NIST Cybersecurity Framework 2.0

1 Linkki viitekehykseen

https://www.nist.gov/cyberframework

2 Käyttöoikeustieto

Viitekehys on kehitetty ja julkaistu Yhdysvaltain National Institute of Standards and Technology (NIST) -viraston toimesta, ja se on tarkoitettu julkiseen käyttöön.

Organisaatiot voivat vapaasti käyttää ja soveltaa viitekehystä omiin tarpeisiinsa ilman lisenssimaksuja.

3 Tyyppi, esimerkiksi viitekehys tai malli

Viitekehys

4 Viitekehyksen kuvaus

NIST Cybersecurity Framework (CSF) on Yhdysvaltain National Institute of Standards and Technologyn (NIST) ja muiden toimijoiden yhteistyössä laatima viitekehys, joka auttaa organisaatioita hallitsemaan kyberturvallisuusriskejä.

Viitekehys tarjoaa systemaattisen lähestymistavan kyberturvallisuuden parantamiseen ja koostuu kuudesta avaintoiminnosta. Toiminnot jakautuvat viitekehyksessä useampaan alikategoriaan sekä näiden yksityiskohtaisempiin toimenpiteisiin ja niiden muodostamiin kyvykkyyksiin.

5 Ylläpito ja tuki

National Institute of Standards and Technology (NIST)

6 Soveltaminen

Organisaatio voi soveltaa viitekehystä kyber- ja digiturvallisuuden kokonaisvaltaiseen hallintaan ja kehittämiseen.

Viitekehys muodostaa kuuden avaintoiminnon kautta kattavan kokonaisuuden kyberturvallisuuden hallinnasta. Viitekehyksen soveltamista voidaan toteuttaa esimerkiksi prosessimaisesti vaiheittain. Tällöin soveltava organisaatio aloittaa tunnistamalla omaan toimintaympäristöön

liittyvät tekijät, kuten suojattavat digitaaliset kohteet, infrastruktuurin, säädökset ja muut vaatimukset. Kun kyberturvallisuuteen liittyvät vaatimukset ja reunaehdot on tunnistettu, voidaan suojautumiseen ja havainnointiin käytetyt ratkaisut suunnitella käyttäen hyödyksi tätä tietoa. Viitekehyksen avaintoimintojen tarkoituksena on lisäksi auttaa rakentamaan kattavat rakenteet poikkeamatilanteisiin reagointiin, niistä palautumiseen sekä kertyneiden oppien ja kokemusten hyödyntämiseen jatkokehittämisessä.

Kuva 1. NIST Cybersecurity Framework 2.0. (kuva: NIST)

Avaintoiminnot ovat:

- **Govern (Hallinnointi):** Organisaatiolla on hallintorakenteet ja prosessit digitaalisen turvallisuuden hallintaan. Käytännössä tämä tarkoittaa, että organisaation digitaaliseen turvallisuuteen liittyvät strategiat, käytännöt ja prosessit ovat linjassa organisaation toiminnan kanssa, ja digitaalista turvallisuutta johdetaan ja kehitetään säännönmukaisesti.

- **Identify (Tunnistaminen):** Organisaatio on tunnistanut oman toimintaympäristönsä sekä toiminnan mahdollistavat ja toiminnan jatkuvuuteen liittyvät kriittiset suojattavat kohteet ja omaisuuden. Lisäksi organisaatio tunnistanut näihin kohdistuvat uhat ja riskit sekä niiden mahdollisen vaikutuksen toimintaansa.

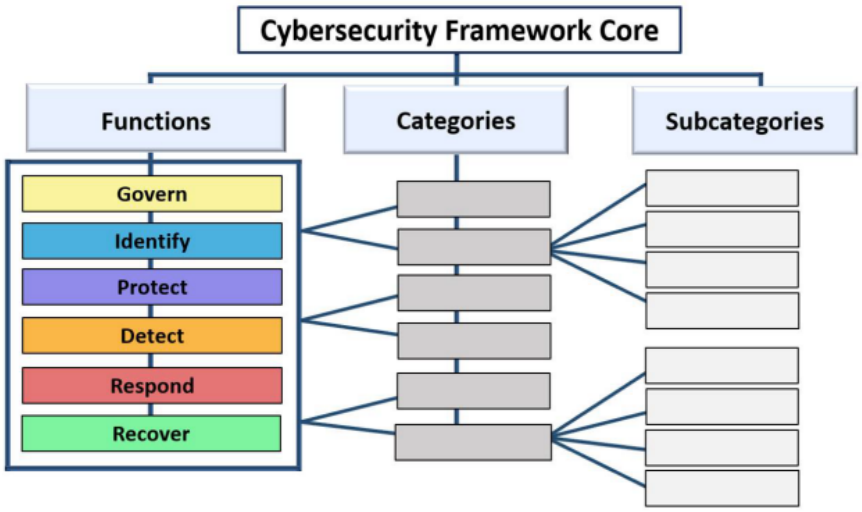
- **Protect (Suojaaminen):** Organisaatio suojaa tunnistetut kohteet, kuten tietojärjestelmät, tietovarannot ja tiedot riskienhallinnan keinoin tunnistetuilta uhilta ja riskeiltä. Käytännössä tämä tarkoittaa muun muassa identiteetin- ja pääsynhallinnan, tietoverkkojen turvallisuuden, tietoturvallisuuden, tietoturvateknologian suunnittelua ja toteuttamista suhteessa tunnistettuihin riskeihin sekä näiden toimenpiteiden dokumentointia ja kuvaamista.

- **Detect (Havainnointi):** Organisaatio kehittää digitaaliseen turvallisuuteen vaikuttavien häiriöiden havainnointikyvykkyyttä. Käytännössä tämä tarkoittaa poikkeamanhallintaprosessin määrittelyä ja toteuttamista siten, että organisaatio on määritellyt digitaalisen turvallisuuden perustason ja ottanut käyttöön prosessin ja menetelmät, joilla digitaalisen turvallisuuteen vaikuttavia tapahtumia havaitaan ja havainnointikyvykkyyttä saadaan parannettua.

- **Respond (Reagointi):** Organisaatiolla on kyvykkyys reagoida havaittuihin digitaalisen turvallisuuden poikkeamiin mahdollisimman nopeasti poikkeamanhallintaprosessin mukaisesti. Käytännössä tämä tarkoittaa poikkeamahallintaprosessin toteuttamista siten, että henkilökunta ja sidosryhmät tietävät tehtävänsä ja roolinsa reagointitoimenpiteissä, viestintä-, koordinaatio- ja raportointikäytännöt on määritelty ja digitaalisen turvallisuuden häiriötapahtumia hallitaan ja niiden vaikutusta lievennetään.

- **Recover (Palautuminen):** Organisaatiolla on kyvykkyys toipua digitaalisen turvallisuuden aiheuttamista häiriöstä takaisin normaaliin toimintatilaan. Käytännössä tämä tarkoittaa kriittisten suojattavien järjestelmien toipumissuunnitelmien luontia ja kehittämistä häiriötilanteista toipumisesta saatujen kokemusten perusteella sekä suunnitelmien tekoa mahdollisten digitaalisen turvallisuuden häiriöstä aiheutuvien mainehaittojen korjaamiseksi.

Edellä mainitut avaintoiminnot jakautuvat viitekehyksissä edelleen jakautuvat useampaan alikategoriaan sekä näiden yksityiskohtaisempiin toimenpiteisiin ja niiden muodostamiin kyvykkyyksiin.



Kuva 2. NIST Cybersecurity Framework 2.0 toiminnot ja kategoriat. (kuva: NIST)

NIST Cybersecurity Framework on suunniteltu joustavaksi ja mukautuvaksi, joten organisaatiot voivat soveltaa sitä omien tarpeidensa ja riskiprofiiliensa mukaan.

7 Muuta huomioitavaa

Digi- ja väestötietoviraston laatima digitaalisen turvallisuuden arkkitehtuurin viitekehys pohjautuu NIST Cybersecurity Framework versioon 1.1. Löydät lisätietoa digitaalisen turvallisuuden arkkitehtuurista avoimesta työtilasta Digitaalisen turvallisuuden arkkitehtuuri sekä eOppivan koulutuksesta Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla.