Suomen Yrittäjäopisto

Euroopan unionin osarahoittama

Yksin- ja pienyrittäjän tieto- ja kyberturvan ABC –verkkovalmennus. 26.9.2024

Tervetuloa!

https://www.syo.fi/digialy-kayttoon-hanke/

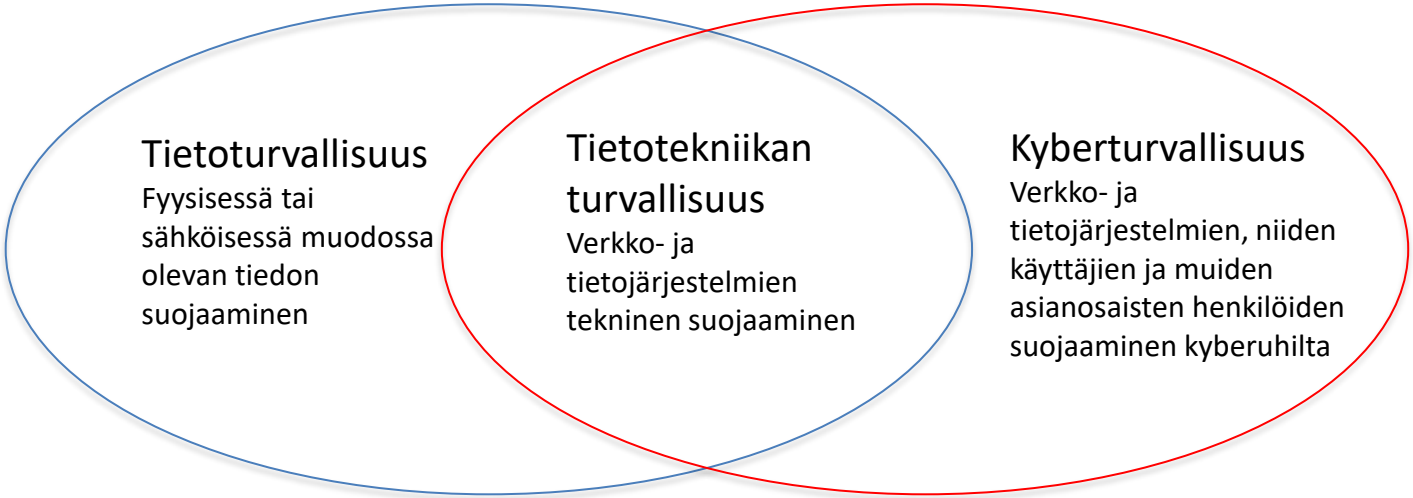
Valmennus on osa Suomen Yrittäjäopiston toteuttamaa Digiäly käyttöön –hankkeen toimenpiteitä. Hanke on EU:n osarahoittama.

Koulutuksen sisältö

- Digitaalisuus luo mahdollisuuksien lisäksi velvollisuuksia
- Mitä on kyber- ja tietoturvallisuus yrityksessä?
- Tietosuoja ja kyberturvallisuus
- Kyberturvallisuus kilpailuetuna
- Yrityksen tavallisimmat kyberuhat ja niiltä suojautuminen

Kouluttaja: Sanna Siuruainen, tietoturva-asiantuntija, Opsec Oy

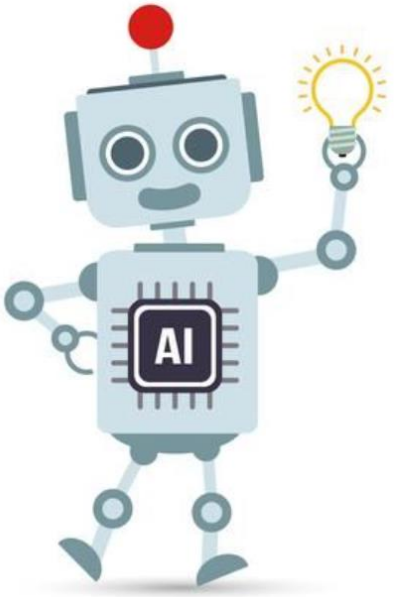
Mutta ihan aluksi: termit tutuiksi!



Digitaalisuus luo mahdollisuuksien lisäksi velvollisuuksia

Digitaalisuuden mahdollisuuksia:

- Maantieteelliset rajat katoavat
- Työn tekemisen tavat ja työsuhteiden ehdot muuttuvat
- Tuottavuuden kasvu, talouden uudistaminen
- Tuotantoketjujen eettisyys
- Työn kuormittavuuden ja työtapaturmien vähentäminen



Digitalisaation aiheuttamia haasteita:

- Lainsäädäntö ei pysy teknologisen kehityksen perässä
- Ammattien ja ammattitaidon katoaminen työtehtävien automatisoituessa
- Työntekijöiden valvonta digitaalisilla järjestelmillä
- Henkilötietojen kerääminen
- Sähköistyneen tiedon suojaaminen
- Digitaalinen myynti ja verkkokaupat
- Sosiaalinen media

Digitaalisuuden velvollisuuksia

Lainsäädäntö ja vaatimustenmukaisuus:

- EU-GDPR
- NIS2
- CRA
- Muut kansalliset ja toimialakohtaiset lait, säädökset ja velvoitteet
- Toimittaja- ja yhteistyösopimusten velvollisuudet

Teknologinen kehitys ja osaaminen

- Kustannukset ja resurssit
- Henkilöstön osaaminen ja tietoisuus

Vastuullisuus ja läpinäkyvyys toiminnassa

- ekologisuus, kestävä kehitys, esteettömyys, syrjimättömyys
- vastuunkanto omasta toiminnasta
- avoin ja rehellinen julkisuuskuva, eettinen mainonta
- muista somen voima: yksikin negatiivinen asiakaspalaute voi kaataa koko bisneksen

Mitä on kyber- ja tietoturvallisuus yrityksessä?

- Riippuvuus digitaalisista palveluista ja järjestelmistä
- Jatkuvasti kehittyvät ja lisääntyvät kyberuhkat

Hyvin rakennettu kyberturvallisuus:

- yrityksen toimintakyky
- digitaaliteknologian hyödyntäminen

Yrityksen tietoturvallisuuden hallintajärjestelmän rakennuspalikat:

Kaiken keskiössä on yrityksen suojattava omaisuus ja elintärkeät toiminnot ja prosessit.

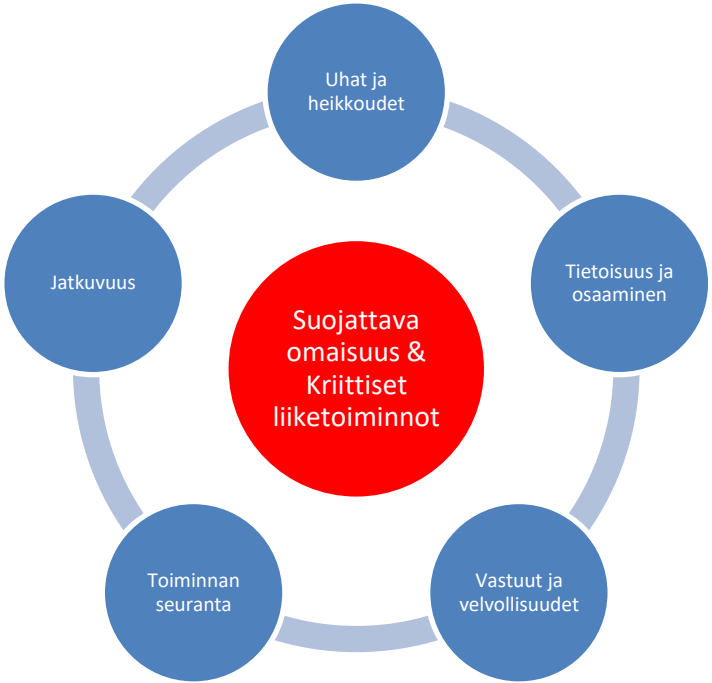
Tietoturvallisuuden hallintajärjestelmän rakennuspalikat

Suojattava omaisuus ja kriittiset liiketoiminnot

Jos ei tunne omaa toimintaa, ei voi suojautua uhkilta.

? Mikä meillä on tärkeää? Mitä ilman toiminta ei jatku? Mikä ei saa paljastua?

- Omaisuuden ja liiketoimintojen tunnistaminen
- Lähtötilanteen määrittäminen



Tietoturvallisuuden hallintajärjestelmän rakennuspalikat

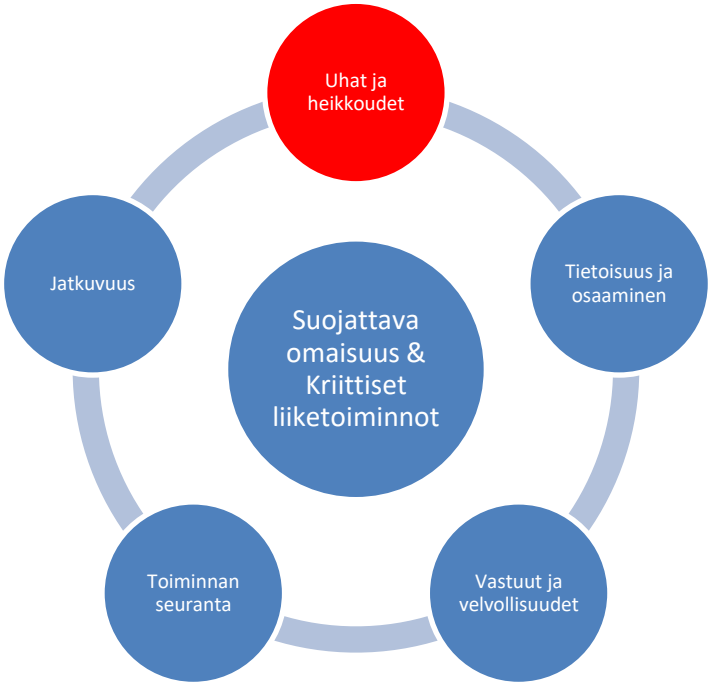
Uhat ja heikkoudet = riskit

Hyvä riskienhallinta ulottuu vaatimusten noudattamista pidemmälle.

? Mikä meitä uhkaa? Mitä heikkouksia kohteiden suojaamiseen liittyy?

Onnettomuudet, vahingot, virheet, laiterikot
- Laiterikot, tietojärjestelmäviat, tiedon menetys
- Sähkönsyötön häiriöt, muut toimitiloihin kohdistuvat häiriöt
- Puutteelliset / hallitsemattomat prosessit
- Loppukäyttäjien tekemät virheet ja vahingot, puutteellinen ohjeistus
- Toimittajaketjun riskit, epäselvät sopimusvastuut
- Luonnonkatastrofit, sodat, pandemiat

Rikollisuus ja väärinkäytökset
- Sisäinen uhka, toimittajariski
- Palvelunestohyökkäykset
- Haittaohjelmien levitys ja tunkeutuminen verkkoon
- Tietojenkalastelu (phishing)
- Huijaukset
- Sabotaasi



Riskienkäsittelyprosessi:

- Tunnistaminen
- Analysointi
- Arviointi
- Riskien käsittely ja hallintakeinot

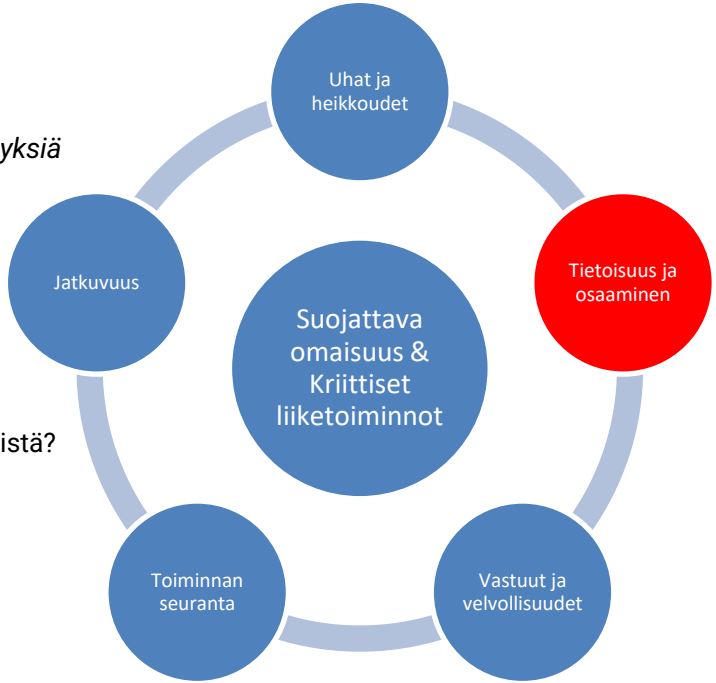
Tietoturvallisuuden hallintajärjestelmän rakennuspalikat

Tietoturvatietoisuus ja osaaminen

Parhaimmillaan organisaation työntekijät voivat olla aktiivinen suojauskerros kyberhyökkäyksiä vastaan.

Pohdittavaksi:

- Onko meillä tulevaisuuden kyberturvallisuushaasteiden ratkaisemiseen kykenevä henkilöstö?
- Millaista asiantuntemusta organisaatiomme tarvitsee kyberriskien hallitsemiseksi?
- Mitkä tehtävät on säilytettävä talon sisäisinä ja mitkä kannattaa ulkoistaa?
- Miten hyvin ja kuinka usein järjestämme henkilöstölle koulutusta turvallisuuskäytännöistä?
- Entä koulutusta erityisistä uhkista, joille voimme olla haavoittuvaisia?



Johda näyttämällä esimerkkiä!

- Avoimuus
- Kyberturvallisuus osana jokapäiväistä toimintaa
- Vaikuttamisen mahdollisuus
- Huolenaiheiden esiintuonti

Tietoturvallisuuden hallintajärjestelmän rakennuspalikat

Vastuut ja velvollisuudet

Kyberturvallisuus vaikuttaa koko organisaatioon – ei pelkästään IT-hallintoon.
Siksi sitä ei saa jättää yhden henkilön varaan.

Rakenna ylhäältä päin – Johto vastaa kyberturvasta

- Johdon vastuut
- IT-asiantuntijoiden vastuut
- Henkilöstön vastuut

! Huom! Lakisääteiset ja sopimukselliset vastuut ja velvollisuudet

Tietoturvallisuuden hallintajärjestelmän rakennuspalikat

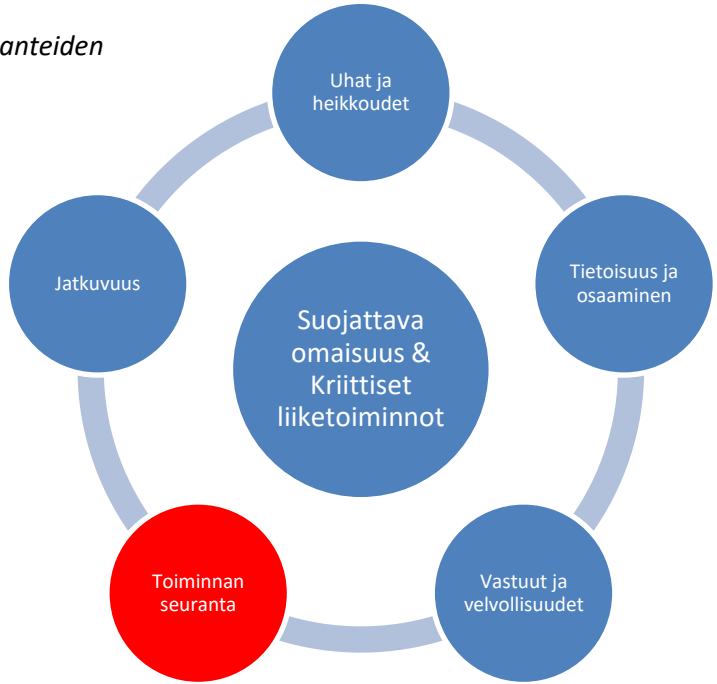
Toiminnan seuranta

Jopa hyvin yksinkertaisten toimenpiteiden toteuttaminen auttaa vähentämään poikkeamatilanteiden todennäköisyyttä ja vaikuttavuutta.

? Miten voimme varmistaa, ovatko toimenpiteemme tehokkaita?

Tietoturvapoikkeamien (ja tietosuojaloukkausten) hallintaprosessin päävaiheet:

- Varautuminen
- Havaitseminen ja analysointi
- Reagointi
- Toipuminen ja jälkiseuranta

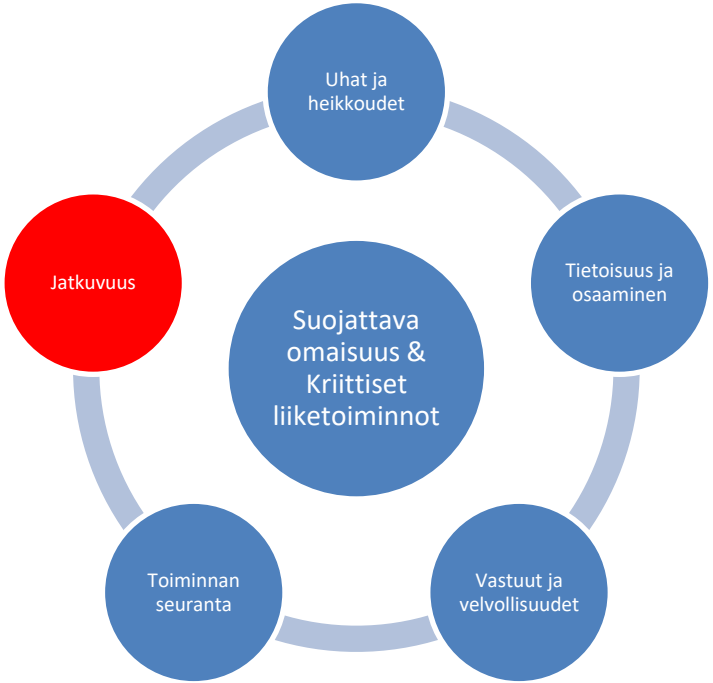


Tietoturvallisuuden hallintajärjestelmän rakennuspalikat

Jatkuvuudenhallinta

Jatkuvuudenhallinta on kuin yrityksen varavirtakytkin: se auttaa selviytymään häiriötilanteista ja toiminnan katkoksista.

- Jatkuvuudenhallinnan tavoitteet
- Jatkuvuudenhallinnan osa-alueet
- Jatkuvuutta edistäviä toimenpiteitä



Tietosuoja ja kyberturvallisuus

Tietosuoja yrityksessä

- Sisäänrakennettu tietosuoja
- Selkeä vastuujako ja riittävä resursointi
- Kattava ja ajantasainen Seloste käsittelytoimista
- Julkiset Tietosuojaselosteet
- Sopimukset tietojenkäsittelystä
- Ohjeistus ja koulutus henkilöstölle
- Henkilötietojen käsittelyn automatisointi
- Toimintamenettelyt tietopyyntöjen ja tietosuojaloukkausten käsittelylle
- Dokumentaation ja prosessien säännöllinen katselmointi

Tietosuoja myynnissä ja markkinoinnissa

- Tehdäänkö markkinointia asiakkuuden tai suostumuksen perusteella
- Asiakkaalla oltava mahdollisuus perua esim. uutiskirje
- Asiakastietojen pitäminen ajan tasalla
- Yhteystietojen kerääminen esim. messuilla

! Jos markkinoinnissa tai myynnissä käytetään B2B-yhteystietoja, etunimi.sukunimi@yritys.fi -muodossa olevia yhteystietoja tulee käsitellä kuten yksityistä henkilötietoa.

Tietosuoja ja kyberturvallisuus

Käytännön tietosuoja

- Vain välttämätön tieto kerätään
- Henkilötietojen monistaminen ja kopiointi pyritään minimoimaan
- Määritetään käyttöoikeudet dataan vain tietoja työssään tarvitseville
- Käytetään vain turvallisia tietojen säilytyspaikkoja ja siirtomekanismeja
- Puhtaan pöydän ja näytön periaate
- Kaikella henkilötiedolla on määritettynä säilytysaika
- Tiedon poistamisvelvollisuutta tulee noudattaa
- Kaikilla rekistereillä on vastuuhenkilöt

Läppäri varastettiin, kovalevy suojattu pelkällä salasanalla – tietosuojavaltuutetun mielestä olisi pitänyt kryptata

21.12.2022 20:26

Salasana ei riitä arkaluontoisten henkilötietojen suojaksi.

Varastettu. Läppärilaukku sisälsi kannettavan lisäksi ulkoisia kiintolevyjä ja asiakirjoja.

Telegram syytetää muassa l levittämi

3.9.2024

Seuraava saattaa l kummem

15.8.202

Apple ot – valmis uhkiin

26.2.202

Vastaamo-uhrien juristi: Ihmisiä on päätynyt itsemurhaan tietomurron ja kiristyksen takia

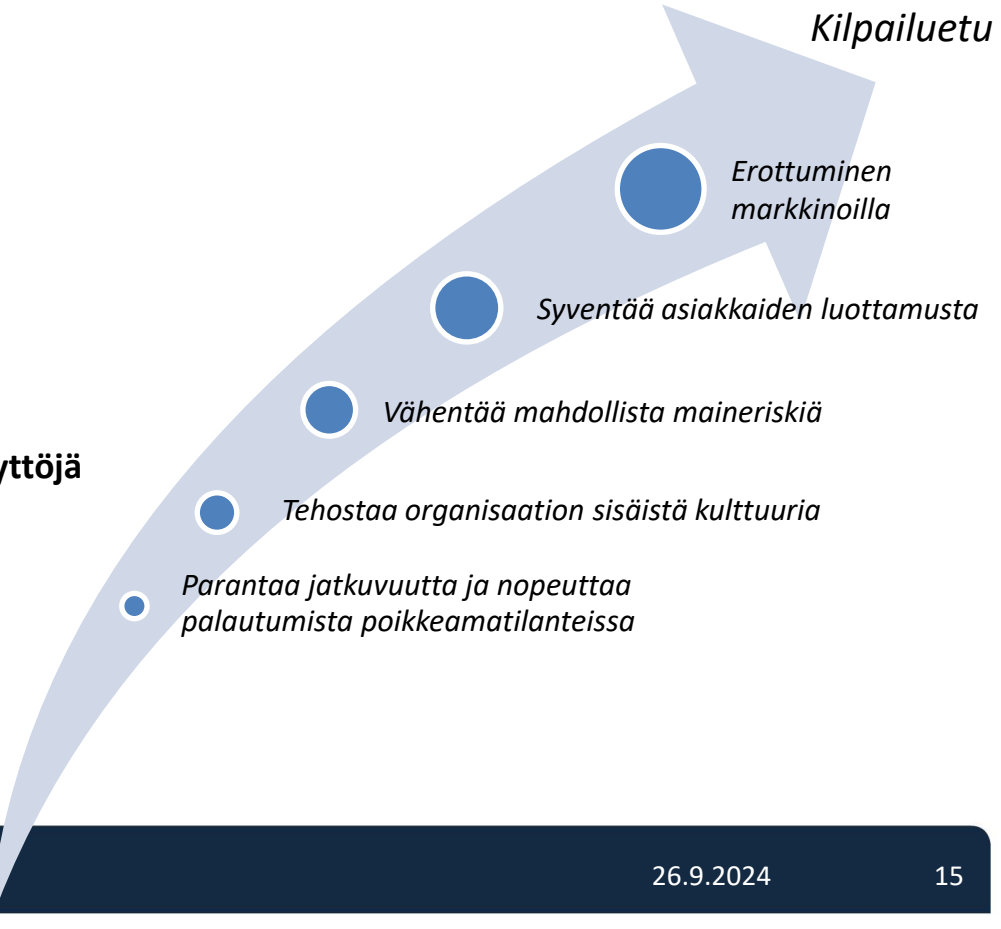
Psykoterapiakeskus Vastaamon potilaita on päätynyt itsemurhaan tietojensa vuotamisen takia, kertoo useita tietomurron ja kiristyksen uhreja edustava juristi.

Kyberturvallisuus kilpailuetuna

- Kyberrikollisuus ei ole vain suurten yritysten haaste.
- Tietovuodon tai tiedon menetyksen vaikutus
- Turvallisuuskyvykkyyden osoittaminen
- Sertifikaateista kilpailuetua

Monet yritykset vaativat alihankkijoiltaan vahvoja näyttöjä tietoturvasta. Sopimuksia ei allekirjoiteta, ennen kuin tietoturvan taso on todennettu.

Tietoturvaosaamisen voi myös ulkoistaa esim. sertifioidulle IT-palveluntarjoajalle



Yrityksen tavallisimmat kyberuhat ja niiltä suojautuminen

Kyberuhkien luonne

Onnettomuudet, vahingot, virheet, laiterikot

- Odottamattomia tilanteita
- Vaikutusmahdollisuuksien ulkopuolella
- Varautuminen vaatii panostuksia henkilöstöön, tiloihin ja laitteisiin

Rikollisuus ja väärinkäytökset

- Hyvin pitkälle automatisoitua
- Rakenteellista ja järjestelmällistä
- Luonteeltaan opportunistista
- Kansainvälistä

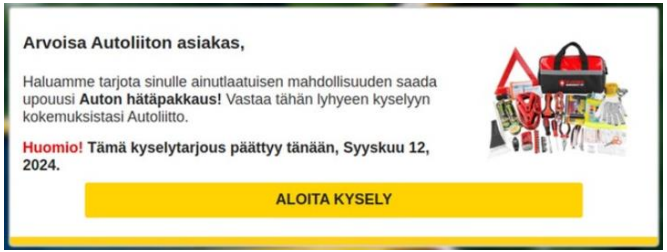
Kalastelut ja huijaukset

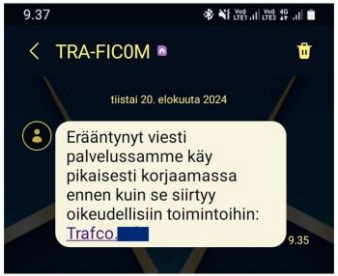
Tietojenkalastelu:

- Henkilötiedot
- Käyttäjätunnukset ja salasanat

Huijausviestit:

- Haittaohjelmat ja virukset
- Kiusanteko
- Rahan kiristäminen





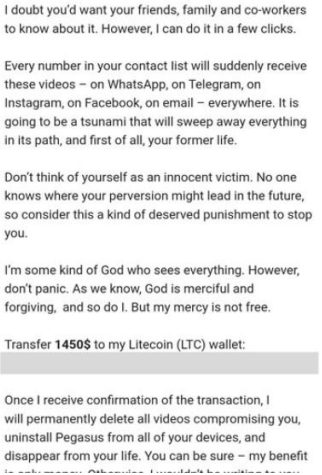

Hello pervert, I've sent this message from your Microsoft account.

I want to inform you about a very bad situation for you. However, you can benefit from it, if you will act wisely.

Have you heard of Pegasus? This is a spyware program that installs on computers and smartphones and allows hackers to monitor the activity of device owners. It provides access to your webcam, messengers, emails, call records, etc. It works well on Android, iOS, macOS and Windows. I guess, you already figured out where I'm getting at.

It's been a few months since I installed it on all your devices because you were not quite choosy about what links to click on the internet. During this period, I've learned about all aspects of your private life, but one is of special significance to me.

I've recorded many videos of you jerking off to highly controversial porn videos. Given that the "questionable" genre is almost always the same, I can


I doubt you'd want your friends, family and co-workers to know about it. However, I can do it in a few clicks.

Every number in your contact list will suddenly receive these videos – on WhatsApp, on Telegram, on Instagram, on Facebook, on email – everywhere. It is going to be a tsunami that will sweep away everything in its path, and first of all, your former life.

Don't think of yourself as an innocent victim. No one knows where your perversion might lead in the future, so consider this a kind of deserved punishment to stop you.

I'm some kind of God who sees everything. However, don't panic. As we know, God is merciful and forgiving, and so do I. But my mercy is not free.

Transfer **1450$** to my Litecoin (LTC) wallet:

Once I receive confirmation of the transaction, I will permanently delete all videos compromising you, uninstall Pegasus from all of your devices, and disappear from your life. You can be sure – my benefit

Palvelunestohyökkäykset ja kiristyshaittaohjelmat

Palvelunestohyökkäysten tyypilliset hyökkäystavat:

- Rajallisten resurssien kuluttaminen.
- Ohjaustietojen muuttaminen
- Vääränlaisen lähetteen syöttäminen palvelimelle, joka kaataa sen käyttöjärjestelmän tai palvelinprosessin.

Kiristyshaittaohjelmien yleisiä tartuntatapoja:

- sähköpostin liite
- saastunut verkkosivusto tai mainos
- suojaamaton wifi-verkko

Kiristyshaittaohjelma pyyhki pois indie-pelikehittäjän kaikkien pelaajien tilit

29.11.2023 07:05

Hakkerit hyökkäsivät pelin pääpalvelimeen ja salasivat sieltä kaiken datan, mukaan lukien paikalliset varmuuskopioasemat.

5.7.2024

Suomessa käynnissä venäjämielisen hakkeriryhmän toteuttama laaja palvelunestöhyökkäys

Kyberturvallisuuskeskuksen mukaan NoName hakee hyökkäyksellään näkyvyyttä.

Suomessa useisiin sivustoihin on viime päivinä kohdistunut laaja palvelunestohyökkäys. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksesta vahvistetaan STT:lle, että kyseessä on venäjämielinen NoName-hakkeriryhmä.

Perjantaina kohteena olivat Kyberturvallisuuskeskuksen mukaan muun muassa valtiovarainministeriö, Keskuskauppakamari, Suomen Pankki, Verohallinto, Osuuspankki ja Helsingin kaupunki.

Hyökkäyksen laajuudesta huolimatta siitä ei koidu kaikille sivustoille välttämättä juurikaan haittaa.

Palvelunestohyökkäykset ja kiristyshaittaohjelmat voivat iskeä myös älypuhelimiin!

Uutinen

Kiristyshaittaohjelma iski verenluovutusjärjestöön

5.8.2024 20:34 | päivitetty 7.8.2024 16:33

Terveysalan organisaatioihin kohdistuu viikossa keskimäärin 1671 kyberhyökkäystä.

Kiristyshyökkäys Tietoevryn datakeskukseen – useiden yritysten verkkosivut kaatuivat

Joakim Kullas 22.1.2024 09:05 | päivitetty 22.1.2024 19:33 KIRISTYSHAITTAOHJELMAT TIETOTURVA KONESALIT

Kiristyshaittaohjelma iski yhteen datakeskukseen Ruotsissa, jossa sijaitsee useiden yritysten verkkosivujen ja sovellusten ylläpitoon käytettäviä virtualisointi- ja hallintapalvelimia.

HSL:n sivuilla palvelunestohyökkäys

MARIKA HARJUMAA

11.8. 12:27 · Päivitetty 11.8. 12:33

Kuuntele juttu 0:35

Helsingin seudun liikenteen HSL:n verkkosivuilla on meneillään palvelunestohyökkäys. HSL kertoo, että hyökkäyksen vuoksi verkkosivu toimii vain ajoittain tai ei laisinkaan. Sen sijaan HSL-sovellus toimii normaalisti.

Ongelma koskee myös HSL-kortin lataamista, mutta siinäkin asiassa sovellus toimii tavalliseen tapaan.

Tietomurrot

- Taloudellinen hyötyminen
- Murretun ympäristön hyödyntäminen osana muita hyökkäyksiä
- Tietovarkaudet
- Haitallisen sisällön jakaminen yrityksen verkkosivustolla
- Identiteettivarkaudet
- Kiusanteko
- Laskutuspetokset

Cyberattack cost MGM Resorts about $100 million, Las Vegas company says

The company said it deliberately shut down a number of services "to mitigate risk to customer information" after the hack last month.

Oct. 6, 2023, 3:40 AM GMT+3

By Kevin Collier

The criminal cyberattack on MGM Resorts in Las Vegas last month resulted in the company's losing around $100 million, it said in a filing Thursday evening with the Securities and Exchange Commission.

The admission is a rare insight into the giant sums that major companies can lose when they fall victim to significant hacks.

Pelättyä laajemmaksi paljastunut tietomurto voi vaarantaa jopa kansallista turvallisuutta, sanoo professori

Helsingin tietomurto | Professori Jouni Isoaho pitää tietomurtoa Suomen mittapuulla poikkeuksellisena.

KRP varoittaa Office 365 -tietomurroista: "Pahinta on, ettei huijausta tunnista"

Microsoft Office 365 -tunnusten tietojenkalastelu on Keskusrikospoliisin mukaan Suomessa erityisen yleistä. Rahalliset menetykset ovat olleet merkittäviä.

Kyberuhilta suojautuminen

Huomioi muutokset kyberturvallisuuden uhkakuvassa

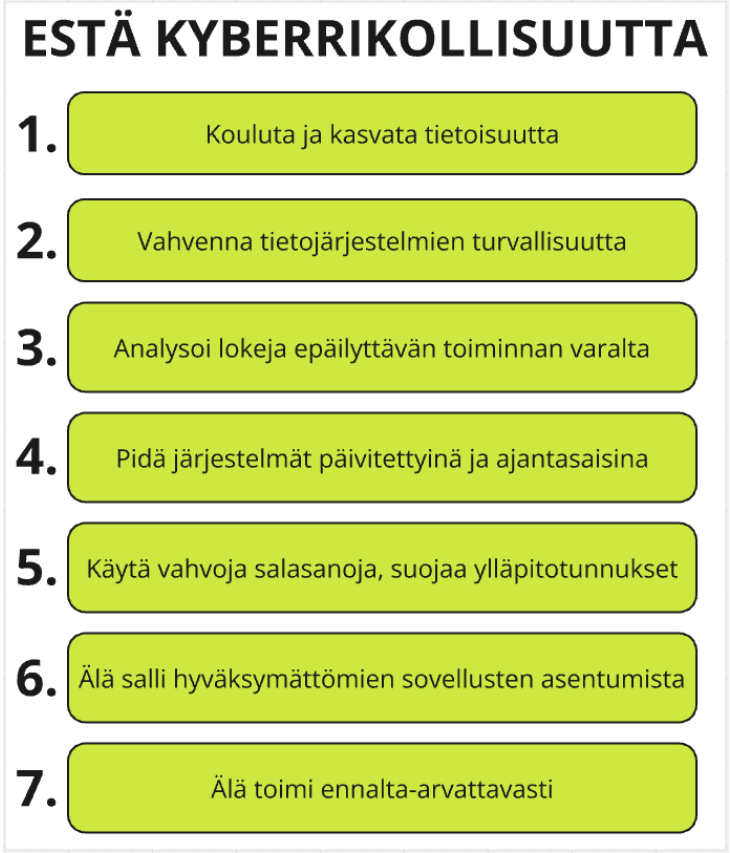
- Tietoturvatyön resurssit
- Suojaustoimenpiteiden ajantasaisuus
- Kyberturvallisuuden tilannekuva

Tekniset suojaustoimet

- Laitteet ja tietojärjestelmät
- Monivaiheinen tunnistautuminen
- Tietoturvapäivitykset
- Tietoliikenteen turvallisuus
- Haittaohjelmasuojaus
- Pilvipalveluiden suojaus
- Turvalliset etäyhteydet
- Varmuuskopiointi
- Julkinen ja sisäinen verkko

Hallinnolliset suojaustoimet

- Koulutus ja tietoisuus
- Riskien- ja poikkeamienhallinta
- Toiminnan jatkuvuus



Kiitos!

Kysymyksiä?

OPSEC OY
Tiedekatu 2, 60320 Seinäjoki
p. 020 198 6690, info@opsec.fi
www.opsec.fi