SecMeter - TSAT Katakri security assessment tool

Katakri 2020 -itsearviointi (sisäinen turvallisuusarviointi)

Tämä lomake ohjaa yrityksen sisäisen Katakri 2020 -itsearvioinnin läpi kaikkien 61 vaatimuksen kautta (Turvallisuusjohtaminen T, Fyysinen turvallisuus F, Tekninen tietoturvallisuus I). Jokaisen vaatimuksen tarkastuskysymykset ja pyydettävä näyttö näkyvät suoraan sivulla vaatimuksen alla. Täytä ensin perustiedot alla, siirry sitten arviointisivuille pisteyttämään jokainen vaatimus, ja Yhteenveto- sekä Johdon raportti -sivut päivittyvät automaattisesti antamiesi arviointien perusteella. Vaaleanpunaiset kentät ovat lukittuja ja lasketaan automaattisesti.

Arvioitavan yrityksen nimi

Järjestelmä / kohde

Arvioijan nimi / rooli

Arviointipäivä (pp.kk.vvvv)

Tavoiteltava turvallisuusluokka (TL) -

Arvioinnin laajuus / kuvaus

Arviointiasteikko kaikilla vaatimuksilla on viisiportainen (1-5) kypsyystasoasteikko, joka mittaa kunkin vaatimuksen toteutumista kohdeorganisaatiossa (tai "Ei sovellu", jos vaatimus ei koske kohdetta). Taso 3 (Perustaso / Lakisääteinen) on minimitaso hyväksynnälle:

1 - Puutteellinen
2 - Osittainen
3 - Perustaso (Lakisääteinen)
4 - Hallittu ja valvottu
5 - Optimoitu

Huomio: lomake kattaa Katakri 2020 -kriteeristön 61 vaatimusta (Turvallisuusjohtaminen T-01-T-13, Fyysinen turvallisuus F-01-F-08.4, Tekninen tietoturvallisuus I-01-I-21), ja jokaisen vaatimuksen tarkastuskysymykset näkyvät suoraan arviointisivuilla. Kyseessä on yrityksen sisäiseen itsearviointiin tarkoitettu apuväline, ei virallinen viranomaisen suorittama Katakri-arviointi tai -todistus.

SecMeter - TSAT Katakri security assessment tool

Seuraava >

T - Turvallisuusjohtaminen (1/5) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

T-01 Johdon tuki, ohjaus ja vastuu - Turvallisuusperiaatteet

- Onko organisaatiolla ylimmän johdon hyväksymät, dokumentoidut turvallisuusperiaatteet?

- Kuvaavatko periaatteet, miten tietoturvallisuustoimenpiteet kytkeytyvät organisaation toimintaan?

- Miten tietoturvallisuustoimenpiteiden toteutumista seurataan ja raportoidaan johdolle?

- Miten organisaatio valvoo tiedonhallintaan liittyvien velvoitteiden ja ohjeiden noudattamista?

Pyydettävä näyttö: Turvallisuuspolitiikka-asiakirja, johdon hyväksyntämerkintä, raportointipöytäkirjat.

T-02 Turvallisuustyön tehtävien ja vastuiden määrittäminen

- Onko turvallisuusjohtamisen, fyysisen turvallisuuden ja teknisen tietoturvallisuuden vastuut ja tehtävät nimetty kirjallisesti?

- Onko organisaatiolla nimetty turvallisuusvastaava (FSO), jolla on riittävä osaaminen ja johdon nimitys?

- Onko tietoturvallisuusdokumentaation ylläpito ja ajantasaisuus vastuutettu?

Pyydettävä näyttö: Tehtävänkuvaukset, organisaatiokaavio, FSO-nimityspäätös.

T - Turvallisuusjohtaminen (2/5) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

T-03 Tietoturvallisuusriskien hallinta

- Onko organisaatiolla systemaattinen prosessi turvallisuusluokiteltuihin tietoihin kohdistuvien riskien tunnistamiseen, analysointiin ja arviointiin?

- Miten riskienhallinnan tuloksia hyödynnetään tietoturvallisuustoimenpiteiden suunnittelussa?

- Onko toimitusketjuihin liittyvät riskit (esim. laitteisto- ja ohjelmistotoimittajat) huomioitu?

- Onko sovelletut valvonta- ja turvatoimet sekä niiden perusteena oleva riskiarviointi dokumentoitu?
Pyydettävä näyttö: Riskiarviointidokumentti, riskirekisteri.

T-04 Turvallisuusohjeistus

- Onko organisaatiolla ajantasaiset ohjeet turvallisuusluokiteltujen tietojen käsittelystä, tietojärjestelmien käytöstä ja käsittelyoikeuksista?

- Kattavatko ohjeet koko tiedon elinkaaren (luonti, käsittely, säilytys, hävittäminen)?

- Miten ohjeiden ajantasaisuudesta ja saatavuudesta huolehditaan?
Pyydettävä näyttö: Turvallisuusohjeet ja niiden versiohistoria.

T-05 Turvallisuustyön resurssit

- Onko turvallisuustehtäviä hoitavilla henkilöillä riittävä ja osoitettava asiantuntemus?

- Arvioidaanko turvallisuustyön resurssien riittävyyttä säännöllisesti?
Pyydettävä näyttö: Koulutustodistukset, resurssisuunnitelma.

T - Turvallisuusjohtaminen (3/5) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

T-06 Toimintahäiriöt ja poikkeustilanteet

- Onko organisaatio tunnistanut turvallisuusluokiteltujen tietojen suojaamisen kannalta kriittiset hätä- ja häiriötilanteet?

- Onko käytössä ennalta ehkäiseviä ja korjaavia toimenpiteitä tietojen suojaamiseksi näissä tilanteissa?

- Onko avainhenkilöiden estyneisyyden varalle varmistettu kyky jatkaa tietojen suojaamista?

Pyydettävä näyttö: Jatkuvuussuunnitelma, häiriötilanneohje.

T-07 Turvallisuuspoikkeamien hallinta

- Onko käytössä ohjeistus ja menettely, jolla poikkeamasta saadaan tieto välittömästi organisaation sisällä?

- Onko määritelty, miten ja kenelle poikkeamista tai niiden epäilyistä ilmoitetaan?

- Tiedetäänkö, mitkä poikkeamat edellyttävät ilmoitusta toimivaltaiselle turvallisuusviranomaiselle?

- Onko poikkeamienhallintaprosessi suunniteltu, koulutettu ja harjoiteltu?

Pyydettävä näyttö: Poikkeamanhallintaohje, harjoitusraportit, ilmoituslokit.

T - Turvallisuusjohtaminen (4/5) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

T-08 Tietojen luokittelu (koskee vain viranomaisen tiedonhallintaa)

- Onko organisaatiolla ohje tietojen luokitteluun?

- Merkitäänkö turvallisuusluokiteltavat asiakirjat, ml. luonnokset, turvallisuusluokkaa kuvaavalla merkinnällä?

- Merkitäänkö asiakirja sen osien (esim. liitteet) ylimmän turvallisuusluokan mukaisesti?

Pyydettävä näyttö: Luokitteluohje, esimerkkiasiakirjat.

T-09 Työsuhteen aikaiset muutokset turvallisuusluokiteltujen tietojen käsittelyssä

- Onko rekrytoinnin, tehtävänmuutosten ja työsuhteen päättymisen yhteydessä käytössä menettelyt käsittelyoikeuksien hallintaan?

- Palautetaanko avaimet, tunnukset ja aineistot työsuhteen päättyessä, ja poistetaanko käyttöoikeudet?

- Muistutetaanko työsuhteen päättyessä salassapito- ja vaitiolovelvollisuudesta?

Pyydettävä näyttö: Rekrytointi-, perehdytys- ja lähtöohjeet sekä tarkastuslistat.

T-10 Henkilöstön luotettavuuden arviointi

- Selvitetäänkö turvallisuusluokiteltua tietoa käsittelevien henkilöiden luotettavuus tarvittaessa henkilöturvallisuusselvityksellä?

- Onko varmistettu, että TL III (CONFIDENTIAL) tai korkeampaa kansainvälistä tietoa käsittelevillä on voimassa oleva henkilöturvallisuusselvitystodistus (PSC) tarvittaessa?

Pyydettävä näyttö: Turvallisuusselvityspäätökset, PSC-todistukset (käsitellään luottamuksellisesti tarkastuksessa).

T - Turvallisuusjohtaminen (5/5) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

T-11 Salassapito- ja vaitiolovelvollisuus

- Onko turvallisuusluokiteltua tietoa käsitteleville selvitetty tietojen suojaamista koskevat periaatteet ja toimenpiteet?

- Onko henkilö antanut vakuutuksen tietojen suojaamista koskevasta vastuustaan, erityisesti jos virkavastuu ei koske häntä?

Pyydettävä näyttö: Salassapitositoumukset, vakuutuslomakkeet.

T-12 Turvallisuuskoulutus

- Onko henkilöstölle tarjolla säännöllistä koulutusta tiedonhallintaa, tietojenkäsittelyä ja salassapitoa koskevista säädöksistä ja ohjeista?

- Koulutetaanko turvallisuusluokiteltuun tietoon kohdistuvat keskeiset uhat ja ajantasaiset ohjeet?

- Pidetäänkö kirjaa koulutuksiin osallistumisesta?

Pyydettävä näyttö: Koulutussuunnitelma, osallistujalistat.

T-13 Tiedonsaantitarve ja käsittely-oikeudet

- Pidetäänkö ajantasaista luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan II tai III tietoja, ja mainitaanko peruste?

- Myönnetäänkö pääsy turvallisuusluokiteltuun tietoon vasta, kun tiedonsaantitarve on selvitetty?

- Onko käytössä menettely käsittelyoikeuksien poistamiseksi tiedonsaantitarpeen päätyttyä?

Pyydettävä näyttö: Käyttöoikeusrekisteri, poistoseloste.

F - Fyysinen turvallisuus (1/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-01 Fyysisten turvatoimien tavoite

- Estävätkö fyysiset turvatoimet luvattoman pääsyn turvallisuusluokiteltuihin tietoihin (ehkäisy, esto, havaitseminen, viivytys)?

Pyydettävä näyttö: Turvasuunnitelma / turva-aluekuvaus.

F-02 Riskien arviointi

- Onko tietojenkäsittelyyn kohdistuvat olennaiset riskit selvitetty ja fyysiset turvatoimet mitoitettu riskiarvion mukaisesti?

- Onko riskiarvioinnissa huomioitu turvallisuusluokka, käsittelymäärä, säilytysaika, sijainti, vasteaika, ulkoistetut palvelut ja uhka-arvio?

- Perustuuko kansainvälisen tiedon fyysisten turvatoimien valinta Suojelupoliisin tai Pääesikunnan uhka-arvioon?

Pyydettävä näyttö: Riskiarviointidokumentti, uhka-arvio.

F-03 Fyysisten turvatoimien valinta (monitasoinen suojaus)

- Onko käytössä ennaltaehkäiseviä, estäviä, havaitsevia ja tilanteen palauttavia toimenpiteitä turvallisuusalueilla?

- Onko monitasoinen suojaus toteutettu yhdistelmällä rakenteellisia esteitä, kulunvalvontaa, tunkeutumisen ilmaisua, vartiointia, kameravalvontaa, valaistusta ja hallinnollisia menettelyjä?

- Tarkastetaanko ja huolletaanko laitteet säännöllisin väliajoin?

Pyydettävä näyttö: Turva-aluesuunnitelma, huoltolokit.

F - Fyysinen turvallisuus (2/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-04 Tiedon käsittely ja säilytys turvallisuusalueilla ja niiden ulkopuolella

- Käsitelläänkö turvallisuusluokiteltua tietoa siten, että pääsy on suojattu sivullisilta sekä alueilla että niiden ulkopuolella?

- Noudatetaanko lisäehtoja tiedon säilyttämiseen turvallisuusalueiden ulkopuolella (esim. valvottu tila, lukittu kaluste, turvapussi)?

Pyydettävä näyttö: Käsittelyohje.

F-05.1 Hallinnollinen alue - alueen raja ja rakenteet

- Onko alueella selkeästi määritelty näkyvä raja?

- Onko rakenteita vahvennettu, jos murtoriski arvioidaan todennäköiseksi?

- Ovatko käyttämättömät aukot lukittavissa tai suljettavissa kulun hallitsemiseksi?

Pyydettävä näyttö: Pohjapiirustus, rakenneselvitys.

F-05.2 Hallinnollinen alue - pääsyoikeuksien myöntäminen

- Onko itsenäinen pääsy alueelle vain asianmukaisesti valtuutetuilla henkilöillä?

- Onko pääsyoikeuksien ja avainhallinnan menettelyt ja roolit määritelty, dokumentoitu ja ohjeistettu?

- Tarkastetaanko pääsyoikeudet säännöllisesti ja pidetäänkö ne ajan tasalla?

Pyydettävä näyttö: Pääsyoikeusluettelo, avainten hallintaohje.

SecMeter - TSAT Katakri security assessment tool

< Edellinen Seuraava >

F - Fyysinen turvallisuus (3/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-05.3 Hallinnollinen alue - vierailijat

- Onko vierailijoilla aina saattaja? -

- Onko organisaatiolla hyväksytty vierailijaohje (tunnistaminen, kirjaaminen, valvonta)? -
Pyydettävä näyttö: Vierailijaohje, vierailulokit.

F-05.4 Hallinnollinen alue - äänieristys

- Estääkö alueen äänieristys asiaan kuulumattomia kuulemasta turvallisuusluokiteltuun tietoon liittyviä keskusteluja selväsanaisena? -
Pyydettävä näyttö: Äänieristysarviointi tai -mittaus.

F-05.5 Hallinnollinen alue - tunkeutumisen ilmaisujärjestelmät

- Onko aluetta tai sen säilytysyksiköitä varustettu tunkeutumisen ilmaisujärjestelmällä, jos murtoriski arvioidaan todennäköiseksi? -
Pyydettävä näyttö: Hälytysjärjestelmädokumentaatio.

F-05.6 Hallinnollinen alue - salaa katselun estäminen

- Onko käytössä toimenpiteitä (sijoittelu, näkösuojat, kaihtimet) salaa katselun riskin torjumiseksi, myös vahingossa tapahtuvan? -
Pyydettävä näyttö: Tilakatselmus.

F - Fyysinen turvallisuus (4/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-05.7 Hallinnollinen alue - tila- ja laitetarkastukset (vain TL II)

- Tarkastetaanko elektroniset laitteet ennen käyttöä TL II -alueella, jos tietoihin kohdistuva uhka arvioidaan korkeaksi?

- Tarkastetaanko alue fyysisesti tai teknisesti säännöllisin väliajoin, sekä epäillyn luvattoman pääsyn jälkeen?

Pyydettävä näyttö: Tarkastuspöytäkirjat.

F-05.8 Hallinnollinen alue - tiedon käsittely ja säilyttäminen

- Säilytetäänkö TL IV -tieto soveltuvassa lukitussa toimistokalusteessa?

- Onko TL III -tiedon säilytys päätelaitteessa toteutettu vaatimusten mukaisesti (valvottu tila tai turvapussi)?

- Vaihdetaanko säilytysyksiköiden numeroyhdistelmät tarvittaessa (henkilöstömuutos, vaarantumisepäily, huolto)?

Pyydettävä näyttö: Säilytysyksikköluettelo, koodinvaihtoloki.

F-06.1 Turva-alue - alueen raja ja rakenteet

- Onko alueella selkeä näkyvä raja?

- Täyttävätkö seinät, lattia, katto, ikkunat ja ovet tietojen säilytyksen edellyttämän turvallisuustason (esim. RC3), jos erillistä säilytysratkaisua ei ole?

- Onko hätäpoistumistiet järjestetty niin, etteivät ne tarpeettomasti vaaranna turva-aluetta?

Pyydettävä näyttö: Rakenneselvitys, RC-luokitustodistus.

F - Fyysinen turvallisuus (5/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-06.2 Turva-alue - kulunvalvonta

- Valvotaanko kaikkea kulkua alueen rajalla kulkulupien tai henkilökohtaisen tunnistamisen avulla?

- Onko kulkuoikeudet myöntävä vastuuhenkilö nimetty, ja katselmoidaanko oikeudet säännöllisesti (esim. 6 kk välein)?
Pyydettävä näyttö: Kulunvalvontarekisteri, katselmointipöytäkirjat.

F-06.3 Turva-alue - pääsyoikeuksien myöntäminen

- Myönnetäänkö itsenäinen pääsyoikeus vain luotettavuudeltaan varmistetulle henkilölle, jolla on erityinen lupa alueelle?

- Edellyttääkö kansainvälisen tiedon käsittely alueella voimassaolevaa henkilöturvallisuusselvitystodistusta (PSC)?
Pyydettävä näyttö: Pääsyoikeuspäätökset.

F-06.4 Turva-alue - vierailijat

- Onko vierailijoilla aina saattaja?

- Onko alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka ilmoitettu selkeästi, jos alueelle tulo merkitsee välitöntä pääsyä tietoihin?

- Onko vierailijoiden luotettavuus varmistettu asianmukaisesti, ellei ole varmistettu, ettei heillä ole pääsyä turvallisuusluokiteltuun tietoon?
Pyydettävä näyttö: Vierailijaohje, ennakkoilmoitusmenettely.

F - Fyysinen turvallisuus (6/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-06.5 Turva-alue - turvallisuusohjeet

- Onko kullekin turva-alueelle laadittu turvallisuusmenettelyt (tiedon säilytys, valvonta- ja suojatoimet, pääsyoikeudet, vierailijat)?

- Tarkastetaanko ohjeiden ajantasaisuus ja jalkautuminen säännöllisesti, vähintään vuosittain?
Pyydettävä näyttö: Turvaohje, tarkastuspöytäkirjat.

F-06.6 Turva-alue - äänieristys

- Estääkö äänieristys turvallisuusluokitellun tiedon kuulemisen alueen ulkopuolelta?
Pyydettävä näyttö: Äänieristysarviointi.

F-06.7 Turva-alue - tunkeutumisen ilmaisujärjestelmät

- Onko alue, jolla ei ole ympärivuorokautista henkilöstöä, tarkastettu työajan päätteeksi/satunnaisesti, tai varustettu murtohälytysjärjestelmällä?

- Testataanko ilmoituksensiirto ja vasteaika säännöllisesti (esim. 1x/kk ja 1x/v) ja dokumentoidaanko testaus?
Pyydettävä näyttö: Testauspöytäkirjat.

F-06.8 Turva-alue - salaa katselun estäminen

- Onko käytössä toimenpiteitä salaa katselun riskin torjumiseksi, myös vahingossa tapahtuvan?
Pyydettävä näyttö: Tilakatselmus.

F - Fyysinen turvallisuus (7/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-06.9 Turva-alue - tila- ja laitetarkastukset (vain TL II)

- Tarkastetaanko elektroniset laitteet ja alue säännöllisesti TL II -turva-alueella, jos uhka arvioidaan korkeaksi?

Pyydettävä näyttö: Tarkastuspöytäkirjat.

F-06.10 Turva-alue - tiedon käsittely ja säilyttäminen

- Säilytetäänkö turvallisuusluokan III ja korkeamman tiedot soveltuvaksi arvioidussa säilytysratkaisussa?

- Vaihdetaanko säilytysyksikön numeroyhdistelmät tarvittaessa (henkilöstömuutos, huolto, vaarantumisepäily)?

Pyydettävä näyttö: Säilytysratkaisudokumentaatio.

F-07 Teknisesti suojattu turva-alue

- Onko alueella tunkeutumisen ilmaisujärjestelmä, ja pidetäänkö alue lukittuna kun sitä ei käytetä sekä vartioituna kun se on käytössä?

- Valvotaanko kaikkien henkilöiden kulkua ja materiaalien tuontia alueelle?

- Onko alueella vain kyseiselle alueelle hyväksyttyjä tietoliikenneyhteyksiä, puhelimia ja muita elektronisia laitteita?

Pyydettävä näyttö: Hyväksyttyjen laitteiden luettelo, tarkastuspöytäkirjat.

F - Fyysinen turvallisuus (8/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-08.1 Tietojen välitys postilla ja kuriirilla

- Pakataanko turvallisuusluokiteltu tieto niin, ettei pakkaus paljasta sisältöä, ja kuljetetaanko se turvallisuusluokan edellyttämällä valvonnalla?

- Käytetäänkö sähköisten tietovälineiden kuljetuksessa turvallisuusluokalle hyväksyttyä salausta?
Pyydettävä näyttö: Kuljetusohje, lähetysrekisteri.

F-08.2 Turvallisuusluokiteltujen tietojen kopioiminen

- Sovelletaanko kopioihin ja käännöksiin samoja turvatoimia kuin alkuperäiseen tietoon?

- Luetteloidaanko turvallisuusluokan II tietojen kopiot ja niiden käsittelijät, ja hankitaanko kopiointilupa tiedon laatijalta?
Pyydettävä näyttö: Kopiointiloki / -rekisteri.

F-08.3 Turvallisuusluokiteltujen tietojen kirjaaminen

- Onko kansainvälistä turvallisuusluokiteltua tietoa käsittelevällä organisaatiolla nimetty kirjaamo, joka on määritetty turva-alueeksi?

- Kirjataanko kansallisten turvallisuusluokkien II-III ja kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tai korkeamman tiedon vastaanotto ja lähetys?
Pyydettävä näyttö: Kirjaamorekisteri.

F - Fyysinen turvallisuus (9/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

F-08.4 Ei-sähköisten tietojen tuhoaminen

- Onko tuhoaminen järjestetty luotettavasti niin, ettei tietoja voida koota uudelleen kokonaan tai osittain? -

- Allekirjoitetaanko kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tiedon tuhoamisesta todistus, joka säilytetään vähintään viisi vuotta? -

- Suorittaako tuhoamisen turvallisuusluokan II tiedoille vain siihen erikseen määrätty henkilö?
Pyydettävä näyttö: Tuhoamistodistukset, silppuamisohje.

SecMeter - TSAT Katakri security assessment tool

< Edellinen Seuraava >

I - Tekninen tietoturvallisuus (1/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-01 Verkon rakenteellinen turvallisuus

- Onko tietojenkäsittely-ympäristö erotettu muista ympäristöistä (vähintään palomuuriratkaisu TL IV:llä)?

- Salataanko hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne toimivaltaisen viranomaisen hyväksymällä ratkaisulla?

- Edellyttääkö kytkentä muiden turvallisuusluokkien ympäristöihin toimivaltaisen viranomaisen hyväksymää yhdyskäytäväratkaisua (TL III-II)?

Pyydettävä näyttö: Verkkokaavio, palomuurisäännöstöt.

I-02 Verkon vyöhykkeistäminen ja suodatussäännöstöt

- Onko tietoliikenneverkko jaettu turvallisuusluokan sisällä erillisiin vyöhykkeisiin/segmentteihin?

- Sallitaanko vyöhykkeiden välillä vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti (default-deny)?

- Onko tietojenkäsittely-ympäristössä varauduttu yleisiin verkkohyökkäyksiin?

Pyydettävä näyttö: Verkkosegmentointidokumentaatio, palomuurisäännöt.

I-03 Suodatus- ja valvontajärjestelmien hallinnointi

- Onko liikennettä suodattavien/valvovien järjestelmien asetusten muutokset vastuutettu ja organisoitu?

- Ylläpidetäänkö verkon ja suodatusjärjestelmien dokumentaatiota osana muutostenhallintaprosessia?

- Tarkastetaanko asetukset ja toiminta määräajoin sekä poikkeuksellisten tilanteiden jälkeen?

Pyydettävä näyttö: Verkkodokumentaatio, tarkastuspöytäkirjat.

I - Tekninen tietoturvallisuus (2/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-04 Hallintayhteydet

- Onko hallintayhteydet rajattu turvallisuusluokittain, ellei käytössä ole hyväksyttyä yhdyskäytäväratkaisua?

- Salataanko turvallisuusluokiteltua tietoa sisältävä hallintaliikenne, kun se kulkee matalamman turvallisuusluokan ympäristön kautta?

- Onko hallintayhteydet rajattu vähimpien oikeuksien periaatteen mukaisesti vain hyväksytyistä lähteistä?

Pyydettävä näyttö: Hallintaverkkokaavio, pääsyoikeusluettelo.

I-05 Langaton tiedonsiirto

- Salataanko langaton tiedonsiirto (esim. WLAN, matkaviestinverkot, Bluetooth) toimivaltaisen viranomaisen hyväksymällä salausratkaisulla?

Pyydettävä näyttö: WLAN-konfiguraatio, salausdokumentaatio.

I-06 Pääsyoikeuksien hallinnointi

- Onko tietojärjestelmien käyttöoikeudet määritelty ja myönnetäänkö ne vain käsittelyoikeuden omaaville henkilöille?

- Noudatetaanko vähimpien oikeuksien periaatetta sekä käyttäjille että automaattisille prosesseille?

- Pidetäänkö käyttöoikeudet ajantasaisina ja katselmoidaanko ne säännöllisesti (esim. 6 kk välein)?

- Onko tehtävien eriyttäminen toteutettu turvallisuusluokissa III-II?

Pyydettävä näyttö: Käyttöoikeusrekisteri, katselmointipöytäkirjat.

SecMeter - TSAT Katakri security assessment tool

< Edellinen Seuraava >

I - Tekninen tietoturvallisuus (3/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-07 Tietojenkäsittely-ympäristön toimijoiden tunnistaminen

- Onko käytössä yksilölliset henkilökohtaiset käyttäjätunnisteet sekä luotettava tunnistus ja todennus?

- Lukittuuko tunnus liian monen peräkkäisen epäonnistuneen kirjautumisyrityksen jälkeen?

- Käytetäänkö turvallisuusluokissa III-II vähintään kahteen tekijään perustuvaa tunnistusta?

- Käytetäänkö turvallisuusluokitellun tiedon käsittelyyn vain organisaation hyväksymiä ja hallinnoimia päätelaitteita?
Pyydettävä näyttö: Tunnistuspolitiikka, konfiguraatiodokumentaatio.

I-08 Järjestelmäkovennus

- Onko käyttöön otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut?

- Onko käytössä dokumentoitu menettelytapa, jolla järjestelmät asennetaan kovennettuina?

- Varmistetaanko kovennusten pysyminen voimassa koko elinkaaren ajan, erityisesti päivitysten jälkeen?
Pyydettävä näyttö: Kovennusohjeet, tarkastuslokit.

SecMeter - TSAT Katakri security assessment tool

< Edellinen Seuraava >

I - Tekninen tietoturvallisuus (4/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-09 Haittaohjelmasuojaus

- Onko haittaohjelmasuojaus asennettu järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille?

- Ovatko torjuntaohjelmistot toimintakykyisiä, ajan tasalla, ja tuottavatko ne lokitietoja ja hälytyksiä?

- Seurataanko haittaohjelmahavaintoja ja hälytyksiä säännöllisesti, ja reagoidaanko niihin?

Pyydettävä näyttö: Haittaohjelmasuojauksen tilaraportit.

I-10 Turvallisuuteen liittyvien tapahtumien jäljitettävyys

- Kerätäänkö riittävät lokitiedot tietojärjestelmien käytöstä ja tietojen luovutuksista?

- Onko käytössä kirjallinen lokien keräys-, luovutus-, hälytys- ja seurantapolitiikka?

- Säilytetäänkö keskeiset lokitiedot vaaditun ajan (esim. vähintään 6 kk, tai 5 vuotta turvallisuusluokasta riippuen)?

- Onko lokitiedot ja niiden kirjauspalvelut suojattu luvattomalta pääsyltä?

Pyydettävä näyttö: Lokipolitiikka, säilytysaikataulukko.

SecMeter - TSAT Katakri security assessment tool

< Edellinen Seuraava >

I - Tekninen tietoturvallisuus (5/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-11 Poikkeamien havainnointikyky ja toipuminen

- Tunnetaanko verkkoliikenteen normaali tila, ja onko menettely poikkeavien tapahtumien havaitsemiseksi?

- Onko menettely, jolla kerätyistä lokeista ja tilannetiedosta pyritään havaitsemaan poikkeamia?

- Onko olemassa menettely havaituista poikkeamista toipumiseen?

Pyydettävä näyttö: Havainnointimenettelydokumentaatio, harjoitusraportit.

I-12 Salausratkaisut

- Onko käytetyt salausratkaisut toimivaltaisen viranomaisen hyväksymiä kyseiselle turvallisuusluokalle ja käyttöympäristölle?

- Ovatko salausavainten hallintaprosessit (jakelu, säilytys, vaihto, valtuuttamattomien vaihtojen esto) dokumentoituja ja asianmukaisesti toteutettuja?

- Onko salausratkaisun toimitusketjun turvallisuudesta varmistuttu?

Pyydettävä näyttö: Hyväksyntäpäätökset, avainhallintaohje.

I - Tekninen tietoturvallisuus (6/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-13 Ohjelmistojen suojaaminen verkkohyökkäyksiltä

- Testataanko tietojenkäsittely-ympäristön tekniset ja muut turvatoimet hyväksymisprosessin aikana?

- Onko ohjelmistojen turvallisuustarpeet arvioitu käyttötarkoituksen, hyökkäyspinta-alan ja käsiteltävän tiedon turvallisuusluokan perusteella?

- Huomioidaanko lainsäädännöstä johdetut vaatimukset (salaus, hallintaliittymät, käyttäjähallinta, kovennukset, jäljitettävyys) ohjelmistotototeutuksissa?
Pyydettävä näyttö: Turvallisuustestausraportit.

I-14 Hajasäteily (TEMPEST) ja elektroninen tiedustelu

- Onko TEMPEST-turvatoimet toteutettu toimivaltaisen viranomaisen hyväksymillä menetelmillä (turvallisuusluokat III-II)?

- Onko elektronisen tiedustelun riskejä pienennetty riittävästi turvallisuusluokkien III-II tiedon sähköisessä käsittelyssä?
Pyydettävä näyttö: NTA:n hyväksyntä, mittausraportit.

I-15 Turvallisuusluokiteltujen tietojen sähköinen välitys

- Salataanko turvallisuusluokiteltu tieto/tietoliikenne hyväksytyllä menetelmällä siirrettäessä turvallisuusalueiden ulkopuolella?

- Varmistetaanko tai tunnistetaanko vastaanottaja riittävän tietoturvallisella tavalla ennen tietojen luovuttamista?
Pyydettävä näyttö: Salausratkaisudokumentaatio.

I - Tekninen tietoturvallisuus (7/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-16 Muutoshallintamenettelyt

-

- Onko tietojenkäsittely-ympäristön kokoonpanosta ajantasainen kirjanpito (laitteisto, ohjelmisto, konfiguraatiot)?

-

- Onko käytössä muutostenhallintamenettely, jonka avulla muutokset ovat jäljitettävissä?

- Tarkkaillaanko tietojenkäsittely-ympäristöä luvattomien muutosten tai laitteiden havaitsemiseksi?

Pyydettävä näyttö: Konfiguraationhallintarekisteri, muutoslokit.

I-17 Sähköisessä muodossa olevien tietojen fyysinen turvallisuus

-

- Käsitelläänkö ja säilytetäänkö tietoa vain toimivaltaisen viranomaisen hyväksymillä turvallisuusalueilla tai hyväksytyillä korvaavilla menettelyillä?

-

- Onko turvallisuusluokan IV tietoja sisältävät tietovarannot ja järjestelmät sijoitettu hyväksytylle turvallisuusalueelle?

- Onko päätelaitteen eheydestä huolehdittu hyväksytyllä menetelmällä, jos turvallisuusluokan III tietoa säilytetään turva-alueen ulkopuolella?

Pyydettävä näyttö: Sijoituskaavio, päätelaiteluettelo.

SecMeter - TSAT Katakri security assessment tool

< Edellinen Seuraava >

I - Tekninen tietoturvallisuus (8/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-18 Etäkäyttö ja etähallinta

- Tunnistetaanko käyttäjät ja päätelaitteet riittävän luotettavasti etäkäytössä ja -hallinnassa?

- Edellyttääkö etäkäyttö/-hallinta vähintään kahteen tekijään perustuvaa käyttäjätunnistusta?

- Onko turvallisuusluokkien III-II järjestelmien etähallinta rajattu toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle?

- Onko henkilöstö koulutettu ja ohjeistettu turvalliseen etäkäyttöön ja -hallintaan?

Pyydettävä näyttö: Etäkäyttöpolitiikka, koulutusmateriaali.

I-19 Ohjelmistohaavoittuvuuksien hallinta

- Seurataanko aktiivisesti viranomaisten ja valmistajien tietoturvatiedotteita, ja asennetaanko turvapäivitykset hallitusti?

- Tarkastellaanko päivitysten asentumisen onnistumista säännöllisesti, esim. kuukausittain?

- Skannataanko verkko ja järjestelmät haavoittuvuuksien varalta säännöllisesti (esim. vuosittain tai puolivuosittain) ja aina merkittävien muutosten jälkeen?

- Onko löydettyjen haavoittuvuuksien ja päivityspuutteiden käsittelyprosessi määritelty?

Pyydettävä näyttö: Haavoittuvuusskannausraportit, päivityslokit.

I - Tekninen tietoturvallisuus (9/9) - valitse arviointitulos jokaiselle vaatimukselle

Arviointitulos
Näytön valmiusaste

I-20 Varmuuskopiointi

- Suojataanko turvallisuusluokiteltua tietoa sisältävät varmuuskopiot vähintään vastaavalla tasolla kuin alkuperäinen tieto?

- Onko varmistusten taajuus (RPO) ja palautusprosessin nopeus (RTO) mitoitettu toimintavaatimuksiin?

- Testataanko varmuuskopioinnin ja palautusprosessin toimivuus säännöllisesti?

- Onko varmuuskopioiden fyysinen sijainti riittävän eriytetty alkuperäisestä järjestelmästä?

Pyydettävä näyttö: Varmuuskopiointipolitiikka, palautustestausraportit.

I-21 Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen

- Onko sähköisten tietojen tuhoaminen järjestetty luotettavasti (esim. ylikirjoitus, silppuaminen, sulattaminen) niin, ettei tietoja voi koota uudelleen?

- Allekirjoitetaanko kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tiedon tuhoamisesta todistus, joka säilytetään vähintään viisi vuotta?

- Suorittaako tuhoamisen turvallisuusluokan II tiedoille vain siihen erikseen määrätty henkilö?

Pyydettävä näyttö: Tuhoamistodistukset, ylikirjoitusohje.

SecMeter - TSAT Katakri security assessment tool

Automaattinen yhteenveto (päivittyy kaikkien 61 vaatimuksen arvioinnin mukaan)

Osa-alue	Kohteita	Arvioitu	Keskiarvo (1-5)
T - Turvallisuusjohtaminen (13)			
F - Fyysinen turvallisuus (27)			
I - Tekninen tietoturvallisuus (21)			

Kokonaistilanne:	
Kokonaisarvio:	
Näytön valmius:	

SecMeter - TSAT Katakri security assessment tool

Johdon raportti (automaattisesti generoitu yhteenveto itsearvioinnin tuloksista)