SUBMARINE SECURITY

CyberSub Dispatch Nro. 01 – 2024

'Detecting threats before they surface'

Pilvipalvelut

Kyberturvallisuuskeskuksen listaamia pilviturvallisuuskäytäntöjä ovat pilvipalvelu-ympäristön erottaminen muusta ympäristöstä ja sen jakaminen segmentteihin, kontrolloitu pilvipalvelun käyttöoikeuksien hallinta, kirjattu pilven kattava tietoturvakäytäntö, relevantti IT-turvallisuusosaaminen, toimivat pilven hallinnointikäytännöt, järjestelmän ja sen käytön monitorointi sekä lopuksi osallistava turvallisuuskulttuuri.

Kyberhygienia

"Kyberhygienia tarkoittaa kyberturvallisuuden kehittämistä ja sen ylläpitämistä, eli omaa ja ympäristön kyberturvallisuutta edistetään säännöllisillä rutiineilla. Kyberhygienian idea on, että turvallisesta toiminnasta tulee osa päivittäistä tekemistä ja tämän takia asiaan tulisi kiinnittää huomiota. Kyberturvallisuus ei ole kaikille ykkösasia, mutta jokaisen tulee tästä huolimatta tiedostaa sen tärkeys ja tehdä välttämätön, jotta pysyy turvassa kybervihollisilta. Hyvän kyberhygienian avulla toimimme turvallisesti arjessamme."

Lähde: Kyberhygienian käsikirja

Digimaturiteetti

Käsiteltäessä aihetta kyberturvallisuuden näkökulmasta on hyvä tiedostaa, mitä kybertoimintaympäristö tarkoittaa. Se ei tarkoita vain elektronista irrallista entiteettiä, vaan se koostuu ihmisten, organisaatioiden ja fyysisten järjestelmien yhdessä muodostamasta vaikutus-ympäristöstä. Kybertoimintaympäristön näkökulmasta kyberturvallisuus osana digitaalista transformaatiota korostaa digimaturiteetin kasvattamisen merkityksen.

NSA (National Security Agency)

NSA:n kymmenen parasta tietoturvauhan lieventämistoimenpidettä:

1) Päivitä ja päivitä ohjelmistot välittömästi
2) Puolusta käyttöoikeuksia ja tilejä
3) Noudata allekirjoitettujen ohjelmistojen suorituskäytäntöjä
4) Harjoittele järjestelmän palautussuunnitelmaa
5) Järjestelmien ja asetusten aktiivinen hallinta
6) Jatkuva verkkojen tunkeutumisen metsästys
7) Tehosta nykyaikaisia laitteiston tietoturvaominaisuuksia
8) Tietoverkkojen erottelu sovellustietoisilla puolustusmekanismeilla
9) Integroi uhkan maineenpalvelut
10) Siirry monivaiheiseen tunnistautumiseen

Resilienssi & Zero Trust -periaate

Resilienssi ymmärretään suomalaisessa turvallisuuskeskustelussa erilaisina yhdistelminä kyvykkyyksiä tai ominaisuuksia.

Resilienssi ja Zero Trust -periaate muodostavat yhdessä keskeisen osan nykyaikaista tietoturvaa. Zero Trust -periaate edustaa nykyaikaista lähestymistapaa tietoturvaan, jossa oletetaan, että verkoston jokainen osa voi olla potentiaalinen hyökkäyksen kohde, ja siksi kaikki verkko-yhteydet ja toimijat tulee varmentaa jatkuvasti.

Vaikka Zero Trust -mallit ovat laajasti käytössä, ne eivät tarjoa kattavia ohjeita kaikilla keskeisillä alueilla, erityisesti tietojen varmuuskopioinnin ja palauttamisen osalta.

keywords - avainsanat: kyberhygienia, digimaturiteetti, resilienssi

Kolme kovaa ladattavaa >> [Download | Read | Share]

Uhkien ennakointi käsittää ensisijaisesti ennalta tehtävät toimenpiteet tietoturvan ja kyberturvallisuuden kannalta.
Parhaita käytäntöjä on paljon. Täältä löydät muutamia. Paremman kyberhygienian puolesta.

- NSA 2018. **NSA'S Top Ten Cybersecurity Mitigation Strategies.** National Security Agency, Central Security Service
- Kyberturvallisuuskeskus 2020. **Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)**. Traficomin julkaisuja 13/2020
- Kyberturvallisuuskeskus 2024. Tietoturva nyt! **Kyberturvallisuuskeskuksen viikkokatsaus - 03/2024**

Tämän dokumentin, (SubmarineSecurity.com -sivuston), tarkoitus on kerätä oikeaa tietoa kyberturvaan liittyvistä aiheista ja jakaa sitä eteenpäin.
Me pyrimme pitämään jakamamme tiedon ajan tasalla säännöllisen päivittämisen ja julkaisutiheyden avulla.

SUBMARINE SECURITY