TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toteuta arviointi

Osiot ja tavoitteet

CRITICAL Kriittisten palveluiden suojaaminen

Organisaation tulee tunnistaa oma roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa ja hallita riskejä sen mukaisesti.

Tavoitteet:

1. Kriittisten palveluiden ja niiden riippuvuuksien tunnistaminen
2. Kriittisten palveluiden hallinta
3. Kriittisten palveluiden kyberhäiriöiden vaikutusten minimointi

Huom. tähän osioon ei kuulu Yleisiä hallintatoimia, eikä osio perustu C2M2-malliin.

ASSET
Omaisuuden, muutoksen ja konfiguraation hallinta

Omaisuuden, muutoksen ja konfiguraation hallinnan osiossa arvioidaan organisaation kykyä hallita toiminnan osa-alueen toimintavarmuuden kannalta tärkeää omaisuutta ja tähän omaisuuteen liittyviä muutoksia ja konfiguraatioita.

Omaisuudella tarkoitetaan organisaation IT- ja OT-omaisuutta (mkl. laitteet ja ohjelmistot) sekä tietovarantoja. Organisaation tulee hallinnoida tätä omaisuutta suhteessa sekä omaisuuteen kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

1. Laitteiden ja ohjelmistojen hallinta
2. Tietovarantojen hallinta
3. Konfiguraation hallinta
4. Muutoksenhallinta
5. Yleisiä hallintatoimia

THREAT Uhkien ja haavoittuvuuksien hallinta

Uhkien ja haavoittuvuuksien hallinnan osiossa arvioidaan organisaation kykyä havaita ja hallita mahdollisia kyberuhkia ja haavoittuvuuksia.

Organisaation tulee määritellä ja ylläpitää suunnitelmia, prosesseja ja teknologiaa, joiden avulla havaita, tunnistaa, analysoida, hallita ja vastata kyberuhkiin ja haavoittuvuuksiin. Toimien tulee olla suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

1. Haavoittuvuuksien vähentäminen
2. Uhkien torjunta ja uhkatiedon jakaminen
3. Yleisiä hallintatoimia

RISK Riskienhallinta

Riskienhallinnan osiossa arvioidaan organisaation kykyä tunnistaa ja hallita toimintaansa kohdistuvia kyberturvallisuusriskejä (eli kyberriskejä). Organisaation tulee luoda ja ylläpitää koko organisaation kattavaa riskienhallintaohjelmaa tunnistaakseen, arvioidakseen ja hallitakseen kyberriskejä.

Riskienhallintaohjelman tulee kattaa kaikki organisaation liiketoimintayksiköt, tytäryhtiöt, toiminnan kannalta kriittisen infrastruktuurin ja tärkeimmät sidosryhmät.

Tavoitteet:

1. Kyberriskienhallinnan suunnitelma
2. Kyberriskien tunnistaminen
3. Riskien analysointi
4. Riskeihin reagointi
5. Yleisiä hallintatoimia

ACCESS Identiteetin- ja pääsynhallinta

Identiteetin ja pääsynhallinnan osiossa arvioidaan organisaation kykyä hallita ja rajoittaa pääsyä suojattaviin kohteisiin. Organisaation tulee luoda ja ylläpitää identiteettejä toimijoille, joille halutaan myöntää pääsy fyysisesti tai verkon yli organisaation suojattaviin kohteisiin.

Organisaation tulee hallita käyttöoikeuksia suojattaviin kohteisiin suhteessa sekä niihin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin. Heikko pääsynhallinta voi johtaa laitteiden, ohjelmistojen tai tiedon luvattomaan käyttöön, julkistamiseen, tuhoamiseen tai peukalointiin. Lisäksi se nostaa tarpeettomasti organisaation riskitaso.a

Tavoitteet

1. Identiteettien luominen ja hallinta
2. Loogisten käyttöoikeuksien hallinta
3. Fyysinen pääsynhallinta
4. Yleisiä hallintatoimia

SITUATION Tilannekuva

Tilannekuvan osiossa arvioidaan organisaation kykyä määritellä ja ylläpitää organisaation kyberturvallisuuden tilannekuvaa. Organisaation tulee määritellä ja ylläpitää prosesseja ja teknisiä ratkaisuja operatiivisen ja kyberturvallisuustiedon keräämiseen, analysointiin, hälytysten nostamiseen, esittämiseen ja käyttämiseen, hyödyntäen muissa Kybermittarin osioissa mainittua informaatiota.

Tilannekuva muodostetaan sekä organisaation toiminnan, että kyberturvallisuuden tasosta.

Tavoitteet

1. Lokienhallinta
2. Ympäristöjen valvonta
3. Tilannekuvan ylläpito
4. Yleisiä hallintatoimia

RESPONSE Tapahtumien ja häiriötilanteiden hallinta

Tapahtumien ja häiriötilanteiden hallinnan osiossa arvioidaan organisaation kykyä hallita, reagoida ja palautua kybertapahtumista ja -häiriöistä.

Organisaation tulee määritellä ja ylläpitää suunnitelmia, prosesseja ja teknologiaa kyberturvallisuuteen liittyvien tapahtumien ja häiriöiden havaitsemiseksi, analysoimiseksi, niihin vastaamiseksi ja niistä palautumiseksi suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

1. Tapahtumien havainnointi
2. Tapahtumien analysointi ja häiriötilanteiden määrittäminen
3. Tapahtumiin ja häiriöihin reagoiminen
4. Kyberturvallisuus osana toiminnan jatkuvuutta
5. Yleisiä hallintatoimia

THIRD-PARTIES
Toimitusketjun ja ulkoisten riippuvuuksien hallinta

Toimitusketjun ja ulkoisten riippuvuuksien hallinnan osiossa arvioidaan organisaation kykyä tunnistaa ja hallita toimitusketjuihin ja kolmansiin osapuoliin liittyviä riskejä.

Riippuvuusriskien hallinta sisältää hallintatoimenpiteitä kuten riippumatonta testausta, koodikatselmointeja, haavoittuvuusskannauksia tai turvallisen ohjelmistokehityksen vaatimuksia. Toimittajien, alihankkijoiden ja muiden kolmansien osapuolten kanssa solmitut sopimukset tuotteista ja palveluista tulee tarkastaa ja hyväksyttää kyberriskien hallinnan näkökulmasta. Toimittajille ja palveluille voidaan asettaa valvonta- ja auditointivaatimuksia varmistamaan, että ne täyttävät niille asetetut kyberturvallisuus- ja toimintakykyvaatimukset.

Tavoitteet

1. Kumppaniverkoston tunnistaminen ja priorisointi
2. Kumppaniverkostoon liittyvien riskien hallinta
3. Yleisiä hallintatoimia

WORKFORCE Henkilöstön hallinta

Henkilöstön hallinnan osiossa arvioidaan organisaation kykyä kehittää ja ylläpitää henkilöstön kyberturvallisuusosaamista ja -valmiutta.

Organisaation tulee määritellä ja ylläpitää suunnitelmia, prosesseja, teknologiaa ja kontrolleja organisaation kyberturvallisuuskulttuurin luomiseksi ja sopivan ja osaavan henkilöstön takaamiseksi, suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

1. Kyberturvallisuuden vastuiden jakaminen
2. Kyberturvallisuuteen keskittyvän henkilöstön kehittäminen
3. Henkilöstöhallinnon prosessit
4. Koulutus ja kybertietoisuuden lisääminen
5. Yleisiä hallintatoimia

ARCHITECTURE Kyberturvallisuusarkkitehtuuri

Kyberturvallisuusarkkitehtuurin osiossa arvioidaan organisaation kykyä hallita ja ylläpitää kyberturvallisuustoimintaansa.

Organisaation tulee luoda ja ylläpitää rakenteita, joilla se hallinnoi ja ohjaa organisaation kyberturvallisuuskontrolleja, -prosesseja ja muiden kyberturvallisuuden osa-alueiden toimintaa suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin.

Tavoitteet

1. Kyberarkkitehtuurin kehittäminen
2. Tietoverkkojen suojaus osana kyberarkkitehtuuria
3. Laitteiden ja ohjelmistojen turvallisuus osana kyberarkkitehtuuria
4. Sovellusturvallisuus osana kyberarkkitehtuuria
5. Tietojen suojaus osana kyberarkkitehtuuria
6. Yleisiä hallintatoimia

PROGRAM Kyberturvallisuusohjelma

Kyberturvallisuusohjelman osiossa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuista kyberturvallisuusohjelmaa.

Kyberturvallisuusohjelman tarkoitus on määritellä kyberturvallisuuden hallintamalli ("governance"), kyberturvallisuuden strateginen kehittäminen ja liiketoimintajohdon tuki kyberturvallisuudelle tavalla, joka on suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin nähden.

Tavoitteet

1. Kyberturvallisuusstrategia
2. Johdon tuki kyberturvallisuusohjelmalle
3. Yleisiä hallintatoimia

YLEISIÄ HALLINTATOIMIA
Yhteinen tavoite kaikkien osioiden arvioinnissa

- Seuraavat käytännöt arvioidaan erikseen jokaisen osion yhteydessä *(pl. osio CRITICAL)*:
  - A. Osion toimintaa varten on määritetty dokumentoidut toimintatavat, joita noudatetaan ja päivitetään säännöllisesti. (kypsyystaso 2)
  - B. Osion toimintaa varten on tarjolla riittävät resurssit (henkilöstö, rahoitus ja työkalut). (kypsyystaso 2)
  - C. Osion toimintaa ohjataan vaatimuksilla, jotka on asetettu organisaation johtotason politiikassa (tai vastaavassa ohjeistuksessa). (kypsyystaso 3)
  - D. Osion toiminnan suorittamiseen tarvittavat vastuut, tilivelvollisuudet ja valtuutukset on osoitettu soveltuville työntekijöille. (kypsyystaso 3)
  - E. Osion toimintaa suorittavilla työntekijöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen. (kypsyystaso 3)
  - F. Osion toiminnan vaikuttavuutta arvioidaan ja seurataan. (kypsyystaso 3)
- Mikäli organisaatio noudattaa samoja käytäntöjä läpi koko organisaation tai useammalla kuin yhdellä osa-alueella, voi samoja vastauksia hyödyntää noissa osioissa