WITH secure

Kyberturvallisuuden tarkastuslista

Kattava lista organisaatiosi suojaamiseen

Mietitkö, mitkä asetukset, ohjelmistot ja hallinnolliset kyberturvallisuustoimenpiteet organisaatiosi tarvitsee?
Tai ehkä et ole varma oikeasta priorisointi- ja toteutussuunnitelmasta?

WithSecure esittelee kattavan tarkastuslistan, joka on kehitetty yhteistyössä eri alojen asiantuntijoiden kanssa. Tämä lista tarjoaa laajan näkökulman kyberturvallisuuteen, jäsentäen tehtävät niiden prioriteetin ja monimutkaisuuden mukaan. Tarkastuslista on suunniteltu erityisesti auttamaan organisaatioita suojaamaan IT-ympäristönsä tehokkaasti.

Kyberturvallisuuden tarkastuslista

1. Peruspilarit →

Omaisuudenhallinta

- [ ] Hanki kattava käsitys IT-järjestelmistä, kuten palvelimista ja tietokoneista, sekä niiden merkityksestä liiketoimintaprosesseissa ja arvoketjuissa.

Verkko- ja päätelaiteturvallisuus

- [ ] Ota käyttöön asianmukaiset verkkoturvakontrollit, kuten palvelu-, verkko- ja päätelaitepalomuurit, sekä päätelaitesuojausohjelmistot laitteiden (työasemat, palvelimet ja mobiililaitteet) turvaamiseksi.

Identiteetin ja pääsynhallinta (IAM)

- [ ] Ota käyttöön monivaiheinen todennus (MFA) kaikille SaaS-palveluille ja varmista, että etäkäytössä olevat laitteet yhdistyvät yrityksen infrastruktuuriin vain VPN + MFA:lla tai muilla vahvoilla todennus- ja salausmenetelmillä.
- [ ] Minimoi järjestelmien ja palveluiden, mukaan lukien päätelaitteiden, ylläpitäjätilien määrä.

Päivitysten hallinta

- [ ] Suunnittele ja toteuta tehokas prosessi kriittisten tietoturvapäivitysten asentamiseksi kaikille teknologioille (käyttöjärjestelmät, verkkolaitteet ja ohjelmistot). Aseta etusijalle internetiin yhteydessä olevat resurssit.

Yhteistyöympäristöjen suojaus

- [ ] Ota käyttöön suojausratkaisut sähköpostille, pilvitallennukselle sekä yhteistyöalustoille ja varmista turvallinen viestintä.

Liiketoiminnan jatkuvuus ja katastrofien hallinta (BC/DR)

- [ ] Toteuta säännölliset varmuuskopiot varmistaaksesi tietojen palauttamisen.

Laitteiden hallinta

- [ ] Ota käyttöön keskitetty hallinta palvelimille ja päätelaitteille (työasemat, mobiililaitteet) ja varmista tehokas valvonta ja hallinta.

Tietosuojatoimenpiteet

- [ ] Salaa päätelaitteet ja tallennetut arkaluontoiset tiedot suojataksesi niitä luvattomalta käytöltä.

Politiikat ja vaatimustenmukaisuus

- [ ] Määrittele hyväksyttävät käyttöpolitiikat sille, miten työntekijöiden tulee käyttää tekoälyä, yrityslaitteita, verkkoja ja tietoja.
- [ ] Tunnista lait, standardit, säännökset (esim. NIS2) ja sopimusvelvoitteet, joita sinun on noudatettava.

Tietoturvatietoisuus ja koulutus

- [ ] Kouluta työntekijöitä kyberturvallisuuden perushygieniaan sekä kyberuhkien tunnistamiseen ja niihin reagointiin.

2. Näkyvyys ja reagointivalmius →

Lokitus ja valvonta

- [ ] Määritä keskitetty lokitus ja priorisoi kriittiset järjestelmät.

Uhkien havaitseminen, valvonta ja reagointi

- [ ] Ota käyttöön Endpoint Detection and Response (EDR) — ohjelmisto tietokoneille ja palvelimille.
- [ ] Laajenna EDR-taitojasi XDR:n avulla: älä rajoitu vain päätelaitteiden suojaamiseen, vaan ota käyttöön myös Identity- ja Cloud Detection and Response -kyvykkyydet.
- [ ] Hanki hallittu havaitsemis- ja reagointipalvelu MDR-palveluntarjoajalta tai kumppanilta jatkuvaa valvontaa ja reagointia varten.
- [ ] Varmista osaavien incident response -asiantuntijoiden saatavuus kriisitilanteessa tekemällä etukäteen IR-palvelusopimus ja sopimalla toimitusehdot.
- [ ] Ota käyttöön edistynyt verkkoliikenteen valvonta poikkeavuuksien havaitsemiseksi.
- [ ] Ota käyttöön SIEM-kyvykkyydet ja priorisoi kriittiset järjestelmät paremman uhkien havainnointikyvyn saavuttamiseksi.

Altistuksen ja riskien hallinta

- [ ] Ota käyttöön altistuksen hallintaratkaisu/palvelu kattavaa riskinarviointia varten. Tämä palvelu yhdistää haavoittuvuudet ja konfigurointivirheet, tunnistaa hyökkäysreitit sekä tarjoaa näkyvyyden laitteisiin, identiteetteihin ja pilviympäristöihin.

Ohjelmisto-omaisuuden hallinta

- [ ] Kehitä kattava ymmärrys ohjelmistosovelluksista ja -lisensseistä sekä niiden vaikutuksesta liiketoimintaprosesseihin ja säännöstenmukaisuus-vaatimuksiin.

Liiketoiminnan jatkuvuus ja katastrofien hallinta (BC/DR)

- [ ] Laadi katastrofipalautumissuunnitelmat liiketoiminnan jatkuvuuden varmistamiseksi.

Uhkatiedustelu

- [ ] Hyödynnä uhkien tiedustelua pysyäksesi askeleen edellä kehittyviä uhkia.

3. Kovennus ja valvonnan syventäminen →

Järjestelmän koventaminen

- [ ] Poista kaikki tarpeettomat palvelut ja ominaisuudet käytettävistä teknologioista, erityisesti jos ne ovat etäyhteyksien kautta saatavilla. Rajoita ja kovenna jäljelle jäävät palvelut teknisellä tasolla mahdollisimman rajoitetuiksi (palveluiden koventaminen, hyökkäyspinnan minimointi).

Sovellushallinta (APM)

- [ ] Salli vain hyväksyttyjen ohjelmistojen, ohjelmistokirjastojen ja skriptien suorittaminen järjestelmissäsi.

Liiketoiminnan jatkuvuus ja katastrofien hallinta (BC/DR)

- [ ] Määritä muuttumattomat varmuuskopiot kriittisille järjestelmille.

Identiteetti- ja pääsynhallinta (IAM)

- [ ] Ota käyttöön single sign-on (SSO) organisaatiossa sujuvan pääsynhallinnan varmistamiseksi.
- [ ] Privileged Access Management (PAM): Rajoita ja valvo etuoikeutettuja käyttäjätilejä.
- [ ] Ota käyttöön Zero Trust -arkkitehtuuri: Mihinkään käyttäjään, laitteeseen tai järjestelmään ei tule luottaa oletuksena, vaan kaikissa pääsypyynnöissä on suoritettava tiukka identiteetin varmennus ja jatkuva valvonta riippumatta siitä, tuleeko pyyntö verkon sisäpuolelta tai ulkopuolelta.
- [ ] Ota käyttöön etäyhteyden aikakatkaisu vähentääksesi luvattoman pääsyn riskiä ja jos mahdollista, ota käyttöön salasanaton ympäristö parannetun turvallisuuden takaamiseksi.

Verkkoturvallisuus

- [ ] Ota käyttöön verkkosegmentointi tarkoituksen ja kriittisyyden mukaan (esim. laskentajärjestelmät, arkaluonteiset tiedot).

Uhkien havaitseminen, valvonta ja reagointi

- [ ] Laadi yksityiskohtaiset häiriötilanteen reagointisuunnitelmat ja pelikirjat eri skenaarioita varten.

Tietojen suojaus

- [ ] Luokittele tiedot arkaluonteisuuden mukaan ja sovella asianmukaisia suojauksia. Ota käyttöön tietovuotojen estämisratkaisut (DLP).
- [ ] Ota käyttöön Data Encryption Everywhere -strategia varmistaaksesi, että kaikki tiedot ovat aina salattuja sekä levossa että siirron aikana.

4. Testaus ja sertifiointi

Altistuksen ja riskien hallinta

- [ ] Tunnista keskeiset toimittajat ja kolmannet osapuolet toimitusketjussasi. Arvioi toimitusketjun kyberturvariskit ja kehitä riskien vähentämisstrategioita toimitusketjun riskien hallitsemiseksi ja liiketoiminnan jatkuvuuden varmistamiseksi.

Liiketoiminnan jatkuvuus ja katastrofien hallinta (BC/DR)

- [ ] Suorita kriisinhallinnan harjoituksia testataksesi ja parantaaksesi palautumissuunnitelmiasi.

Tietoturvatietoisuus ja koulutus

- [ ] Järjestä säännöllisiä huijausviestiharjoituksia työntekijöille tietoisuuden lisäämiseksi.

Uhkien havaitseminen, valvonta ja reagointi

- [ ] Suorita kyberhyökkäyksen hallintaharjoituksia testataksesi ja parantaaksesi häiriötilanteiden suunnitelmiasi.
- [ ] Suorita purple team -harjoitus testataksesi ja parantaaksesi tietoturvatasoasi.

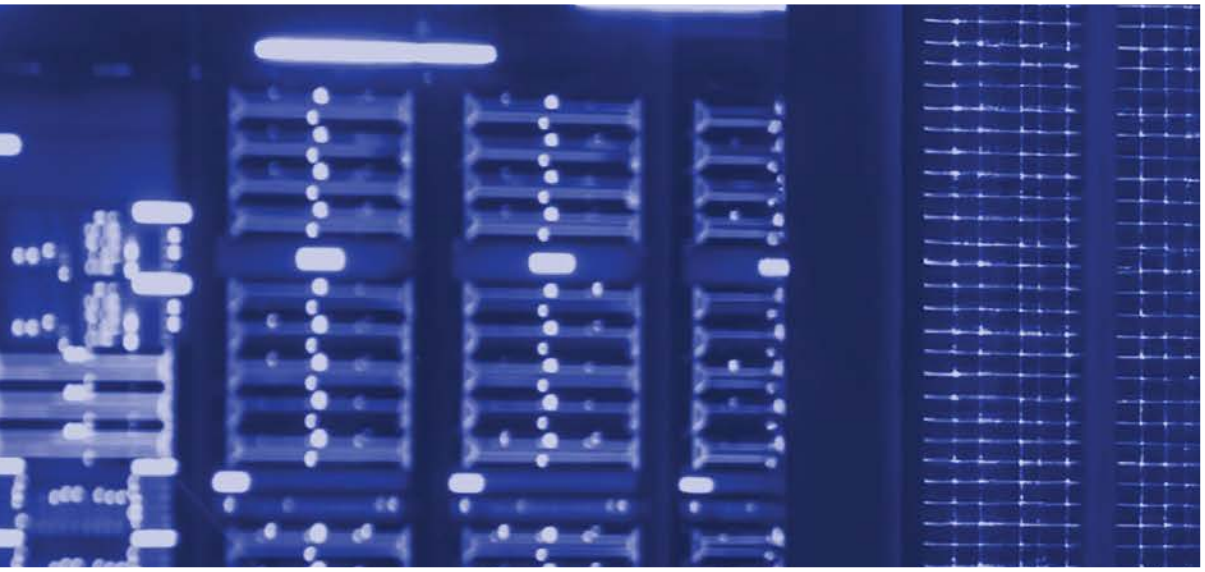
Sääntöjenmukaisuus ja hallinta

- [ ] Ota käyttöön ja ylläpidä tietoturvallisuuden hallintajärjestelmää (ISMS), joka tarjoaa järjestelmällisen lähestymistavan arkaluonteisen tiedon hallintaan, varmistaa sen luottamuksellisuuden, eheyden ja saatavuuden sekä tukee standardien, kuten ISO 27001:n, noudattamista riskienhallinnan ja sääntöjenmukaisuuden parantamiseksi.
- [ ] Aloita sertifikaattien, kuten ISO 27001 tai SOC2, hankkiminen osoittaaksesi sääntöjenmukaisuuden.
- [ ] Säännölliset tarkastukset ja arvioinnit: suorita itsenäisiä ja ulkopuolisia arviointeja kyberturvatasostasi.

Prioriteetti / Vaikeustaso liikennevalot:

- — välttämätön, kriittinen
- — tärkeä
- — korkeat kustannukset, korkeatasoinen valmius

WITH secure



Tarvitsetko apua kyberturvallisuusprojektien priorisoinnissa ja toteutuksessa?

Suojaa organisaatiosi – ota yhteyttä WithSecureen ja aloita jo tänään!

URL www.withsecure.com/fi/about-us/company-contacts/contact-sales

WithSecure Corporation
Välimerenkatu 1
00180 Helsinki
Finland