IT-asiantuntijan tietoturva

ICT-päätelaitteiden hallinnan parhaat käytännöt ja ajankohtaiskatsaus

talous
hallinnon
koulutukset

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

24.10.2023

talous hallinto liitto

Huoltovarmuuskeskus

Päätelaitteiden hallinnan parhaat käytännöt

Ajankohtaiskatsaus

IT-asiantuntijoiden webinaari

2024

2

Sisältö

talous hallinto liitto

Huoltovarmuuskeskus

Päätelaitteiden hallinnan parhaat käytännöt

1. Tietoturvauhat ja riskit päätelaitteille
2. Tietoturvan inhimilliset tekijät
3. Päätelaitteiden hallinnan keskeiset osa-alueet
4. Identiteettien ja pääsynhallinnan kehittäminen

Ajankohtaiskatsaus

- Akira- ja Lockbit-kiristyshaittaohjelmat
- Mennyt ja tuleva vuosi

4

Tietoturvauhat ja riskit päätelaitteille

talous hallinto liitto

Huoltovarmuuskeskus

- Päätelaitteisiin, kuten työasemiin ja puhelimiin, kohdistuvat yleisimmät tietoturvauhat ovat haittaohjelmat, tietojenkalastelu, laitteiden katoaminen tai varastaminen, päivittämättömien ohjelmistojen haavoittuvuudet sekä luvaton pääsy.
- Nämä uhat voivat johtaa organisaatiossa tietovuotoihin, toiminnan häiriöihin, luottamuksen menetykseen ja oikeudellisiin seuraamuksiin.

25.11.2024 ©Taloushallintoliitto

5

Tietoturvan inhimilliset tekijät

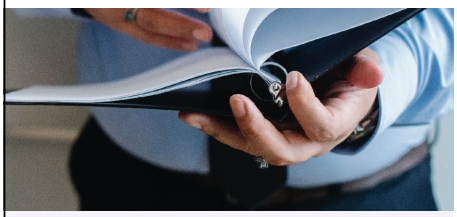
- Vaikka ihmiset voivat olla päätelaitteiden tietoturvan heikoin lenkki huolimattomuuden ja tietämättömyyden kautta, heillä on myös mahdollisuus toimia organisaation tietoturvan selkärankana.
- Hyvin koulutetut, vastuulliset ja turvallisuutta arvostavat työntekijät ovat keskeinen osa kaikkien tietoturvaratkaisujen onnistumista.

25.11.2024 ©Taloushallintoliitto

6

Zero Trust -periaatteet

Zero Trust on tietoturvastrategia. Se ei ole tuote tai palvelu, vaan lähestymistapa seuraavien tietoturvaperiaatteiden suunnitteluun ja toteuttamiseen.



Älä koskaan luota, varmista aina

Tunnista ja valtuuta aina käyttäjät ja päätelaitteet kaikkien saatavilla olevien tietojen perusteella.

Noudata vähimmän oikeuden periaatetta

Rajoita käyttäjien pääsyä hyödyntämällä riskiin perustuvia mukautuvia käytäntöjä sekä tietojen suojausta.

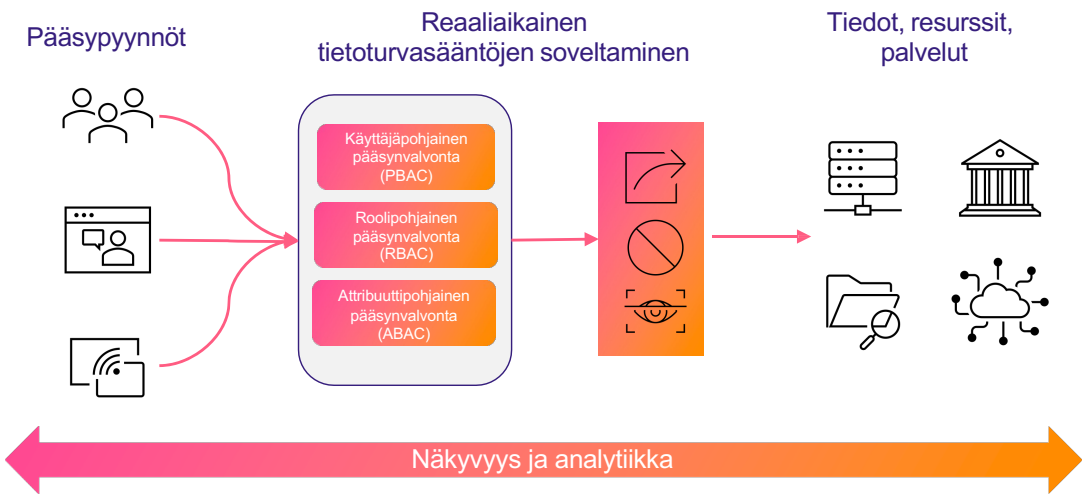
Oleta, että tietomurrot ovat väistämättömiä

Minimoi vahinkojen laajuus ja segmentoi pääsy. Varmista päästä päähän -salaus ja käytä analytiikkaa näkyvyyden parantamiseksi, uhkien tunnistamiseksi ja puolustuksen vahvistamiseksi.

25.11.2024 ©Taloushallintoliitto

7

Zero Trust -arkkitehtuuri



25.11.2024 ©Taloushallintoliitto

8

Päätelaitteiden hallinnan keskeiset osa-alueet

1. Käyttöjärjestelmien ja sovellusten päivittäminen
2. Käyttäjien tunnistaminen ja todennus
3. Tietoturvaohjelmistot
4. Käyttöoikeuksien hallinta
5. Laitteiden salaus
6. Etähallinta ja -valvonta
7. Varmuuskopiointi
8. Käyttäjien koulutus

25.11.2024 ©Taloushallintoliitto

9

Identiteettien ja pääsynhallinnan kehittäminen

- IT on muuttumassa järjestelmistä palveluiksi, ja tämä on muuttanut identiteettien eli tunnusten hallinnan ja pääsynhallinnan roolia tietoturvassa.
- Esimerkiksi Googlen ja Microsoftin identiteettipalveluissa on kehittyneitä toimintoja, jotka tunnistavat mahdollisia väärinkäytöksiä analysoimalla esimerkiksi
  - käyttäjän toimintaa,
  - päätelaitteiden ominaisuuksia, ja
  - sijaintitietoja.
- Huomioi että vaikka nämä palvelut muodostavat audit-lokeja automaattisesti, lokit eivät ole oletuksena saatavilla kuin muutamia kuukausia. Pidempi säilytysaika edellyttää asiakaskohtaisia toimenpiteitä.

25.11.2024 ©Taloushallintoliitto

10

Aloita tästä

Tärkeintä on aloittaa Zero Trust -mallin rakentaminen perusasioista, jotka mahdollistavat tietoturvan vahvistamisen heti. Luo vankka tietoturvan perusta, jossa identiteetti, laitteet, data ja verkot ovat hallinnassa.

Tavoitteet:

- **Identiteetin hallinta ja vahva tunnistautuminen:** Ota käyttöön monivaiheinen tunnistautuminen (MFA) kaikille käyttäjille. Hallitse käyttäjien pääsyoikeuksia vähimmän oikeuden periaatteella.
- **Laitteiden turvallisuus:** Varmista, että kaikki päätelaitteet ovat ajantasaisia ja suojattuja haittaohjelmilta. Laitteiden turvallisuuden tila tulee tarkistaa ennen resurssien käyttöä.
- **Datansuojaus:** Salaa kaikki data levossa ja siirron aikana. Varmista, että arkaluonteista tietoa ei säilytetä tai käsitellä suojaamattomissa ympäristöissä.
- **Verkon segmentointi:** Jaa verkko osiin niin, että pääsy on rajattu vain niille palveluille ja järjestelmille, joita käyttäjä tai laite tarvitsee.

Mieti seuraavia kysymyksiä:

- Ovatko kaikki käyttäjätunnukset ja niiden käyttöoikeudet ajan tasalla?
- Onko monivaiheinen tunnistautuminen (MFA) otettu käyttöön kaikille käyttäjille?
- Noudatetaanko vähimmän oikeuden periaatetta pääsynhallinnassa?
- Tunnistetaanko ja hallitaanko kaikki organisaation päätelaitteet?
- Ovatko käyttöjärjestelmät ja sovellukset ajan tasalla?
- Käytetäänkö päätelaitteiden salausta ja tietoturvaohjelmistoja?
- Salaammeko kaiken datan levossa ja siirron aikana?

25.11.2024 ©Taloushallintoliitto

11

Kehitä: Vahvista toimintaa ja lisää automaatiota

Kun perustoimenpiteet ovat kunnossa, laajenna Zero Trust -mallin kattavuutta ja automaatiota. Lisää älykkäitä valvonta- ja automaatioratkaisuja sekä syvennä henkilöstön tietämystä.

Tavoitteet:

- **Dynaaminen pääsynhallinta:** Implementoi järjestelmiä, jotka tarkistavat käyttäjän, laitteen ja kontekstin (sijainti, aika, käytetty sovellus) ennen pääsyn myöntämistä.
- **Tapahtumapohjainen valvonta:** Käytä SIEM- ja SOC-palveluja tunnistamaan epäilyttävä toiminta ja reagoimaan siihen nopeasti.
- **Tietovirtojen hallinta:** Tarkista datan kulku järjestelmissä ja varmista, että vain sallitut tietovirrat ovat käytössä.
- **Käyttäjien koulutus:** Kehitä työntekijöiden tietoturvatietoisuutta ja varmista, että he ymmärtävät roolinsa tietoturvan toteuttamisessa.

Mieti seuraavia kysymyksiä:

- Valvotaanko pääsyä jatkuvasti ja reagoidaanko muuttuviin olosuhteisiin (esim. sijainti, käytetty laite)?
- Onko käytössä teknologioita, jotka arvioivat riskiä pääsypyynnön yhteydessä?
- Onko käytössä keskitetty lokitietojen keräys ja analysointi (esim. SIEM)?
- Tunnistammeko epäilyttävän käyttäytymisen tai poikkeamat tehokkaasti?
- Ovatko työntekijät tietoisia tietoturvavelvoitteistaan?
- Onko tietoturvakäytäntöjen noudattamista integroitu osaksi päivittäistä toimintaa?

12

Paranna: Optimointi ja jatkuva kehitys

Tässä vaiheessa keskitytään mallin tehokkuuden parantamiseen ja kehittyneiden uhkien torjuntaan. Optimoi toimintaa, kehitä järjestelmän reagointikykyä ja varmista jatkuva auditointi ja kehitys.

Tavoitteet:

- **Analytiikka ja koneoppiminen:** Hyödynnä edistyneitä analytiikkatyökaluja, jotka havaitsevat poikkeamia käyttäytymisessä ja mahdollistavat nopean reagoinnin.
- **Testaaminen ja simulaatiot:** Testaa organisaation kykyä torjua hyökkäyksiä realistisilla simulaatioilla ja kehitä toimintatapoja tulosten perusteella.
- **Automatisoitu uhkien torjunta:** Kehitä järjestelmiä, jotka eivät pelkästään havaitse uhkia, vaan myös pystyvät torjumaan ne automaattisesti.

Mieti seuraavia kysymyksiä:

- Hyödynnämmekö koneoppimista tai tekoälyä poikkeamien havaitsemiseksi?
- Ovatko työkalumme ajan tasalla uusimpien uhkien torjumiseksi?
- Kuinka hyvin järjestelmämme reagoi simuloituihin uhkiin?
- Vastaavatko tietoturvakäytäntömme alan standardeja ja hyviä käytäntöjä?
- Keräämmekö palautetta käyttäjiltä, jotta voimme parantaa järjestelmän käytettävyyttä ja turvallisuutta?
- Kuinka tehokkaasti hyödynnämme saatuja havaintoja toiminnan kehittämisessä?

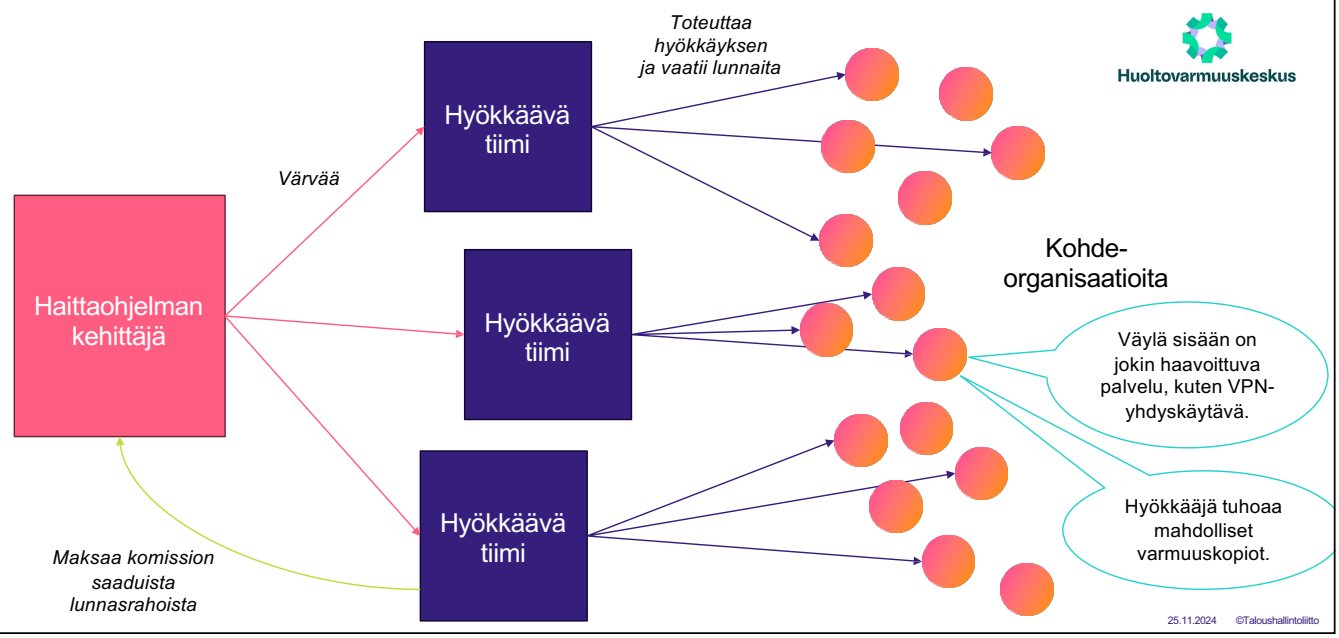
Akira- ja Lockbit-kiristyshaittaohjelmat

talous hallinto liitto

Huoltovarmuuskeskus

- Kyberturvallisuuskeskuksen mukaan kiristyshaittaohjelmat ovat yksi merkittävimmistä organisaatioihin kohdistuvista kyberuhista.
- Viime vuosina Suomessa havaituissa kiristyshaittaohjelmahyökkäyksissä ovat korostuneet Akira ja Lockbit.
- Kyse on järjestäytyneestä rikollisuudesta jonka tavoitteena on rahallinen hyöty.

15 **Järjestäytyneen rikollisuuden toimintamalli**



16 **Kyberturvallisuuden pelikenttä: dataa, ennusteita, strategioita**

Microsoftin vuotuinen digitaalisen suojauksen raportti	• https://www.microsoft.com/en/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
Google's Cybersecurity Forecast 2025	• https://www.gstatic.com/gumdrop/files/cybersecurity-forecast-2025.pdf
Suomen kyberturvallisuus-strategia 2024 -2035	• https://julkaisut.valtioneuvosto.fi/handle/10024/165860

25.11.2024 ©Taloushallintoliitto

17

Raporttien yhteiset teemat

talous hallinto liitto

Huoltovarmuuskeskus

Teknologian nopea kehitys

Tekoäly tuo uusia työkaluja uhkien torjuntaan, mutta antaa myös hyökkääjille välineitä sosiaaliseen manipulointiin ja väärän tiedon levittämiseen.

Geopoliittiset kyberuhat

Venäjä, Kiina, Iran ja Pohjois-Korea jatkavat kybervakoilua ja vaikutusoperaatioita. Lunnas- ja kiristyshaittaohjelmat lisäävät riskejä organisaatioille.

Kyberturvallisuuden painopisteet 2025

Organisaatioiden on panostettava pilvipohjaisiin ratkaisuihin, vahvaan pääsynhallintaan ja uhkien ennakointiin sekä varauduttava kvanttijälkeiseen kryptografiaan.

Kiitos!

Mika Tolvanen

mika.tolvanen@traktal.fi

talous hallinto liitto

Huoltovarmuuskeskus