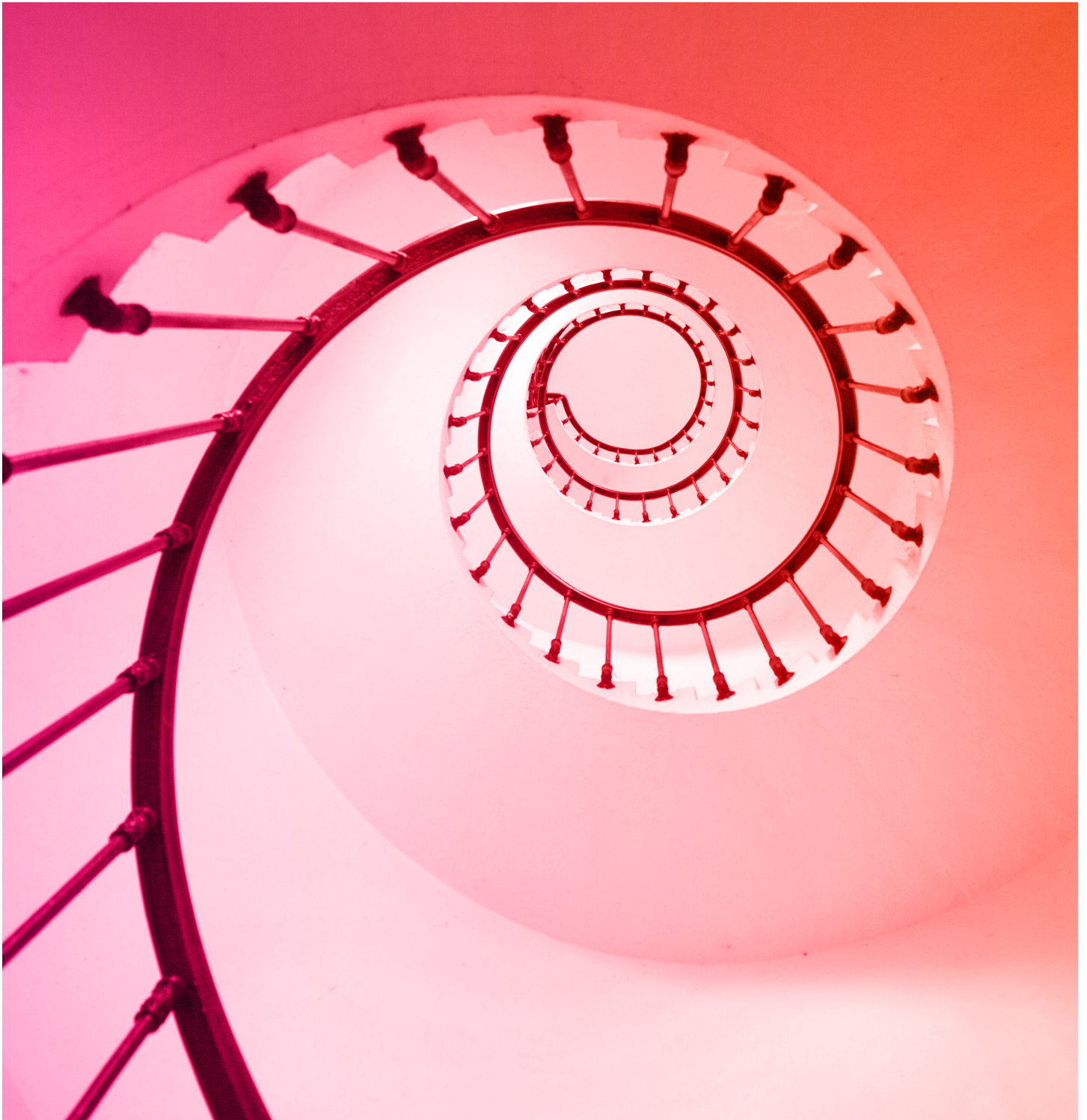




IT-asiantuntijan tietoturva

**Tietoturva ja tietosuoja taloushallinto-alalla
– ajankohtaiset uhat ja trendit**

1 Järjestömme noudattaa kilpailulakia



Kilpailulaki kieltää sellaiset sopimukset, päätökset sekä yhdenmukaistetut menettelytavat, joiden tarkoituksena on merkittävästi estää, rajoittaa tai vääristää kilpailua tai joista seuraa, että kilpailu merkittävästi estyy, rajoittuu tai vääristyy.

Mikäli keskustelu liittyy kiellettyyn teemaan, kaikkien osallistujien tehtävä on lopettaa keskustelu. Emme keskustele seuraavista teemoista, jotka sisältävät jäsenen luottamuksellista tietoa:

- Yksityiskohtaiset sopimusehdot
- Toimittajat, asiakkaat
- Tarjoukset
- Tuotantomäärät
- Laajentumissuunnitelmat, jotka eivät vielä julkisia
- Muut tulevaisuudensuunnitelmat (esim. T&K-panostukset, tuotantoseisokit)

- Alan yleinen hintataso ja siihen vaikuttaminen
- Hinnoittelukäytännöt ja –mekanismit
- Osto- ja myyntihinnat
- Markkinaosuudet
- Kustannukset
- Kannattavuus
- Yhteiset boikotit



**talous
hallinto
liitto**



Huoltovarmuuskeskus

Tietoturva ja tietosuoja taloushallintoalalla

IT-asiantuntijoiden verkkokoulutus 1

2024

17.9.2024 ©Taloushallinto Liitto

² **Tervetuloa IT-asiantuntijoiden tietoturva- ja tietosuojakoulutukseen**



- Koulutuksen tavoite
- Kohderyhmä
- Koulutuksen kulku ja aikataulu
 - 20.9.2024 Tietoturva ja tietosuoja taloushallintoalalla
 - 4.10.2024 IT toimittajayhteistyö
 - 25.10.2024 Jatkuvuudenhallinta ja ICT-infrastruktuurin hallinnan parhaat käytännöt
 - 29.11.2024 ICT-päätelaitteiden hallinnan parhaat käytännöt

17.9.2024 ©Taloushallinto Liitto

3

Koulutuksen agenda

1. Tietoturvallisuuden perusteet ja merkitys taloushallintoalalla
2. Taloushallintoalan organisaatioon vaikuttava tietosuoja- ja tietoturvalainsäädäntö
3. Miten IT-asiantuntijan tulee huomioida lainsäädäntö?
4. Ajankohtaiskatsaus



1. Tietoturvallisuuden perusteet ja merkitys taloushallintoalalla

5

Tietosuoja ja tietoturva lukuina



Huoltovarmuuskeskus

- Tietosuojavaltuutetun toimistossa tuli vireille liki 7 000 tietoturvaloukkauksilmoitusta (2023)
- Korkein yksittäiselle organisaatiolle määrätty seuraamusmaksu oli yli 400 000 euroa (2023)
- Kyberturvallisuuskeskus käsitteli yli 200 ilmoitusta palvelunestohyökkäyksistä (2023)
- Suomessa on KTK:n mukaan yli miljoona huijausyritystä kuukausittain (2024)
- Suomalaisilta huijattu pankkien tietojen mukaan 44 miljoonaa euroa (2023)
- Paras tapa ehkäistä tietosuojaan ja tietoturvaan liittyviä ongelmia, on systemaattisesti huolehtia näistä asioista. Aloitetaan tämä kurssi käymällä läpi tarkemmin merkitystä taloushallintoalan näkökulmasta.

17.9.2024 ©Taloushallinto Liitto

Tietoturvan merkitys taloushallintoalalla



Huoltovarmuuskeskus



- Taloushallinnon ammattilaisten ja taloushallintoalan yritysten merkittävä vaikutus
- Yhteiskunnan toiminnan kannalta keskeiset tehtävät
- Taloushallinnon tehtävien suorittaminen vaatii onnistuakseen toimivia ja turvallisia ICT-järjestelmiä.

©Taloushallinto Liitto

Tietoturva



- Tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaaminen
- Tietoturvatoinenpiteet ja -kontrollit
- Henkilöstö, prosessit, teknologiat
- Uhkat, haavoittuvuudet ja riskit

©Taloushallinto Liitto

Yleisiä organisaatioiden tietoturvauhkia

Uhka	Kuvaus	Suojautumistoimia
Tietojenkalastelu	Hyökkääjät lähettävät viestejä, jotka näyttävät tulevan luotettavalta lähteeltä, mutta niiden tarkoitus on kalastella tunnuksia ja salasanoja.	Käyttäjän huolellisuus ja tietojenkalasteluviestien tunnistaminen, ajantasainen haittaohjelmasuojaus päätelaitteissa, ajantasainen roskapostisuodatus sähköpostissa.
Haittaohjelmat	Hyökkääjät voivat kiristyshaittaohjelmalla lukita yrityksen tiedostot ja vaatia lunnaita niiden vapauttamiseksi, mikä voi pysäyttää liiketoiminnan ja aiheuttaa tappioita.	Ajantasainen haittaohjelmasuojaus päätelaitteissa ja yleinen käyttäjän huolellisuus internetin käytössä.
Palvelunesto-hyökkäykset	Palvelunestohyökkäykset ylikuormittavat yrityksen verkkopalvelut, mikä voi estää niiden käytön.	Tietojärjestelmien ja tietoliikenneyhteyksien suunnittelu kuormitusilanteita kestäväksi.
Haavoittuvuuksien hyödyntäminen	Hyökkääjät voivat hyödyntää yrityksen tietojärjestelmissä olevia tunnettuja haavoittuvuuksia, jos niitä ei ole korjattu.	Tietojärjestelmien säännölliset päivitykset ja turvalliset asetukset.

©Taloushallinto Liitto

9 Tietoturvan toteuttaminen yhteistyössä



Tiedon luokittelu Varmistamaan, että tietoja käsitellään asianmukaisesti niiden kriittisyyden mukaan.	Turvalliset työkalut Ohjelmistot ja laitteet, joita käytetään tietojen käsittelyyn tavalla, joka täyttää tietoturvan ja tietosuojan vaatimukset.	Tietoturvan hallintatoimet Tekniset ja organisatoriset toimenpiteet, joilla suojataan tietoja.	Dokumentointi Olennainen osa tietoturvan ylläpitämistä ja valvontaa

17.9.2024 ©Taloushallinto Liitto

2. Taloushallintoalan organisaatioon vaikuttava tietosuoja- ja tietoturvalainsäädäntö

17.9.2024 ©Taloushallinto Liitto

11 Johdanto tietoturva - ja tietosuojalainsäädäntöön



Toimintaympäristön vaatimukset

- Kirjanpitolaki
- EU:n yleinen tietosuoja-asetus (GDPR)
- Laki yksityisyyden suojasta työelämässä

Epäsuorat vaatimukset

- **NIS2** (Network and Information Systems Directive 2) on EU-direktiivi, joka asettaa tiukemmat kyberturvavaatimukset kriittisille infrastruktuureille ja laajentaa tietoturvaluottamussäännösten soveltamisalaa. Noudatettava 18.10.2024
- **DORA** (Digital Operational Resilience Act) on EU-asetus, joka keskittyy finanssialan digitaalisen toimintavarmuuden vahvistamiseen, edellyttäen, että finanssilaitokset kykenevät kestämaan, reagoimaan ja toipumaan erilaisista kyberuhista. Noudatettava 17.1.2025

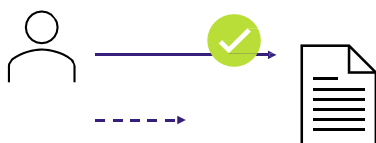
17.9.2024 ©Talouhallintoliitto

12 Kirjanpitolaki

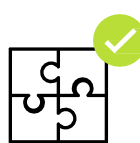


- Keskeinen taloushallintoalan sääntely tulee Kirjanpitolaista. Kirjanpitolaki sisältää useita säädöksiä, joilla on liittämäpinta tietoturvaan. Tietoturvan kolme keskeistä osa-aluetta – luottamuksellisuus, saatavuus ja eheys – ovat olennaisia kirjanpitolain noudattamisessa, koska kirjanpidon tiedot ovat taloudellisesti ja oikeudellisesti merkittäviä, ja niiden suojaaminen on tärkeää.

Luottamuksellisuus



Eheys



Saatavuus



17.9.2024 ©Talouhallintoliitto

Tietosuojan sääntely



- Tietosuojaperiaatteita on noudatettava aina, kun käsitellään henkilötietoja.
- Tarkoituksena on suojella ihmisten oikeutta henkilötietojensa suojaan ja sitä kautta varmistaa kaikille ihmisille kuuluvien perusoikeuksien toteutuminen.

©Taloushallinto Liitto

Sääntely: Roolit ja vastuut



Rekisterinpitäjä

määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään.



Henkilötietojen käsittelijä

käsittelee henkilötietoja rekisterinpitäjän lukuun.



Työntekijä

noudattaa oman organisaationsa tietosuojakäytäntöjä.

©Taloushallinto Liitto

Sääntely: Tietosuojaperiaatteet

Periaate	Mitä periaatteella tarkoitetaan
Lainmukaisuus, asianmukaisuus ja läpinäkyvyys	Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti suhteessa käsittelyn tarkoitukseen ja läpinäkyvästi suhteessa rekisteröityihin.
Käyttötarkoituksidonnaisuus	Henkilötietoja kerätään ja käytetään vain ennalta määriteltyihin, laillisiin tarkoituksiin, eikä niitä käsitellä alkuperäisen käyttötarkoituksen kanssa yhteensopimattomalla tavalla.
Tietojen minimointi	Henkilötietoja saa kerätä ja käsitellä vain siinä laajuudessa kuin on tarpeellista käsittelyn tarkoituksen kannalta. Henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta. Henkilötietojen säilytysaika on pidettävä mahdollisimman lyhyenä.
Tietojen täsmällisyys	Henkilötiedot pidetään täsmällisinä ja ajan tasalla, ja epätarkat tai virheelliset tiedot oikaistaan tai poistetaan viipymättä.
Säilytyksen rajoittaminen	Henkilötietoja säilytetään vain niin kauan kuin on tarpeen niiden käsittelyn tarkoitusten ja lakivelvoitteiden toteuttamiseksi. Esimerkiksi kirjanpitoa- ja arkistolaista tai toimialakohtaisista laeista voi aiheutua vaatimuksia arkistointiajoille.
Luottamuksellisuus ja turvallisuus	Henkilötietoja käsitellään siten, että niiden asianmukainen turvallisuus varmistetaan, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä ja vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

17.9.2024 ©Taloushallinto/tili

16 Tietosuojaperiaatteet käytännössä?



Henkilötietojen käsittely

Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti suhteessa käsittelyn tarkoitukseen ja läpinäkyvästi suhteessa rekisteröityihin.



Suostumus ja oikeudet

Henkilötietojen käsittely vaatii selkeän perusteen tai suostumuksen. Rekisteröidyillä on laajat oikeudet omiin tietoihinsa.



Kansainväliset siirrot

Henkilötietojen siirto EU:n/ETA:n ulkopuolelle on sallittua vain, jos kohdamaa tarjoaa riittävän tietosuojan tason tai jos käytetään sopivia suojatoimia.

17.9.2024 ©Taloushallinto/tili

3. Miten IT-asiantuntijan tulee huomioida lainsäädäntö?

18 Miten IT-asiantuntijan tulee huomioida lainsäädäntö?



Tietosuoja ja tietoturvan suunnitelmallinen toteuttaminen



Tietoturvakäytäntöjen kehittäminen ja ylläpito



Tietojen hallinta ja käsittely (ml. säilytys ja poistaminen)



Tietoturvaloukkausten hallinta ja ilmoittaminen



Hankintojen ja toimitusketjun turvallisuus

19 Yksinkertaisimmillaan, kysy nämä 4 keskeistä kysymystä



Mitä olemme tekemässä?

Mitä voisi mennä pieleen?

Mitä aiomme tehdä niille asioille, jotka voivat mennä pieleen?

Teimmekö tarpeeksi hyvää työtä edellisessä vaiheessa?

17.9.2024 ©Taloushallinto.fi

Ajankohtaiskatsaus

17.9.2024 ©Taloushallinto.fi

21

Ajankohtaiskatsaus



Huoltovarmuuskeskus

Katsauksen tavoitteena on

- luoda yhdessä katsaus uusimpiin taloushallintoalaan liittyviin tietoturvatapahtumiin, ja
- tutustua Kyberturvallisuuskeskuksen Kybersää-julkaisuun.

17.9.2024 ©Taloushallintoliitto

22

Kybersää



Huoltovarmuuskeskus

Traficomin Kyberturvallisuuskeskuksen kuukausittain julkaisema Kybersää on ”suunnattu organisaatioiden eri tasoilla tietoturvan parissa työskenteleville. Kybersään tavoitteena on kertoa kybermaailman tapahtumista mahdollisimman ymmärrettävästi ja tiiviissä paketissa.”

Muita tärkeitä Kyberturvallisuuskeskuksen palveluita ovat muun muassa johonkin vakavaan uhkaan liittyvät melko harvinaiset varoitukset:

<https://www.kyberturvallisuuskeskus.fi/fi/varoitukset>

Esimerkiksi vuonna 2024 on julkaistu toistaiseksi vain yksi varoitus, koskien Palo Alto GlobalProtect-tuotetta.

17.9.2024 ©Taloushallintoliitto

23 Kybersään sisältö



Huoltovarmuuskentus

Kybersää käsittelee kuluneen kuukauden tilannetta, ja sisältää seuraavat taloushallintoalalle tärkeät osa-alueet:

- **Tietomurroissa ja -vuodoissa** käsitellään suojauskeinoja sekä kyberturvallisuuskeskuksen tietoon tulleita trendejä tietomurroista ja -vuodoista.
- **Huijauksiin ja tietojenkalasteluun** sisältyy käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia, kiristyskiä ja muita vastaavia huijauksia.
- **Haittaohjelmissa ja haavoittuvuuksissa** käsitellään aihealueen merkittävimmät julkaisut ja havainnot sekä annetaan toimenpidesuosituksia ja linkkejä lisätietoihin.

Muita osa-alueita ovat **Automaatio ja IoT**, viestintäpalveluiden toimivuutta koskeva **Verkkojen toimivuus**, sekä **Vakoiluosio**, joka käsitellään valtiollisten toimijoiden tai niihin liitettyjen ryhmien harjoittamaa kybervakoilua ja -vaikuttamista.

17.9.2024 ©Taloushallinto Liitto

24 Heinäkuun yleistilanne



Huoltovarmuuskentus

Kybersää heinäkuu 2024

Tietomurrot ja -vuodot

- M365-tiliurrot synkistivät aurinkoista kesäsäätä. Heinäkuussa murtojen määrä kasvoi edellisiin kuukausiin nähden. Tunnusten havittelussa käytettiin erityisesti AITM-tekniikkaa.
- Kokonaisuutena tietomurto-ilmoitusten määrä on kesän aikana puolittunut alkuvuoteen nähden.

Huijaukset ja kalastelut

- Huijari väittää soittavansa pankista ja pelottelee uhreja epäilyttävillä tilisiirroilla ulkomaille. Huijari pyytää pankkitunnuksia "palautustiliä" varten.
- Tekstiviesteissä pelotellaan taas "ulosottoon siirtyvällä sakolla" viranomaiselta muistuttavilla TRAF COMin ja TRAF CORNin nimillä.

Haittaohjelmat ja haavoittuvuudet

- CrowdStriken 19.7. häiriö sai opportunistit liikkeelle: CrowdStriken nimissä kalastellaan tietoja ja levitetään haittaohjelmia, joiden väitettiin korjaavan päivityksen aiheuttamat ongelmat.
- Cisco Secure Email Gatewaysta (entinen IronPort) löytyi kriittinen haavoittuvuus.

Automaatio ja IoT

- Langattomien murtosuojaus- ja kameravalvontajärjestelmien häiritseminen on teknisesti helppoa. Yhdysvalloissa poliisit ovat varoittaneet ilmiön olevan kasvussa. Osasyys kasvulle lienee valvontakameroiden yleistymisen kodeissa.^[1]

Verkkojen toimivuus

- Heinäkuussa yleisissä viestintäverkoissa 9 toimivuushäiriötä.
- Palvelunestohyökkäyksiä raportoitii myös kesäaikana, mutta palveluvaikutukset ovat olleet olemattomia.
- Kaikki palvelunestohyökkäykset eivät ole yhdistettävissä haktivistitoimijoihin.

Vakoilu

- Pohjois-Koreaan liitetty kyberuhkatoimija APT45 (Andariel) on hyökännyt kiristyslaitto-ohjelmilla yhdysvaltalaisia terveydenhuollon tarjoajia vastaan ansaitakseen rahaa valtiolle.
- APT45:n vakoiluun kohteena on ollut mm. puolustusteollisuus, ilmailuala ja ydinvoimaan liittyvät organisaatiot.^[4, 5, 6, 7]

TRAFICOM Lähene: ja viestintävirasto
kyberturvallisuuskeskus

Heinäkuun Kybersää 8.8.2024 4

17.9.2024 ©Taloushallinto Liitto

25 Tapaus CrowdStrike



Huoltovarmuuskentus

CrowdStrike-tietoturvaohjelmiston päivitys aiheutti heinäkuussa Windows-laitteissa toistuvan uudelleenkäynnistymistilan (boot loop). Tapauksesta aiheutui häiriöitä ja käyttökatkoja organisaatioille ja eri palveluille ympäri maailmaa.

Ylläpitäjien oli mahdollista korjata ongelma, mutta se edellytti käyntiä tietokoneen luona. Tämän vuoksi häiriön vaikutukset pitkittyivät.

Kyberturvallisuuskeskus julkaisi aiheesta Tietoturva Nyt!-artikkelin:
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/crowdstriken-paivitys-aiheuttanut-hairioita-windows-laitteissa>

17.9.2024 ©Taloushallintoliitto

26 Elokuun yleistilanne



Huoltovarmuuskentus

Kybersää elokuu 2024

Tietomurrot ja -vuodot

- Tietomurroissa kesä jatkui rauhallisena, eikä tavanomaista syksyistä kasvua ilmoitusmäärissä ole nähty.

Huijaukset ja kalastelut

- Veronpalautukset olivat elokuun suosituin huijauksen aihe. Kymmenillä erilaisilla tekstiviestihuijauksilla yritettiin varastaa verkkopankkitunnuksia.
- Pankkitunnuksia kalasteltiin muillakin verukkeilla, kuten sähköyhtiön, teleoperaattorin, Kanta-palvelun, viranomaisten ja tietysti myös pankkien nimissä.

Haittaohjelmat ja haavoittuvuudet

- SonicWall SSL VPN -haavoittuvuutta hyväksikäytetään aktiivisesti.
- Havaintoja on tehty tavanomaista enemmän Quad7- ja Miral-botti-verkoista.
- Laitteiden päivitys ja vanhojen uusiminen korostuvat edelleen tietoturvaohjelmien suojautumisessa.

Automaatio ja IoT

- IoT-järjestelmien hallinta siirtyy yhä enemmän pilveen. Julkisuudessa tuotiin esiin, ettei hajautetun sähköntuotannon ja sähkön varastoinnin pilvipohjaisten etähallintajärjestelmien kyberturvallisuus ole aina riittävän hyvä.
- Palveluiden loppukäyttäjien kannalta tilanne on hankala, ellei turvallisia vaihtoehtoja ole tarjolla.

Verkkojen toimivuus

- Elokuussa yleisissä viestintäverkoissa havaittiin 10 toimivuushäiriötä.
- Viime aikoina on raportoitu paljon lyhytkestoisia palvelunestohyökkäyksiä suomalaisten organisaatioiden palveluihin. Vaikutukset ovat kuitenkin olleet vähäisiä.

Vakoilu

- APT29:n kerrottiin päässeen käsiksi joihinkin Iso-Britannian valtionhallinnon sähköposteihin Microsoftin kohdistuneen tietomurron seurauksena.
- Sama toimija hyödynsi kaupallisten vakoiluohjelmien käyttämiä menetelmiä Mongoliassa. Kohteisiin murtautumisessa hyödynnettiin murretua valtionhallinnon verkkosivua.

TRAFICOM Lähenne- ja viestintävirasto
 Kyberturvallisuuskeskus

Elokuun Kybersää 12.9.2024 4

17.9.2024 ©Taloushallintoliitto

Kybersää nosto: Top 5 uhat lähitulevaisuudessa



Huoltovarmuuskeskus

1. Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista.

2. Kiristyshaittaohjelmat – Merkittävä uhka organisaatioille

Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi.

3. Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

4. Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

Organisaatioiden olisi hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.

5. Tietoliikenneinfran suojaamisen tärkeys korostuu

17.9.2024 ©Taloushallinto Liitto

Kiitos!

Mika Tolvanen ja
Anna Koskinen

mika.tolvanen@taloushallinto.fi



talous
hallinto
liitto



Huoltovarmuuskeskus