TIETOLIIKENNETURVALLISUUDEN JOHTAMINEN JA RISKIENHALLINTA

Auditoinnin tavoite

Selvittää, johdetaanko tietoliikenneturvallisuutta tavoitteellisesti ja riskiperusteisesti sekä ovatko vastuut, resurssit ja kehittämistoimet määritelty.

1. Onko tietoliikenneturvallisuuden johtaminen ja riskienhallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko tietoliikenneympäristön kriittiset palvelut, yhteydet, riippuvuudet ja tietovirrat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: verkkokartat, palveluluettelo, riippuvuusanalyysit, tietovirtakuvaukset.

3. Onko tietoliikenteen suojausvaatimukset, hyväksyttävä riskitaso ja lakisääteiset velvoitteet määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: tietoliikenneturvallisuuspolitiikka, riskikriteerit, vaatimusrekisteri, päätökset.

4. [KRIITTINEN] Varmistetaanko, että merkittävät tietoliikenneriskit käsitellään ja jäännösriskit hyväksytään valtuuksien mukaisesti?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: riskirekisteri, käsittelysuunnitelmat, hyväksymispäätökset, toimenpideseuranta.

5. Onko prosessin omistajuus, päätöksenteko-, raportointi- ja eskalointivastuut määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: organisaatiokaavio, vastuumatriisi, tehtävänkuvat, eskalointiohje.

6. Varmistetaanko, että turvallisuustavoitteet, mittarit ja resursointi kytketään liiketoiminnan tarpeisiin?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: tavoite- ja mittariraportit, budjetit, resurssisuunnitelmat, johdon pöytäkirjat.

7. Hallitaanko riskienhallintamallin, politiikkojen ja suojausperiaatteiden muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospäätökset, versiohistoria, katselmuspöytäkirjat, viestintäaineistot.

8. Valvotaanko riskitasoa, tavoitteita, kontrollien toteutumista ja poikkeamia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: riskiraportit, mittaritaulut, kontrolliarvioinnit, johdon katselmukset.

9. Käsitelläänkö tietoliikenteeseen liittyvät turvallisuuspoikkeamat ja riskien realisoituminen hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, juurisyyanalyysit, riskirekisterin päivitykset.

10. [KRIITTINEN] Varmistetaanko, että johtamismallin toimivuutta arvioidaan johdon katselmuksissa ja harjoituksissa?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: katselmuspöytäkirjat, harjoitusraportit, auditoinnit, kehityssuunnitelmat.

VERKKOYMPÄRISTÖN ARKKITEHTUURIN HALLINTA

Auditoinnin tavoite

Selvittää, onko verkkoympäristö suunniteltu, dokumentoitu ja ylläpidetty turvallisuus-, käytettävyys- ja jatkuvuusvaatimusten mukaisesti.

1. Onko verkkoympäristön arkkitehtuurin hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko verkot, aliverkot, yhteydet, verkkolaitteet, palvelut, rajapinnat ja riippuvuudet tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: verkkokaaviot, laiteluettelo, IP-suunnitelma, palvelu- ja yhteysrekisteri.

3. Onko arkkitehtuurin turvallisuus-, kapasiteetti-, käytettävyys- ja jatkuvuusvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: arkkitehtuuriperiaatteet, vaatimusmäärittelyt, riskiarviot, jatkuvuusvaatimukset.

4. [KRIITTINEN] Varmistetaanko, että arkkitehtuuriratkaisut katselmoidaan ja hyväksytään ennen toteutusta tai merkittävää muutosta?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: arkkitehtuurikatselmukset, hyväksymismerkinnät, suunnittelupäätökset, riskipoikkeamat.

5. Onko arkkitehtuurin omistajat, suunnittelijat, hyväksyjät ja ylläpitovastuut määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: RACI-matriisi, tehtävänkuvat, hyväksymisvaltuudet, ylläpitosopimukset.

6. Varmistetaanko, että luottamusrajat, hallintayhteydet, redundanssi ja turvalliset oletusratkaisut kuvataan?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: turvallisuusarkkitehtuuri, luottamusrajakaaviot, redundanssisuunnitelmat, standardit.

7. Hallitaanko verkkotopologian, yhteyksien, palveluiden ja luottamusrajojen muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, päivitetyt verkkokuvat, toteutus- ja palautussuunnitelmat.

8. Valvotaanko arkkitehtuurin ajantasaisuutta, poikkeamia, teknistä velkaa ja kapasiteettia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: arkkitehtuurikatselmukset, poikkeamalistat, kapasiteettiraportit, teknisen velan rekisteri.

9. Käsitelläänkö arkkitehtuurivirheet, dokumentaatiopuutteet ja suojaamattomat yhteydet hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamailmoitukset, ongelmarekisteri, korjaussuunnitelmat, jälkiarvioinnit.

10. [KRIITTINEN] Varmistetaanko, että arkkitehtuurin palautettavuus ja vaihtoehtoiset yhteydet testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: palautumistestit, varayhteystestit, harjoitusraportit, kehitystoimet.

VERKON SEGMENTOINTI JA VYÖHYKKEISTÄMINEN

Auditoinnin tavoite

Selvittää, erotellaanko verkon käyttäjät, laitteet ja palvelut riskien mukaisiin vyöhykkeisiin ja valvotaanko vyöhykkeiden välistä liikennettä.

1. Onko verkon segmentointi ja vyöhykkeistäminen dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko verkkovyöhykkeet, aliverkot, luottamustasot, palvelut ja niiden väliset tietovirrat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: vyöhykekaaviot, VLAN- ja aliverkkoluettelot, tietovirtamatriisit, CMDB.

3. Onko segmentointiperusteet, sallitut tietovirrat ja vyöhykkeiden suojaustasot määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: segmentointiperiaate, luokittelumalli, riskiarviot, tietovirtavaatimukset.

4. [KRIITTINEN] Varmistetaanko, että kriittiset tuotanto-, hallinta- ja palvelinverkot on erotettu käyttäjä-, vierailija- ja ulkoverkoista?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: verkkokaaviot, palomuurisäännöt, reititystaulut, tekniset testitulokset.

5. Onko vyöhykkeiden omistajat sekä sääntöjen hyväksyntä- ja ylläpitovastuut määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: vastuumatriisi, hyväksymispäätökset, muutostyönkulut, ylläpito-ohjeet.

6. Varmistetaanko, että vyöhykkeiden välinen liikenne sallitaan vain dokumentoidun tarpeen perusteella?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: tietovirtamatriisi, ACL- ja palomuurisäännöt, poikkeusluvat, katselmukset.

7. Hallitaanko segmenttien, reitityksen, ACL-sääntöjen ja tietovirtojen muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, testitulokset, konfiguraatioversiot, palautussuunnitelmat.

8. Valvotaanko vyöhykkeiden välistä liikennettä, sääntörikkomuksia ja luvattomia yhteyksiä säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: liikennelokit, hälytykset, SIEM-havainnot, sääntökatselmukset.

9. Käsitelläänkö segmentoinnin ohitukset, väärät reititykset ja luvattomat tietovirrat hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, reititysanalyysit, korjausmuutokset, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että segmentoinnin toimivuus testataan häiriö-, hyökkäys- ja palautumistilanteissa?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: penetraatiotestit, eristystestit, harjoitusraportit, korjaavat toimet.

PALOMUURI- JA LIIKENNESÄÄNTÖJEN HALLINTA

Auditoinnin tavoite

Selvittää, hyväksytäänkö, toteutetaanko, valvotaanko ja poistetaanko palomuuri-, reititys- ja suodatussäännöt hallitusti.

1. Onko palomuuri- ja liikennesääntöjen hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko palomuurit, suodatuspisteet, sääntökannat, objektit, yhteydet ja sääntöjen omistajat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: palomuuriluettelo, sääntörekisteri, objektikannat, yhteysmatriisit.

3. Onko sääntöjen liiketoimintaperusteet, vähimmän sallimisen periaate ja määräajat määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: palomuuripolitiikka, sääntöpyynnöt, riskiarviot, poikkeusluvat.

4. [KRIITTINEN] Varmistetaanko, että avoimet, laajat tai kriittisiin ympäristöihin kohdistuvat säännöt hyväksytään riskiperusteisesti?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: hyväksymismerkinnät, riskiperustelut, sääntökatselmukset, määräaikaiset luvat.

5. Onko sääntöjen tilaajat, tekniset toteuttajat, tarkastajat ja hyväksyjät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: roolit, valtuusmatriisi, työjonot, neljän silmän tarkastukset.

6. Varmistetaanko, että säännöissä rajataan lähde, kohde, palvelu, suunta ja voimassaoloaika mahdollisimman tarkasti?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: sääntökonfiguraatiot, standardit, tekniset tarkastukset, sääntöanalyysit.

7. Hallitaanko uusien sääntöjen, muutosten, poikkeusten ja poistojen käsittely järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, testaukset, toteutuslokit, palautussuunnitelmat.

8. Valvotaanko sääntöjen osumia, käyttämättömiä sääntöjä, poikkeuksia ja luvattomia muutoksia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: palomuurilokit, sääntöosumaraportit, käyttämättömien sääntöjen raportit, hälytykset.

9. Käsitelläänkö virheelliset säännöt, estynyt liikenne, luvattomat avaukset ja sääntömuutokset hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: häiriö- ja poikkeamaraportit, korjausmuutokset, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että sääntökannat varmistetaan ja palautusmenettelyt testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: konfiguraatiovarmistukset, palautustestit, varalaitetestit, harjoitusraportit.

VERKKOLAITTEIDEN TURVALLINEN HALLINTA

Auditoinnin tavoite

Selvittää, asennetaanko, konfiguroidaanko, ylläpidetäänkö ja poistetaanko verkkolaitteet turvallisesti koko elinkaarensa ajan.

1. Onko verkkolaitteiden turvallinen hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko reitittimet, kytkimet, palomuurit, kuormantasaajat, tukiasemat ja hallintajärjestelmät tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: CMDB, laiteluettelo, sarjanumerot, sijainti- ja omistajatiedot.

3. Onko laitteiden kovennus-, päivitys-, hallinta-, lokitus- ja elinkaarivaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: kovennusstandardit, valmistajaohjeet, päivitysvaatimukset, riskiluokitus.

4. [KRIITTINEN] Varmistetaanko, että oletustunnukset poistetaan, hallintaliikenne suojataan ja tarpeettomat palvelut estetään?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: konfiguraatio-otokset, hallintaverkkokaaviot, tunnistusasetukset, porttiskannaukset.

5. Onko laiteomistajat, pääkäyttäjät, ylläpitäjät ja hyväksyjät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: pääkäyttäjäluettelo, käyttöoikeuspäätökset, roolit, ylläpitosopimukset.

6. Varmistetaanko, että hyväksyttyjä kovennusmalleja, vahvaa tunnistamista ja salattuja hallintaprotokollia käytetään?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: kovennusraportit, asetuspohjat, tarkistuslistat, vaatimustenmukaisuusskannaukset.

7. Hallitaanko konfiguraatioiden, ohjelmistoversioiden ja laitteistojen muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, konfiguraatioversiot, testitulokset, toteutuslokit.

8. Valvotaanko laitteiden tilaa, kirjautumisia, konfiguraatiomuutoksia ja hälytyksiä säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: laitelokit, NMS-raportit, autentikointilokit, konfiguraatiopoikkeamat.

9. Käsitelläänkö laiteviat, väärät määritykset, luvattomat kirjautumiset ja hallintayhteydet hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: häiriöraportit, lokianalyysit, korjaustoimet, toimittajailmoitukset.

10. [KRIITTINEN] Varmistetaanko, että konfiguraatiot varmistetaan ja laitteiden vaihto- sekä palautusmenettelyt testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: varmuuskopiot, palautustestit, varalaiteluettelo, vaihtoharjoitukset.

ETÄYHTEYKSIEN HALLINTA

Auditoinnin tavoite

Selvittää, toteutetaanko henkilöstön, ylläpidon ja kumppaneiden etäyhteydet tunnistetusti, salatusti, rajatusti ja valvotusti.

1. Onko etäyhteyksien hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko etäyhteysratkaisut, käyttäjäryhmät, kumppanit, päätelaitteet ja yhteyskohteet tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: VPN- ja etäyhteysluettelo, käyttäjäryhmät, kumppanirekisteri, kohdeluettelo.

3. Onko etäyhteyksien hyväksyntä-, tunnistus-, salaus-, päätelaite- ja lokitusvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: etäkäyttöpolitiikka, hyväksymiskriteerit, MFA-vaatimukset, päätelaitevaatimukset.

4. [KRIITTINEN] Varmistetaanko, että etäylläpito kriittisiin järjestelmiin edellyttää vahvaa tunnistamista ja erillistä valvottua hallintakanavaa?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: MFA-asetukset, hallintayhteyskaaviot, istuntotallenteet, tekniset testit.

5. Onko yhteyksien tilaajat, hyväksyjät, tekniset ylläpitäjät ja valvojat määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: käyttöoikeuspyynnöt, hyväksymispäätökset, roolit, vastuuluettelot.

6. Varmistetaanko, että yhteydet rajataan käyttäjän, laitteen, kohteen, ajan ja käyttötarkoituksen mukaan?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: VPN-konfiguraatiot, ryhmäpolitiikat, laitevaatimukset, aikarajoitukset.

7. Hallitaanko etäkäyttöoikeuksien, VPN-ratkaisujen, asetusten ja kumppaniyhteyksien muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, käyttöoikeuskatselmukset, asetusten versiohistoria, testit.

8. Valvotaanko etäkirjautumisia, epäonnistuneita yrityksiä, sijainteja, laitteita ja istuntoja säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: VPN-lokit, autentikointilokit, SIEM-hälytykset, istuntoraportit.

9. Käsitelläänkö luvattomat etäyhteydet, tunnusten väärinkäyttö ja poikkeavat istunnot hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, tunnusten sulkemiset, lokianalyysit, tutkintaraportit.

10. [KRIITTINEN] Varmistetaanko, että etäyhteyspalvelun kapasiteetti, vararatkaisut ja sulkemismenettelyt testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: kapasiteettitestit, varayhteystestit, sulkemisharjoitukset, palautusohjeet.

LANGATTOMIEN VERKKOJEN TURVALLISUUDENHALLINTA

Auditoinnin tavoite

Selvittää, suojataanko langattomat verkot, tukiasemat, käyttäjät ja laitteet riskitason mukaisesti ja erotetaanko eri käyttötarkoitukset toisistaan.

1. Onko langattomien verkkojen turvallisuudenhallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko langattomat verkot, SSID:t, tukiasemat, ohjaimet, peittoalueet ja käyttäjäryhmät tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: WLAN-luettelo, tukiasemakartat, SSID-rekisteri, peittoaluekartoitukset.

3. Onko salauksen, tunnistamisen, segmentoinnin, vierailijakäytön ja laitehallinnan vaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: WLAN-politiikka, salausstandardit, vierailijaverkon vaatimukset, riskiarviot.

4. [KRIITTINEN] Varmistetaanko, että yritys-, vierailija- ja laiteverkot erotetaan ja heikkojen salausmenetelmien käyttö estetään?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: konfiguraatiot, segmentointitestit, salausasetukset, langattomat skannaukset.

5. Onko WLAN-palvelun omistajat, ylläpitäjät, hyväksyjät ja valvontavastuut määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: roolit, käyttöoikeusluettelot, ylläpitosopimukset, hyväksymispäätökset.

6. Varmistetaanko, että vahvaa salausta, yksilöllistä tunnistamista, sertifikaatteja ja turvallisia asetuksia käytetään?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: ohjainasetukset, sertifikaattimääritykset, kovennustarkastukset, testiraportit.

7. Hallitaanko SSID-, salaus-, tunnistus-, kanava- ja tukiasemamuutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, konfiguraatioversiot, hyväksynnät, toteutuslokit.

8. Valvotaanko luvattomia tukiasemia, heikkoja signaaleja, poikkeavia kirjautumisia ja kuormitusta säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: WLAN-lokit, WIDS/WIPS-hälytykset, kuormitusraportit, luvattomien laitteiden havainnot.

9. Käsitelläänkö luvattomat tukiasemat, heikot asetukset, tunnusten väärinkäyttö ja häirintä hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, paikannustiedot, korjaustoimet, tutkintalokit.

10. [KRIITTINEN] Varmistetaanko, että langattoman verkon kapasiteetti, vararatkaisut ja palautus testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: kapasiteetti- ja palautustestit, varalaitteet, harjoitusraportit, suunnitelmat.

TIEDONSIIRRON SALAUKSEN HALLINTA

Auditoinnin tavoite

Selvittää, suojataanko luottamukselliset tiedot siirron aikana hyväksytyillä salausmenetelmillä ja hallitaanko avaimet sekä varmenteet turvallisesti.

1. Onko tiedonsiirron salauksen hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko salattavat tietovirrat, protokollat, varmenteet, avaimet, päätepisteet ja omistajat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: tietovirtakartat, salausrekisteri, varmenne- ja avainluettelot, palveluomistajat.

3. Onko tiedon luokitteluun perustuvat salaus-, protokolla-, avain- ja varmennevaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: salauspolitiikka, tiedonluokittelu, hyväksytyt algoritmit, tekniset standardit.

4. [KRIITTINEN] Varmistetaanko, että luottamuksellisia tietoja ei siirretä salaamattomilla tai vanhentuneilla protokollilla?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: protokollaskannaukset, TLS-konfiguraatiot, tekniset testit, poikkeusluvat.

5. Onko salausratkaisujen omistajat, avainhallinnan ylläpitäjät ja hyväksyjät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: avainhallintaroolit, käyttöoikeudet, tehtävien eriytys, hyväksymispäätökset.

6. Varmistetaanko, että vain hyväksyttyjä algoritmeja, avainpituuksia, protokollaversioita ja varmenteita käytetään?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: konfiguraatiot, varmenneketjut, avainpituudet, vaatimustenmukaisuusraportit.

7. Hallitaanko salausasetusten, algoritmien, avainten, varmenteiden ja päätepisteiden muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, varmenteiden uusinnat, avainvaihtolokit, testitulokset.

8. Valvotaanko varmenteiden voimassaoloa, heikkoja protokollia, salausvirheitä ja poikkeamia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: varmennevalvonta, protokollaskannaukset, hälytykset, virheraportit.

9. Käsitelläänkö vanhentuneet varmenteet, avainvuodot, salausvirheet ja suojaamattomat tietovirrat hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, avainten sulkemiset, varmenteiden peruutukset, tutkintatiedot.

10. [KRIITTINEN] Varmistetaanko, että avainten ja varmenteiden uusiminen, palautus ja hätätilanteen vaihto testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: avainten palautustestit, hätäuusimiset, varajärjestelyt, harjoitusraportit.

VERKKOPALVELUJEN SUOJAAMINEN

Auditoinnin tavoite

Selvittää, suojataanko internetissä ja sisäverkossa tarjottavat verkkopalvelut hyökkäyksiltä, väärinkäytöltä ja luvattomalta pääsyltä.

1. Onko verkkopalvelujen suojaaminen dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko julkiset ja sisäiset verkkopalvelut, rajapinnat, päätepisteet, taustajärjestelmät ja omistajat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: palveluluettelo, rajapintarekisteri, verkkokaaviot, omistajatiedot.

3. Onko palvelukohtaiset tunnistus-, salaus-, suodatus-, kovennus- ja saatavuusvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: turvallisuusvaatimukset, uhkamallit, riskiarviot, palvelukohtaiset suunnitelmat.

4. [KRIITTINEN] Varmistetaanko, että julkiset palvelut suojataan kerroksittain ja erotetaan sisäverkon kriittisistä resursseista?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: WAF- ja palomuurisäännöt, DMZ-ratkaisut, penetraatiotestit, hyväksynnät.

5. Onko palveluomistajat, tekniset ylläpitäjät, turvallisuusvastuut ja hyväksyjät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: vastuumatriisi, ylläpitoroolit, palvelusopimukset, hyväksymispäätökset.

6. Varmistetaanko, että kovennusta, vähimpiä palveluja, WAF-suojausta ja turvallisia protokollia käytetään tarpeen mukaan?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: kovennusraportit, porttiskannaukset, protokolla-asetukset, tarkistuslistat.

7. Hallitaanko palveluiden, rajapintojen, suodatusten, sertifikaattien ja taustayhteyksien muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, testitulokset, julkaisu- ja palautussuunnitelmat, lokit.

8. Valvotaanko palvelujen saatavuutta, hyökkäyksiä, virheitä, haavoittuvuuksia ja poikkeavaa käyttöä säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: WAF-lokit, palvelulokit, valvontahälytykset, saatavuusraportit.

9. Käsitelläänkö hyökkäykset, väärinkäytökset, tietovuodot ja palvelun häiriöt hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, tutkintalokit, korjausjulkaisut, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että palvelujen palautuminen, kuormansieto, varaympäristöt ja sulkeminen testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: kuormitus- ja palautustestit, varaympäristöt, harjoitusraportit, suunnitelmat.

NIMIPALVELU-, OSOITE- JA REITITYSTURVALLISUUS

Auditoinnin tavoite

Selvittää, hallitaanko DNS-, DHCP-, IP-osoite- ja reitityspalvelut keskitetysti, turvallisesti, jäljitettävästi ja häiriönsietoisesti.

1. Onko nimipalvelu-, osoite- ja reititysturvallisuus dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko DNS- ja DHCP-palvelut, IP-osoitealueet, reititykset, nimialueet ja hallintavastuut tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: DNS-alueet, IPAM-rekisteri, DHCP-alueet, reititystaulut, palvelinluettelo.

3. Onko nimipalvelun, osoitehallinnan, reitityksen, valtuutusten ja jatkuvuuden vaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: DNS/DHCP/IPAM-standardit, reitityspolitiikka, turvallisuusvaatimukset, riskiarviot.

4. [KRIITTINEN] Varmistetaanko, että kriittiset nimipalvelu- ja reititysmuutokset hyväksytään, todennetaan ja suojataan väärentämiseltä?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: DNSSEC-asetukset, reitityssuodatus, muutosten hyväksynnät, tekniset testit.

5. Onko DNS-, DHCP-, IPAM- ja reitityspalvelujen omistajat, ylläpitäjät ja hyväksyjät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: ylläpitoroolit, käyttöoikeudet, valtuusmatriisi, tehtävien eriytys.

6. Varmistetaanko, että hallintayhteydet, vyöhykesiirrot, dynaamiset päivitykset ja reititysprotokollat suojataan?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: palvelinkonfiguraatiot, vyöhykesiirtorajoitukset, reititysasetukset, kovennusraportit.

7. Hallitaanko nimi-, osoite-, reititys-, delegointi- ja palvelinmuutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, IPAM-merkinnät, konfiguraatioversiot, toteutuslokit.

8. Valvotaanko nimikyselyitä, reititysmuutoksia, osoiteristiriitoja, väärinkäyttöä ja saatavuutta säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: DNS- ja DHCP-lokit, reitityshälytykset, IP-konfliktiraportit, valvontanäkymät.

9. Käsitelläänkö DNS-väärentäminen, reittikaappaus, osoiteristiriidat ja palvelukatkot hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, lokianalyysit, reittitarkastukset, korjaustoimet.

10. [KRIITTINEN] Varmistetaanko, että nimipalvelun, osoitehallinnan ja reitityksen varajärjestelyt testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: varapalvelintestit, reitityksen failover-testit, palautusharjoitukset, raportit.

VERKKOLIIKENTEEN VALVONTA JA LOKIENHALLINTA

Auditoinnin tavoite

Selvittää, kerätäänkö, suojataanko, analysoidaanko ja säilytetäänkö verkkoliikenteen sekä verkkolaitteiden lokit riittävästi poikkeamien havaitsemiseksi.

1. Onko verkkoliikenteen valvonta ja lokienhallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko valvottavat verkot, laitteet, tietovirrat, lokilähteet, keräimet ja käyttötapaukset tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: lokilähdeluettelo, verkkokartat, SIEM-käyttötapaukset, tietovirtakuvaukset.

3. Onko lokitettavat tapahtumat, säilytysajat, aikasynkronointi, suojaus ja hälytysrajat määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: lokituspolitiikka, säilytysvaatimukset, käyttötapausmäärittelyt, aikasynkronointiohje.

4. [KRIITTINEN] Varmistetaanko, että kriittisten verkkolaitteiden ja rajapintojen lokit toimitetaan keskitettyyn valvontaan muuttumattomina?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: SIEM-liitännät, lokinäytteet, eheystarkastukset, lähdekattavuusraportit.

5. Onko lokilähteiden omistajat, valvontatiimi, tutkijat ja käyttöoikeuksien hyväksyjät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: käyttöoikeusmatriisi, valvontavastuut, päivystyslistat, hyväksymispäätökset.

6. Varmistetaanko, että lokit suojataan poistamiselta, muuttamiselta ja luvattomalta katselulta?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: säilytysasetukset, salaus, WORM-ratkaisut, käyttöoikeuslokit, tarkastukset.

7. Hallitaanko lokilähteiden, keräyksen, hälytyssääntöjen ja säilytysaikojen muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, hälytyssääntöjen versiot, testitulokset, hyväksynnät.

8. Valvotaanko liikennepoikkeamia, tunnistusvirheitä, konfiguraatiomuutoksia ja hyökkäysindikaattoreita säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: SIEM-näkymät, hälytysraportit, valvontapäiväkirjat, poikkeamaraportit.

9. Käsitelläänkö puuttuvat lokit, valvontakatkot, epäilyttävä liikenne ja luvattomat muutokset hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: tutkintatapaukset, valvontakatkoraportit, korjaustoimet, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että lokikeräyksen kapasiteetti, varmistus, palautus ja valvonnan jatkuvuus testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: kapasiteettitestit, varmistus- ja palautustestit, valvontaharjoitukset, raportit.

TUNKEUTUMISEN JA PALVELUNESTOHYÖKKÄYSTEN TORJUNTA

Auditoinnin tavoite

Selvittää, tunnistetaanko ja torjutaanko verkkohyökkäykset sekä palvelunestot riskien mukaisilla teknisillä ja toiminnallisilla keinoilla.

1. Onko tunkeutumisen ja palvelunestohyökkäysten torjunta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko suojattavat yhteydet, palvelut, IDS/IPS-ratkaisut, DDoS-suojaukset ja reagointikanavat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: IDS/IPS- ja DDoS-luettelo, suojattujen palvelujen lista, yhteyskaaviot.

3. Onko havainto-, esto-, kapasiteetti-, eskalointi- ja palveluntarjoajavaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: torjuntavaatimukset, palvelutasot, riskiarviot, eskalointikriteerit.

4. [KRIITTINEN] Varmistetaanko, että kriittisille internet-palveluille on käytössä testattu palvelunesto- ja tunkeutumissuojaus?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: tekniset konfiguraatiot, suojaustestit, kapasiteettitiedot, palvelusopimukset.

5. Onko suojausratkaisujen omistajat, valvontatiimi, operaattorit ja päätöksentekijät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: vastuumatriisi, päivystyslista, operaattoriyhteydet, päätösvaltuudet.

6. Varmistetaanko, että havainto- ja estoprofiilit pidetään ajantasaisina ja väärät positiiviset hallitaan?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: allekirjoituspäivitykset, estoprofiilit, poikkeusluvat, virityspöytäkirjat.

7. Hallitaanko suojauslaitteiden, allekirjoitusten, estoprofiilien ja palveluntarjoajaratkaisujen muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, testitulokset, konfiguraatioversiot, hyväksynnät.

8. Valvotaanko hyökkäysliikennettä, estotapahtumia, kapasiteettia ja suojauspalvelun saatavuutta säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: IDS/IPS-lokit, DDoS-raportit, liikenneanalyysit, kapasiteettihälytykset.

9. Käsitelläänkö tunkeutumisyritykset, palvelunestot, väärät estot ja suojauskatkot hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: hyökkäysraportit, estotoimet, liikennekaappaukset, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että DDoS-ohjaus, puhdistuspalvelu, eskalointi ja palautuminen harjoitellaan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: DDoS-harjoitukset, operaattoritestit, palautumisraportit, kehitystoimet.

VERKKOHAAVOITTUVUUKSIEN JA PÄIVITYSTEN HALLINTA

Auditoinnin tavoite

Selvittää, tunnistetaanko verkkolaitteiden ja -palvelujen haavoittuvuudet sekä korjataanko ne riskiperusteisesti ja määräajoissa.

1. Onko verkkohaavoittuvuuksien ja päivitysten hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko verkkolaitteet, ohjelmistoversiot, verkkopalvelut, valmistajat ja tukiajat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: laite- ja ohjelmistoluettelo, versiotiedot, tukiaikarekisteri, omistajatiedot.

3. Onko haavoittuvuuksien seuranta-, luokittelu-, korjausaika-, testaus- ja poikkeusvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: haavoittuvuudenhallintaohje, korjausajat, riskiluokitus, poikkeusmenettely.

4. [KRIITTINEN] Varmistetaanko, että kriittiset, aktiivisesti hyväksikäytetyt haavoittuvuudet käsitellään nopeutetulla menettelyllä?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: haavoittuvuustiedotteet, riskipäätökset, kiireelliset muutokset, korjausraportit.

5. Onko omistajat, haavoittuvuuksien arvioijat, päivittäjät, testaajat ja hyväksyjät määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: vastuumatriisi, työjonot, tehtävänkuvat, hyväksymismerkinnät.

6. Varmistetaanko, että päivitykset hankitaan luotetuista lähteistä ja testataan ennen tuotantoon vientiä?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: päivityspaketit, allekirjoitustarkastukset, testiympäristöt, testiraportit.

7. Hallitaanko ohjelmisto-, laiteohjelmisto-, allekirjoitus- ja konfiguraatiopäivitykset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, päivityslokit, palautussuunnitelmat, konfiguraatioversiot.

8. Valvotaanko haavoittuvuuksia, valmistajailmoituksia, tukiaikoja ja korjausten etenemistä säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: skannausraportit, valmistajasyötteet, korjausmittarit, vanhentumisraportit.

9. Käsitelläänkö hyväksikäyttöyritykset, epäonnistuneet päivitykset ja ylitetyt korjausajat hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, epäonnistuneiden päivitysten selvitykset, korjaavat toimet.

10. [KRIITTINEN] Varmistetaanko, että päivitysten palautus, varalaitteet ja kiireellisen korjauksen menettely testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: palautustestit, varalaitetestit, kiireellisen muutoksen harjoitukset, raportit.

VERKKOLAITTEIDEN HALLINTAPALVELUJEN JA -YHTEYKSIEN TURVALLISUUS

Auditoinnin tavoite

Selvittää, onko yrityksen reitittimien ja muiden verkkolaitteiden hallintapalvelut suojattu, tarpeettomat ja vanhentuneet palvelut poistettu käytöstä sekä hallintaliikenne rajattu, valvottu ja jäljitettävä.

1. [KRIITTINEN] Onko SNMPv1 poistettu käytöstä kaikissa verkkolaitteissa?

Hyväksymiskriteeri: SNMPv1 ei ole käytössä tuotanto-, testi- eikä varalaitteissa. Mahdolliset poikkeukset on dokumentoitu, riskit arvioitu ja käytölle on määritelty hyväksytty määräaika sekä korvaava suojaus.

Todentava näyttö: verkkolaitteiden asetukset, konfiguraatio-otteet, verkkolaiterekisteri, poikkeuspäätökset, haavoittuvuusskannauksen tulokset.

2. [KRIITTINEN] Onko SNMPv2 ja SNMPv2c poistettu käytöstä kaikissa verkkolaitteissa?

Hyväksymiskriteeri: SNMPv2- ja SNMPv2c-versioita ei käytetä verkkolaitteiden valvontaan tai hallintaan. Mahdolliset väliaikaiset poikkeukset on hyväksytty, dokumentoitu ja suojattu rajoittavilla verkkosäännöillä.

Todentava näyttö: verkkolaitteiden konfiguraatiot, valvontajärjestelmän asetukset, SNMP-yhteisömerkkijonojen tarkastus, poikkeusrekisteri.

3. [KRIITTINEN] Käytetäänkö SNMP-hallinnassa SNMPv3 authPriv-suojaustasoa?

Hyväksymiskriteeri: SNMPv3-yhteydet käyttävät authPriv-suojaustasoa, jossa käyttäjä tunnistetaan vahvasti ja tietoliikenne salataan. Käytössä olevat tunnistus- ja salausmenetelmät ovat yrityksen hyväksymiä ja ajantasaisia.

Todentava näyttö: SNMPv3-asetukset, käyttäjä- ja ryhmämääritykset, valvontajärjestelmän määritykset, salaus- ja tunnistusasetukset, yhteystestien tulokset.

4. [KRIITTINEN] Onko Cisco Smart Install poistettu käytöstä kaikissa Cisco-verkkolaitteissa?

Hyväksymiskriteeri: Cisco Smart Install -palvelu ei ole käytössä verkkolaitteissa, ellei sen käytölle ole dokumentoitua, hyväksyttyä ja riskiperusteisesti perusteltua tarvetta. Tarpeettomat palveluun liittyvät määritykset on poistettu.

Todentava näyttö: Cisco-laitteiden konfiguraatiot, palvelutilan tarkastus, verkkoskannauksen tulokset, muutospyynnöt ja toteutusmerkinnät.

5. [KRIITTINEN] Onko verkkolaitteiden hallintaporttien käyttö internetistä estetty?

Hyväksymiskriteeri: Internetistä ei ole suoraa pääsyä TFTP-, Smart Install- tai SNMP-hallintapalveluihin. Vähintään seuraavien porttien tarpeeton liikenne on estetty: UDP 69, TCP 4786, UDP 161 ja 162 sekä TCP/UDP 10161 ja 10162.

Todentava näyttö: palomuurisäännöt, reitittimien ACL-säännöt, ulkoisen porttiskannauksen tulokset, verkkokaaviot, palomuurilokit.

6. Hyväksytäänkö välttämättömät internetistä avattavat hallintayhteydet riskiperusteisesti?

Hyväksymiskriteeri: Internetistä sallittu hallintayhteys perustuu dokumentoituun liiketoimintatarpeeseen ja hyväksyttyyn riskiarvioon. Yhteys on rajattu lähdeosoitteen, kohteen, portin ja käyttötarkoituksen perusteella sekä suojattu vahvalla tunnistautumisella ja salauksella.

Todentava näyttö: hyväksymispäätös, riskiarvio, palomuuri- ja ACL-säännöt, yhteyskuvaus, määräaikainen poikkeuslupa, käyttö- ja valvontalokit.

7. [KRIITTINEN] Onko verkkolaitteiden hallintaliikenne rajattu erilliseen hallintaverkkoon tai hyväksytyille hallintalaitteille?

Hyväksymiskriteeri: Verkkolaitteiden hallintayhteydet sallitaan ACL- tai palomuurisäännöillä vain nimetyistä hallintaverkoista, hallintapalvelimista tai hyväksytyistä ylläpitolaitteista. Tavallisista käyttäjä-, vierailija- ja tuotantoverkoista ei ole tarpeetonta pääsyä hallintapalveluihin.

Todentava näyttö: verkkokaavio, verkon vyöhykemäärittely, ACL-säännöt, palomuurisäännöt, hallintalaitteiden luettelo, yhteystestien tulokset.

8. [KRIITTINEN] Ovatko reitittimien ja muiden verkkolaitteiden ohjelmistot tietoturvallisesti ajan tasalla?

Hyväksymiskriteeri: Verkkolaitteiden käyttöjärjestelmä- ja laiteohjelmistoversiot tunnetaan, valmistajien tietoturvatiedotteita seurataan ja kriittiset päivitykset asennetaan yrityksen määrittelemissä määräajoissa. Päivitykset testataan ja toteutetaan hallitulla muutosmenettelyllä.

Todentava näyttö: verkkolaiterekisteri, ohjelmistoversioraportit, päivityssuunnitelmat, muutospyynnöt, valmistajien tietoturvatiedotteet, toteutus- ja testausraportit.

9. [KRIITTINEN] Korvataanko elinkaarensa päässä olevat verkkolaitteet hallitusti?

Hyväksymiskriteeri: Valmistajan tuen, ohjelmistopäivitysten tai tietoturvakorjausten ulkopuolella olevat laitteet tunnistetaan ja niille laaditaan hyväksytty korvaussuunnitelma. Väliaikaiset riskit käsitellään rajoittavilla suojaustoimilla.

Todentava näyttö: laite- ja elinkaarirekisteri, valmistajan tukitiedot, korvaussuunnitelma, investointipäätökset, riskiarviot, poikkeusluvat.

10. Käytetäänkö verkkolaitteissa yksilöllisiä ja turvallisesti suojattuja salasanoja?

Hyväksymiskriteeri: Verkkolaitteissa ei käytetä yhteisiä oletussalasanoja tai samaa salasanaa useissa laitteissa tai käyttäjätunnuksissa. Cisco-laitteissa salasanat tallennetaan yrityksen hyväksymällä turvallisella menetelmällä; salasanatyyppiä 8 suositaan ja suojaamattomia tai heikkoja tyyppejä 0, 4 ja 7 vältetään.

Todentava näyttö: salasanapolitiikka, Cisco-laitteiden konfiguraatio-otteet, tunnusluettelo, pääsynhallintajärjestelmän asetukset, teknisen tarkastuksen tulokset.

11. Valvotaanko verkkolaitteisiin luotuja paikallisia käyttäjätilejä?

Hyväksymiskriteeri: Verkkolaitteiden paikalliset käyttäjätilit on yksilöity, hyväksytty ja rajattu välttämättömiin käyttötarkoituksiin. Uusista, muutetuista tai epätavallisista paikallisista käyttäjätileistä muodostetaan hälytys tai ne tarkastetaan viipymättä.

Todentava näyttö: paikallisten tunnusten luettelo, laitekonfiguraatiot, käyttöoikeushyväksynnät, SIEM- tai valvontahälytykset, tarkastusraportit.

12. Hälytetäänkö paikallisilla tunnuksilla tehdyistä kirjautumisista?

Hyväksymiskriteeri: Paikallisilla verkkolaitetunnuksilla tehdyt kirjautumiset kirjataan keskitetysti ja niistä muodostetaan riskiin perustuvia hälytyksiä. Hälytykset tutkitaan ja niiden käsittely voidaan jäljittää.

Todentava näyttö: kirjautumislokit, SIEM-säännöt, hälytysraportit, tutkintamerkinnät, pääsynhallinnan raportit.

13. [KRIITTINEN] Havaitaanko ja käsitelläänkö SNMP Set -pyynnöt?

Hyväksymiskriteeri: SNMP Set -pyynnöt on lähtökohtaisesti estetty, ellei niiden käytölle ole hyväksyttyä tarvetta. Sallitut pyynnöt rajataan nimetyille järjestelmille ja käyttäjille, kirjataan lokeihin ja poikkeavasta käytöstä muodostetaan hälytys.

Todentava näyttö: SNMP-oikeusmääritykset, read-only- ja read-write-asetukset, ACL-säännöt, SNMP-lokit, SIEM-hälytykset, tutkintaraportit.

14. Kerätäänkö verkkolaitteiden turvallisuustapahtumat keskitettyyn lokienhallintaan?

Hyväksymiskriteeri: Verkkolaitteiden kirjautumiset, käyttäjämuutokset, konfiguraatiomuutokset, SNMP-tapahtumat ja hallintayhteydet välitetään keskitettyyn lokienhallinta- tai valvontajärjestelmään. Lokit on aikaleimattu, suojattu ja niitä säilytetään yrityksen vaatimusten mukaisesti.

Todentava näyttö: lokienhallintajärjestelmän asetukset, lokilähdeluettelo, NTP-asetukset, lokiotteet, säilytysasetukset, valvontaraportit.

15. Tarkastetaanko verkkolaitteiden hallintapalvelujen turvallisuus säännöllisesti?

Hyväksymiskriteeri: Yritys tarkastaa määräajoin käytössä olevat hallintapalvelut, avoimet portit, SNMP-versiot, käyttäjätilit, ohjelmistoversiot ja hallintayhteyksien rajaukset. Havaituille puutteille määritellään vastuuhenkilö, määräaika ja korjaava toimenpide.

Todentava näyttö: tarkastussuunnitelma, konfiguraatioauditoinnit, portti- ja haavoittuvuusskannaukset, poikkeamaraportit, korjaavien toimenpiteiden seuranta.

VERKKOKONFIGURAATIOIDEN JA MUUTOSTEN HALLINTA

Auditoinnin tavoite

Selvittää, suunnitellaanko, hyväksytäänkö, testataanko, toteutetaanko ja palautetaanko verkkokonfiguraatioiden muutokset hallitusti.

1. Onko verkkokonfiguraatioiden ja muutosten hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko hallittavat verkkolaitteet, konfiguraatiot, asetuspohjat, versiot ja riippuvuudet tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: CMDB, konfiguraatiorekisteri, asetuspohjat, riippuvuuskartat.

3. Onko muutosten riskinarviointi-, hyväksyntä-, testaus-, ajoitus- ja palautusvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: muutoshallintaohje, riskiluokitus, huoltoikkunat, hyväksymisrajat.

4. [KRIITTINEN] Varmistetaanko, että korkean riskin ja laajavaikutteiset verkkomuutokset hyväksytään erikseen ja toteutetaan valvotusti?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: muutospyynnöt, vaikutusarviot, hyväksymispäätökset, toteutussuunnitelmat.

5. Onko muutoksen tilaajat, arvioijat, hyväksyjät, toteuttajat ja valvojat määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: roolit, valtuusmatriisi, työjonot, tehtävien eriytys.

6. Varmistetaanko, että tuotantokonfiguraatioita muutetaan vain henkilökohtaisilla tunnuksilla hyväksytyn työjonon kautta?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: pääkäyttäjälokit, automaatiotunnukset, käyttöoikeudet, konfiguraatiotarkastukset.

7. Hallitaanko normaalit, kiireelliset, vakioidut ja automaattiset verkkomuutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutoskalenteri, testitulokset, toteutus- ja palautuslokit, jälkiarvioinnit.

8. Valvotaanko luvattomia muutoksia, konfiguraatiopoikkeamia, epäonnistumisia ja muutosten vaikutuksia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: konfiguraatiovalvonta, muutosauditoinnit, hälytykset, onnistumismittarit.

9. Käsitelläänkö epäonnistuneet muutokset, luvattomat asetukset ja muutoksista aiheutuneet häiriöt hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: häiriöraportit, luvattomien muutosten tutkinnat, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että konfiguraatioiden varmistus, palautus ja hätämuutoksen menettely testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: konfiguraatiovarmistukset, palautustestit, hätämuutosharjoitukset, raportit.

ULKOPUOLISTEN TIETOLIIKENNEYHTEYKSIEN HALLINTA

Auditoinnin tavoite

Selvittää, hyväksytäänkö, rajataanko, dokumentoidaanko ja valvotaanko kumppani-, pilvi-, toimittaja- ja asiakasyhteydet turvallisesti.

1. Onko ulkopuolisten tietoliikenneyhteyksien hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko ulkopuoliset yhteydet, vastapuolet, päätepisteet, tietovirrat, sopimukset ja omistajat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: yhteysrekisteri, kumppaniluettelo, tietovirtakuvat, päätepistetiedot.

3. Onko yhteyskohtaiset tunnistus-, salaus-, rajaus-, valvonta-, sopimus- ja päättämisvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: turvallisuusvaatimukset, sopimusehdot, riskiarviot, palvelutasot.

4. [KRIITTINEN] Varmistetaanko, että kriittiset kumppaniyhteydet erotetaan muusta verkosta ja niille määritellään valvottu katkaisumenettely?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: segmentointi, palomuurisäännöt, salausasetukset, katkaisusuunnitelmat.

5. Onko liiketoimintaomistajat, tekniset omistajat, tietoturvan hyväksyjät ja vastapuolten yhteyshenkilöt määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: omistaja- ja yhteyshenkilöluettelot, vastuumatriisi, hyväksymispäätökset.

6. Varmistetaanko, että yhteydet rajataan vain sovittuihin osoitteisiin, palveluihin, aikoihin ja tietovirtoihin?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: yhteyskonfiguraatiot, rajaukset, sertifikaatit, tekniset testit.

7. Hallitaanko uusien yhteyksien, päätepisteiden, sääntöjen, vastapuolten ja sopimusten muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, sopimusmuutokset, testitulokset, poistopäätökset.

8. Valvotaanko ulkopuolisten yhteyksien liikennettä, saatavuutta, poikkeamia ja käyttämättömyyttä säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: liikenne- ja saatavuusraportit, palomuurilokit, poikkeamahälytykset.

9. Käsitelläänkö luvattomat tietovirrat, vastapuolen vaarantuminen ja yhteyksien väärinkäyttö hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, vastapuoli-ilmoitukset, katkaisulokit, tutkintatiedot.

10. [KRIITTINEN] Varmistetaanko, että yhteyksien katkaisu, varayhteydet, vastapuoliviestintä ja palautuminen testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: katkaisu- ja varayhteystestit, yhteysharjoitukset, palautusraportit.

VERKKOPÄÄSYN HALLINTA

Auditoinnin tavoite

Selvittää, pääsevätkö verkkoon vain tunnistetut, hyväksytyt ja vaatimustenmukaiset käyttäjät, laitteet sekä palvelut.

1. Onko verkkopääsyn hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko verkkopääsyn käyttäjät, laitteet, palvelut, portit, tunnistuslähteet ja käyttöoikeusryhmät tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: NAC-rekisteri, laiteluettelo, käyttäjäryhmät, portti- ja SSID-tiedot.

3. Onko tunnistus-, valtuutus-, laitevaatimus-, vierailija-, karanteeni- ja lokitusvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: verkkopääsypolitiikka, laitevaatimukset, roolimalli, poikkeusmenettely.

4. [KRIITTINEN] Varmistetaanko, että tuntemattomat tai vaatimustenvastaiset laitteet estetään tai ohjataan erilliseen karanteeniverkkoon?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: NAC-säännöt, karanteeniprofiilit, 802.1X-asetukset, tekniset testit.

5. Onko käyttöoikeuksien tilaajat, hyväksyjät, identiteettien ylläpitäjät ja verkkovalvojat määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: käyttöoikeuspyynnöt, hyväksynnät, roolit, tehtävien eriytys.

6. Varmistetaanko, että vahvaa tunnistamista, sertifikaatteja, 802.1X-ratkaisuja ja vähimpiä oikeuksia käytetään?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: sertifikaatit, tunnistusasetukset, laiteprofiilit, vaatimustenmukaisuustarkastukset.

7. Hallitaanko verkkopääsyroolien, laiteprofiilien, tunnistuslähteiden ja poikkeusten muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, roolikatselmukset, poikkeusluvat, testitulokset.

8. Valvotaanko pääsypäätöksiä, epäonnistuneita tunnistuksia, tuntemattomia laitteita ja poikkeuksia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: NAC-lokit, RADIUS-lokit, laitehavainnot, epäonnistuneiden kirjautumisten raportit.

9. Käsitelläänkö luvattomat laitteet, tunnusten väärinkäyttö, virheelliset roolit ja NAC-häiriöt hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: poikkeamaraportit, estolokit, tunnusten sulkemiset, tutkintatiedot.

10. [KRIITTINEN] Varmistetaanko, että tunnistuspalvelun varajärjestelyt, karanteeni ja hätäkäyttö testataan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: varatunnistus-, karanteeni- ja palautustestit, harjoitusraportit.

TIETOLIIKENNEPOIKKEAMIEN HALLINTA

Auditoinnin tavoite

Selvittää, havaitaanko, luokitellaanko, rajataanko, tutkitaanko ja korjataanko tietoliikennepoikkeamat oikea-aikaisesti ja jäljitettävästi.

1. Onko tietoliikennepoikkeamien hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko poikkeamatyypit, havaintolähteet, yhteyshenkilöt, työkalut ja eskalointikanavat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: poikkeamaluettelo, hälytyslähteet, päivystyslista, yhteystiedot.

3. Onko luokittelu-, vasteaika-, ilmoitus-, tutkinta-, todistusaineisto- ja viestintävaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: poikkeamaohje, luokittelumalli, palvelutasot, ilmoitusvelvoitteet.

4. [KRIITTINEN] Varmistetaanko, että vakavat tietomurto-, tietovuoto- ja laajavaikutteiset verkkohäiriöt eskaloidaan välittömästi?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: vakavien tapausten raportit, eskalointilokit, johdon päätökset, ilmoitukset.

5. Onko poikkeaman johtaja, tekniset tutkijat, viestintä, johto ja ulkoiset osapuolet määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: vastuumatriisi, päivystyslista, kriisiorganisaatio, yhteystietorekisteri.

6. Varmistetaanko, että rajaamisessa huomioidaan liiketoimintavaikutus, todistusaineiston säilyminen ja turvallinen palautuminen?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: rajaamissuunnitelmat, tutkintalokit, aineiston käsittelyketju, palautuspäätökset.

7. Hallitaanko poikkeamaprosessin, yhteystietojen, luokittelun ja reagointiohjeiden muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: ohjeversiot, harjoitushavainnot, yhteystietotestit, hyväksymispäätökset.

8. Valvotaanko poikkeamien määriä, vasteaikoja, vakavuutta, toistuvuutta ja korjaustoimia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: poikkeamamittarit, vasteaikaraportit, trendit, toimenpideseuranta.

9. Käsitelläänkö luvattomat yhteydet, haitallinen liikenne, väärät määritykset ja tietoliikennehäiriöt hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: tapausraportit, liikennekaappaukset, lokit, juurisyyanalyysit, korjaustoimet.

10. [KRIITTINEN] Varmistetaanko, että poikkeamien reagointi-, viestintä-, eristys- ja palautumismenettelyt harjoitellaan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: harjoitusraportit, eristys- ja palautustestit, kehityssuunnitelmat.

TIETOLIIKENTEEN JATKUVUUDEN JA PALAUTUMISEN HALLINTA

Auditoinnin tavoite

Selvittää, onko kriittisten tietoliikenneyhteyksien ja verkkopalvelujen jatkuvuus, redundanssi ja palautuminen suunniteltu sekä testattu.

1. Onko tietoliikenteen jatkuvuuden ja palautumisen hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko kriittiset yhteydet, verkkolaitteet, palvelut, operaattorit, riippuvuudet ja varajärjestelyt tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: kriittisyysluettelo, riippuvuuskartat, operaattori- ja yhteysrekisteri, verkkokaaviot.

3. Onko saatavuus-, palautumisaika-, palautumispiste-, kapasiteetti- ja varayhteysvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: jatkuvuusvaatimukset, RTO/RPO-tavoitteet, palvelutasot, vaikutusanalyysit.

4. [KRIITTINEN] Varmistetaanko, että kriittisille yhteyksille ja verkkolaitteille on riippumattomat, dokumentoidut ja testatut varajärjestelyt?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: redundanssikaaviot, varayhteydet, reititystestit, hyväksymispäätökset.

5. Onko jatkuvuusomistajat, tekniset vastuuhenkilöt, operaattorit ja kriisijohto määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: jatkuvuusvastuut, yhteystietolistat, päivystysjärjestelyt, sopimukset.

6. Varmistetaanko, että redundanssi ei sisällä tunnistamattomia yhteisiä vikaantumispisteitä?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: yhteisten vikapisteiden analyysit, laite- ja reittierottelut, katselmukset.

7. Hallitaanko jatkuvuusratkaisujen, varayhteyksien, reitityksen ja palautussuunnitelmien muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, päivitetyt suunnitelmat, testitulokset, hyväksynnät.

8. Valvotaanko saatavuutta, katkoja, palautumisaikoja, varayhteyksien tilaa ja riippuvuuksia säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: saatavuusraportit, katkolokit, SLA-raportit, varayhteyshälytykset.

9. Käsitelläänkö yhteyskatkot, laiteviat, operaattorihäiriöt ja epäonnistuneet siirtymiset hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: häiriöraportit, operaattori-ilmoitukset, failover-lokit, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että failover-, palautus-, kriisiviestintä- ja vaihtoehtoisten työmenetelmien harjoitukset toteutetaan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: jatkuvuus- ja palautusharjoitukset, testiraportit, korjaavat toimenpiteet.

KAPASITEETIN JA SUORITUSKYVYN HALLINTA

Auditoinnin tavoite

Selvittää, seurataanko ja suunnitellaanko tietoliikenteen kapasiteettia sekä suorituskykyä niin, että häiriöt ja ylikuormitukset voidaan ennakoida.

1. Onko kapasiteetin ja suorituskyvyn hallinta dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko yhteydet, verkkolaitteet, palvelut, liikennemäärät, viiveet ja kapasiteettirajat tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: kapasiteettiluettelo, yhteysrekisteri, mittauspisteet, palveluomistajat.

3. Onko kapasiteetti-, viive-, käytettävyys-, kasvunvara- ja hälytysvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: kapasiteettitavoitteet, SLA:t, kasvuarviot, hälytysrajat, riskikriteerit.

4. [KRIITTINEN] Varmistetaanko, että kriittisille yhteyksille on määritelty mitatut kapasiteettirajat, hälytysrajat ja kasvunvara?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: kapasiteettiraportit, kuormitustestit, hälytysasetukset, investointipäätökset.

5. Onko kapasiteettiomistajat, palveluomistajat, verkkovalvonta ja hankintavastuut määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: vastuumatriisi, raportointivastuut, hankintasuunnitelmat, omistajaluettelo.

6. Varmistetaanko, että kapasiteettimittaus kattaa ruuhkahuiput, varayhteydet ja kriittiset riippuvuudet?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: valvontanäkymät, ruuhkahuippuraportit, varayhteysmittaukset, trendit.

7. Hallitaanko kapasiteetin, yhteysnopeuksien, palvelutasojen ja valvontarajojen muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: muutospyynnöt, kapasiteettipäätökset, päivitetyt rajat, testitulokset.

8. Valvotaanko käyttöastetta, viivettä, pakettihävikkiä, virheitä, saatavuutta ja trendejä säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: NMS-raportit, liikennegraafit, viive- ja pakettihävikkimittarit, SLA-raportit.

9. Käsitelläänkö ylikuormitukset, kapasiteettipuutteet, suorituskyvyn heikkeneminen ja mittauskatkot hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: häiriöraportit, ylikuormitusselvitykset, korjaustoimet, toimittajaraportit.

10. [KRIITTINEN] Varmistetaanko, että kuormitus-, failover- ja kapasiteetin palautumistestit toteutetaan?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: kuormitus- ja failover-testit, palautumismittaukset, harjoitusraportit.

TARKASTUKSET, TESTAUKSET JA JATKUVA KEHITTÄMINEN

Auditoinnin tavoite

Selvittää, arvioidaanko tietoliikenneturvallisuuden kontrollien toimivuutta säännöllisesti ja johdetaanko havainnoista korjaavia sekä ehkäiseviä toimenpiteitä.

1. Onko tarkastukset, testaukset ja jatkuva kehittäminen dokumentoitu, hyväksytty ja ajantasainen?

Hyväksymiskriteeri: Prosessin tarkoitus, laajuus, vaiheet, vastuut, hyväksynnät ja käytettävät järjestelmät on kuvattu ja ohje on henkilöstön saatavilla.

Todentava näyttö: prosessikuvaus, politiikka tai työohje, hyväksymispäätös, versionhallintatiedot.

2. Onko tarkastettavat verkot, yhteydet, laitteet, palvelut, kontrollit ja vastuuhenkilöt tunnistettu ja dokumentoitu?

Hyväksymiskriteeri: Kohteilla on yksilöivät tiedot, omistaja, kriittisyys, sijainti tai yhteys sekä ajantasainen elinkaaritieto.

Todentava näyttö: tarkastuskohdeluettelo, verkkokartat, kontrollirekisteri, vuosikello.

3. Onko auditointi-, tekninen testaus-, riippumattomuus-, otanta-, raportointi- ja korjausvaatimukset määritelty riskien ja liiketoiminnan tarpeiden perusteella?

Hyväksymiskriteeri: Vaatimukset ovat kirjallisia, mitattavia, kohteisiin sovellettavia ja säännöllisesti katselmoituja.

Todentava näyttö: auditointiohjelma, testausstandardit, otantaperusteet, raportointikriteerit.

4. [KRIITTINEN] Varmistetaanko, että kriittiset verkot ja internetrajapinnat testataan riskiperusteisesti riippumattomilla menetelmillä?

Hyväksymiskriteeri: Kriittinen kontrolli on toteutettu kaikissa soveltuvissa kohteissa, poikkeukset on riskinarvioitu ja hyväksytty määräajaksi.

Todentava näyttö: penetraatiotestit, konfiguraatioauditoinnit, haavoittuvuusskannaukset, hyväksynnät.

5. Onko auditointien tilaajat, testaajat, kohdeomistajat, hyväksyjät ja toimenpideomistajat määritelty ja eriytetty?

Hyväksymiskriteeri: Vastuut, valtuudet, tehtävien eriytys, varahenkilöt ja eskalointitiet on dokumentoitu ja viestitty.

Todentava näyttö: toimeksiannot, pätevyystiedot, riippumattomuusarviot, vastuumatriisi.

6. Varmistetaanko, että testit suunnitellaan niin, etteivät ne aiheuta hallitsematonta tuotantoriskiä tai tietovuotoa?

Hyväksymiskriteeri: Menettely toteutetaan hyväksytyillä teknisillä ratkaisuilla ja yhdenmukaisilla asetuksilla; poikkeamat dokumentoidaan.

Todentava näyttö: testisuunnitelmat, riskinarviot, luvat, valvonta- ja palautusjärjestelyt.

7. Hallitaanko tarkastusohjelman, testimenetelmien, kohteiden ja hyväksymiskriteerien muutokset järjestelmällisesti?

Hyväksymiskriteeri: Muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus, dokumentointi ja palautusmenettely käsitellään ennen käyttöönottoa.

Todentava näyttö: päivitetyt vuosiohjelmat, menetelmämuutokset, hyväksymispäätökset, versiohistoria.

8. Valvotaanko havaintojen vakavuutta, korjausaikoja, toistuvuutta, kattavuutta ja vaikuttavuutta säännöllisesti?

Hyväksymiskriteeri: Valvonnalle on määritelty kattavuus, hälytysrajat, vastuuhenkilöt, käsittelyajat ja raportointi; merkittävät havainnot eskaloidaan.

Todentava näyttö: havaintorekisteri, mittariraportit, kattavuusanalyysit, trendiraportit.

9. Käsitelläänkö kriittiset havainnot, epäonnistuneet testit, ylitetyt määräajat ja toistuvat puutteet hallitusti?

Hyväksymiskriteeri: Poikkeamat kirjataan, luokitellaan, rajataan, tutkitaan ja korjataan; merkittävistä tapauksista tehdään juurisyyanalyysi.

Todentava näyttö: kriittisten havaintojen eskaloinnit, poikkeuspäätökset, juurisyyanalyysit.

10. [KRIITTINEN] Varmistetaanko, että korjausten vaikuttavuus varmistetaan uusintatestauksilla ja johdon katselmuksilla?

Hyväksymiskriteeri: Jatkuvuus-, palautus- tai kehittämismenettelyllä on omistaja, tavoite, testausaikataulu ja havaintojen perusteella seurattavat toimenpiteet.

Todentava näyttö: uusintatestit, jälkiauditoinnit, johdon katselmukset, vaikuttavuusarviot.