 : Varaosakauppa

TEKNOLOGIAT DIGI RISKIT	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet, viestintä, kommunikaatio ja telepresens ★	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot ★	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly ★	4. AUTOMAAATIO IoT, Sensorit, etäkäyttö ja etävalvonta	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi)
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyshäiriöt	#1a	#2a	#3a	#4a	#5a
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot ▲	#1b	#2b	#3b	#4b	#5b
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä ▲	#1c	#2c	#3c	#4c	#5c
d. TALOUS-RIKOLLISUUS Kirstytys, Petos, Identiteetti- varkaudet ▲	#1d	#2d	#3d	#4d	#5d
e. KYBER-RIKOLLISUUS Virukset ja Hakkerointi ▲	#1e	#2e	#3e	#4e	#5e

Ratkaisukuvaus #4

Mahdollinen uusi liiketoiminta: Varaosakauppa

Teknologia: Selain ohjelmisto, verkkokauppa-alusta, tuoteluettelot, maksuyhteydet (transaktiot)

Koostuu useista tekniikoista:

Verkkokauppalvelin, kauppapaikkaohjelmisto, tuoteluettelot; Asiakastiedot; Maksupalveluyhteydet ja käyttöohjelmisto (esim. selainkäyttö)

Teknologia-alueet DigiTurva -matriisissa:

(1)verkko, (3)käsittely, (2)tietovarannot

Digiriskit:

- e. **kyberrikollisuus/hakkerointi**: tunkeutuminen verkkoon käyttäjätilin kautta, rikollinen pääsee järjestelmiin
- b. **tietoturva/tietovarkaus**: tietoliikenteen seuranta/vakoilu, yritykselle tärkeät tiedot vieraisa käsissä
- d. **talousrikollisuus/identiteettivarkaus**: petos, käyttäjän identiteettivarkaus, rikollinen pääsee esiintymään käyttäjänä
- c. **palvelunestohyökkäys /WEB**: ei saada verkkoyhteyttä palvelukohteeseen

Ratkaisukuvaus: Tietoturvaohjeisto ja henkilöstön koulutus; Luotettava kauppapaikka- ja pankkiyhteyssovellus; Palvelinten, ohjelmistojen ja palvelujen suojaus (https/SSL salaus ja käyttäjän vahva tunnistautuminen); Virusturvaohjelmat ja palomuurit verkkorajapointoihin; Salatut ja suojatut yhteydet (VPN); Käytön valvonta ja VÄLITÖN raportointi häiriöistä.

Esimerkki #5 : Etävalmistus ja valvonta

	1. VERKKO Tietoliikennetekniikka, verkkoyhteydet , viestintä, kommunikaatio ja telepresens 	2. TIETOVARANNOT WEB, Datan keruu, tiedostot, tietokannat ja tietovarastot 	3. KÄSITTELY Ohjelmistot, tietojärjestelmät, pilvipalvelut ja tekoäly 	4. AUTOMAAATIO IoT, Sensorit, robotiikka, etäkäyttö ja etävalvonta 	5. VIRTUAALISUUS Virtuaalimallit, VR/XR ja virtuaaliläsnäolo (metaversumi)
a. TEKNISET HÄIRIÖT Käyttökeskeytys, yhteyshäiriöt	#1a	#2a	#3a	#4a	#5a
b. TIETOTURVA Tietovarkaudet, teollisuusvakoilu, tietovuodot 	#1b	#2b	#3b	#4b	#5b
c. PALVELUNESTO Estohyökkäykset, tietoliikenne- häirintä 	#1c	#2c	#3c	#4c	#5c
d. TALOUS- RIKOLLISUUS Kirstitys, petos, Identiteetti- varkaudet 	#1d	#2d	#3d	#4d	#5d
e. KYBER- RIKOLLISUUS Virukset ja Hakkerointi 	#1e	#2e	#3e	#4e	#5e

Ratkaisukuvaus #5

Mahdollinen uusi liiketoiminta: Etävalmistus ja ennakoiva huoltopalvelu riskihallitulla digitaalisella teknologialla

Teknologia: Etä-valmistus 3D-teknologialla, valvonta ja diagnostiikka

Koostuu useista tekniikoista:

IoT sensorit, kameravalvonta, robotiikka, tuotemallit, datankeruu ja käyttöohjelmisto

Teknologia-alueet DigiTurva -matriisissa:

(4)automaatio, (1)verkko, (3)käsittely, (2)tietovarannot

Digiriskit:

- e. kyberrikollisuus/hakkerointi: tunkeutuminen verkkoon käyttäjätilin kautta, rikollinen pääsee järjestelmiin
- b. tietoturva/tietovarkaus: tietoliikenteen seuranta/vakoilu, yritykselle tärkeät tiedot vieraisa käsissä
- d. talousrikollisuus/identiteettivarkaus: käyttäjän identiteettivarkaus, rikollinen pääsee esiintymään käyttäjänä
- c. palvelunestohyökkäys /WEB: ei saada verkkoyhteyttä palvelukohteeseen

Ratkaisukuvaus: Tietoturvaohjeisto ja henkilöstön koulutus, Palvelinten, ohjelmistojen ja palvelujen suojaus (https/SSL salaus ja käyttäjän vahva tunnistautuminen); Virussuojaohjelmat ja palomuurit verkkorajapointoihin; Salatut ja suojatut yhteydet (VPN); Käytön valvonta ja raportointi häiriöistä.

Digiturvallisuuden kehitys ja ylläpito

1. Oppeja digiturvallisuudesta

- ✓ MPK-Koulutus <https://mpk.fi/koulutukset/kyber-ja-informaatioturvallisuus/>
- ✓ JYU avoin oppi <https://www.jyu.fi/fi/ajankohtaista/arkisto/2021/10/digiturvallisuutta-jokaiselle-maksuttomalta-avoimen-yliopiston-kurssilta>
- ✓ Kansalaisen kyberturvallisuus <https://www.avoin.jyu.fi/fi/opintotarjonta/informaatioteknologia/kyberturvallisuus>
- ✓ Kyberturvallisuuskeskus <https://www.kyberturvallisuuskeskus.fi/fi/>

2. Tietoturvaohjeita

- ✓ VAHTI <https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet>

3. Digiturvan standardi

- ✓ ISO/IEC 27001 https://en.wikipedia.org/wiki/ISO/IEC_27001
- ✓ Tietoturvan hallinta https://en.wikipedia.org/wiki/Information_security_management#Information_security_management_system

4. Suojaaminen

- ✓ **Arkkitehtuuri, verkkoyhteydet ja teknologiaratkaisut**
- ✓ **Palomuurit, tunnistautuminen ja sala**us
- ✓ **Digiturvaohjeisto, ISO/IEC 27001**
- ✓ F-Secure <https://www.f-secure.com/fi>

5. Digiriskien tunnistaminen ja testaus

- ✓ Tietoturvan tarkastukset https://en.wikipedia.org/wiki/Security_controls
- ✓ SSL Server Test <https://www.ssllabs.com/ssltest/>
- ✓ Kali LINUX työkalupakki https://fi.wikipedia.org/wiki/Kali_Linux