Alhainen — Maturiteetti — Korkea

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.

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.

Identiteetin- ja pääsynhallinta (IAM): Minimoi järjestelmien ja palveluiden, mukaan lukien päätelaitteiden, ylläpitäjätilien määrä.

Politiikat ja vaatimustenmukaisuus: Määrittele hyväksyttävät käyttöpolitiikat sille, miten työntekijöiden tulee käyttää tekoälyä, yrityslaitteita, verkkoja ja tietoja.

Tietoturvatietoisuus ja koulutus: Kouluta työntekijöitä kyberturvallisuuden perushygieniaan sekä kyberuhkien tunnistamiseen ja niihin reagointiin.

Politiikat ja vaatimustenmukaisuus: Tunnista lait, standardit, säännökset (esim. NIS2) ja sopimusvelvoitteet, joita sinun on noudatettava.

Näkyvyys ja reagointivalmius

Uhkien havaitseminen, valvonta ja reagointi: Ota käyttöön Endpoint Detection and Response (EDR) -ohjelmisto tietokoneille ja palvelimille.

Uhkien havaitseminen, valvonta ja reagointi – Laajenna EDR: Älä rajoitu vain päätelaitteiden suojaamiseen, vaan ota käyttöön myös Identity- ja Cloud Detection and Response -toiminnot

Lokitus ja valvonta: Määritä keskitetty lokitus ja priorisoi kriittiset järjestelmät.

Uhkien havaitseminen, valvonta ja reagointi: Hanki hallittu havaitsemis- ja reagointipalvelu MDR-palveluntarjoajalta tai kumppanilta jatkuvaa valvontaa ja reagointia varten.

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 vaatimustenmukaisuuteen.

Liiketoiminnan jatkuvuus ja katastrofipalautuminen: Laadi katastrofipalautumissuunnitelmat liiketoiminnan jatkuvuuden varmistamiseksi.

Uhkien havaitseminen, valvonta ja reagointi: Hanki tapahtumavastepalvelu varmistaaksesi pätevien toimijoiden saatavuus.

Uhkien havaitseminen, valvonta ja reagointi: Ota käyttöön edistynyt verkkoliikenteen valvonta poikkeavuuksien havaitsemiseksi.

Uhkien havaitseminen, valvonta ja reagointi: Ota käyttöön SIEM-kyvykkyydet ja priorisoi kriittiset järjestelmät paremman uhkien havainnointikyvyn saavuttamiseksi.

Uhkatiedustelu: Hyödynnä uhkien tiedustelua ja pysy askeleen edellä nousevia uhkia.

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.

Identiteetti- ja pääsynhallinta (IAM): Ota käyttöön single sign-on (SSO) organisaatiossa sujuvan pääsynhallinnan varmistamiseksi.

Liiketoiminnan jatkuvuus ja palautumissuunnitelma (BC/DR): Määritä muuttumattomat varmuuskopiot kriittisille järjestelmille.

Verkkoturvallisuus: Ota käyttöön verkkosegmentointi tarkoituksen ja kriittisyyden mukaan (esim. laskentajärjestelmät, arkaluonteiset tiedot).

Identiteetti- ja pääsynhallinta (IAM): Privileged Access Management (PAM): Rajoita ja valvo etuoikeutettuja käyttäjätilejä.

Identiteetti- ja pääsynhallinta (IAM): 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 vai ulkopuolelta.

Identiteetti- ja pääsynhallinta (IAM): Ota käyttöön etäyhteyden aikakatkaisu vähentääksesi luvattoman pääsyn riskiä ja jos mahdollista, ota käyttöön salasanaton ympäristö parannetun turvallisuuden takaamiseksi.

Uhkatunnistus, valvonta ja reagointi: Laadi yksityiskohtaiset häiriötilanteen reagointisuunnitelmat ja pelikirjat eri skenaarioita varten.

Tietojen suojaus: Luokittele tiedot sensitiivisyyden mukaan ja sovella asianmukaisia suojauksia. Ota käyttöön tietovuotojen estämisratkaisut (DLP).

Tietosuoja: Ota käyttöön Data Encryption Everywhere -strategia varmistaaksesi, että kaikki tiedot ovat aina salattuja sekä levossa että siirron aikana.

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 palautumissuunnitelma (BC/DR): Suorita kriisinhallinnan harjoituksia testataksesi ja parantaaksesi palautumissuunnitelmiasi.

Uhkien havaitseminen, valvonta ja reagointi: Suorita häiriötilanteiden hallintaharjoituksia testataksesi ja parantaaksesi häiriötilanteiden suunnitelmiasi.

Tietoturvatietoisuus ja koulutus: Järjestä säännöllisiä huijausviestiharjoituksia työntekijöille tietoisuuden lisäämiseksi.

Sääntöjenmukaisuus ja hallinta: Ota käyttöön ja ylläpidä Tietoturvallisuuden hallintajärjestelmää (ISMS), joka luo järjestelmällisen lähestymistavan arkaluonteisen tiedon hallintaan, varmistaa sen luottamuksellisuuden, eheyden ja saatavuuden, sekä tukee standardeja, kuten ISO 27001, parempaan riskienhallintaan ja sääntöjenmukaisuuteen.

Sääntöjenmukaisuus ja hallinta: Aloita sertifikaattien, kuten ISO 27001 tai SOC2, hankkiminen osoittaaksesi sääntöjenmukaisuuden.

Uhka havainto, valvonta ja reagointi: Suorita purple team -harjoitus testataksesi ja parantaaksesi tietoturvatasoasi.

Sääntöjen noudattaminen ja hallinta: Säännölliset tarkastukset ja arvioinnit – suorita itsenäisiä arviointeja kyberturvatasostasi.

Prioriteetti / Vaikeustaso liikennevalot Välttämätön, kriittinen — Tärkeä — Korkeat kustannukset, hyvä maturiteetti

WITH secure