
Tunne huominen.
XAMK
Kaakkois-Suomen
ammattikorkeakoulu

Digitaalisen Turvallisuuden Kontrollit

Kaakkois-Suomen ammattikorkeakoulu
South-Eastern Finland University of Applied Sciences

www.xamk.fi

Kaakkois-Suomen ammattikorkeakoulu

Digitaalisen turvallisuuden kontrollit (mekanismit)

Digitaalisen turvallisuuden kontrollit voidaan jakaa kolmeen päätyyppiin: **teknisiin, hallinnollisiin ja fyysisiin** kontrollimekanismeihin. Näitä käytetään yhdessä riskienhallinnan tukemiseksi ja riskien vähentämiseksi hyväksyttävälle tasolle.

Tekniset kontrollit

Tekniset kontrollit ovat ratkaisevia digitaalisen turvallisuuden takaamisessa, sillä ne muodostavat ensisijaisen suojauksen tietojärjestelmille ja -varoille. Ne ovat työkaluja ja mekanismeja, jotka estävät uhkia, havaitsevat haitallista toimintaa ja mahdollistavat turvallisuuteen liittyvien vaatimusten toteuttamisen.

Tunnistautuminen ja pääsynhallinta

Tunnistautumisen ja pääsynhallinnan avulla rajoitetaan tietojen ja järjestelmien käyttö vain oikeutetuille käyttäjille.

Keskeisiä mekanismeja:

- **Salasanat ja PIN-koodit:** Perinteinen tapa tunnistaa käyttäjä. Salasanojen vahvuutta voidaan parantaa käyttämällä salasanapolitiikkoja.

- **Monivaiheinen tunnistautuminen (MFA):** Yhdistää useita tunnistautumistapoja, kuten salasanan ja kertakäyttöisen koodin, lisäämään turvallisuutta.

- **Biometriset tunnisteet:** Sormenjäljet, kasvotunnistus tai iiriksen skannaus.

- **Pääsynvalvontajärjestelmät (Access Control):** Määrittävät, mitä tietoja tai järjestelmiä käyttäjä voi käyttää (esim. roolipohjainen pääsynhallinta, RBAC).

Tietojen salaaminen

Salaus suojaa tietoja niiden siirron, tallennuksen ja käytön aikana.

Salausmenetelmiä:

- **Symmetrinen salaus:** Sama avain salauksen ja purkamisen välillä (esim. AES).
- **Epäsymmetrinen salaus:** Julkisen ja yksityisen avaimen yhdistelmä (esim. RSA).
- **TLS/SSL:** Suojaa tietoliikennettä verkkoyhteyksissä (esim. HTTPS).
- **Tietokannan salaus:** Tietokannan tietojen salaaminen hyödyntäen algoritmeja.
- **Levyn salaus:** Kokonaisen levyaseman (esim. BitLocker) tai yksittäisten tiedostojen salaus.

Käyttökohteita: Sähköpostien, verkkosivustojen ja arkaluonteisten tiedostojen suojaaminen.

Verkkoturvallisuuden työkalut

Verkkoturvallisuuden kontrollit suojaavat verkon infrastruktuuria ja tietoliikennettä.

Työkaluja:

- **Palomuurit:** Estävät luvattoman liikenteen verkon ja ulkomaailman välillä.
- **IDS/IPS:** Tunkeutumisen havaitseminen (Intrusion Detection Systems) ja estäminen (Intrusion Prevention Systems) analysoivat verkon liikennettä haitallisen toiminnan varalta.
- **VPN (Virtual Private Network):** Salaa etäyhteyksiä ja mahdollistaa turvallisen pääsyn verkkoon.
- **Segmentointi:** Verkon jakaminen aliverkkoihin, jotka rajoittavat pääsyä kriittisiin resursseihin.
- **DDoS-suojaus:** Palvelunestohyökkäysten havaitseminen ja lieventäminen.

Haittaohjelmien torjunta

Haittaohjelmien torjunta estää viruksia, troijalaisia, kiristysohjelmia ja muita haittaohjelmia vahingoittamasta järjestelmiä.

Tapoja torjua haittaohjelmia:

- **Virustorjuntaohjelmat:** Havaitsevat ja poistavat tunnettuja haittaohjelmia.
- **Reaaliaikainen valvonta:** Seuraa tiedostojen ja ohjelmien toimintaa haitallisen käytöksen varalta.
- **Hiekkalaatikot (Sandboxing):** Haitallisen ohjelman suorittaminen eristetyssä ympäristössä vaikutusten analysoimiseksi.

Tietojen varmuuskopiointi ja palautus

Tietojen varmuuskopioinnin kontrollit varmistavat, että tietoja voidaan palauttaa järjestelmävian tai kyberhyökkäyksen jälkeen.

Varmuuskopiointistrategioita:

- **Off-site-varmuuskopiointi:** Kopiointi erilliseen fyysiseen tai pilvipohjaiseen sijaintiin.

- **Ajantasaiset varmuuskopiot:** Mahdollistaa nopean palautuksen lyhyellä aikaviiveellä (RPO, Recovery Point Objective).

- **Disaster Recovery -järjestelmät:** Suunnitelmat ja teknologiat nopeaan toiminnan palauttamiseen.

Haavoittuvuuksien hallinta ja päivitykset

Haavoittuvuuksien hallinta estää hyökkäyksiä päivittämällä ohjelmistot ja poistamalla tunnetut heikkoudet.

Keskeiset käytännöt:

- **Patch management:** Haavoittuvuuksien korjaaminen ajankohtaisilla päivityksillä.
- **Penetraatiotestaus:** Haavoittuvuuksien aktiivinen etsintä ja hyödyntämisen simulointi.
- **Suojauskonfiguraatiot:** Palvelimien ja sovellusten koventaminen minimoimalla niiden hyökkäyspinta-ala.

Lokienhallinta ja valvonta

Tekniset valvontajärjestelmät auttavat havaitsemaan ja reagoimaan poikkeavuuksiin.

Teknologiat:

- **SIEM-järjestelmät (Security Information and Event Management):** Tietoturvalokien ja hälytysten keskitetty analyysi.
- **Reaaliaikainen valvonta:** Verkon ja järjestelmien jatkuva seuranta.
- **Lokitietojen analyysi:** Poikkeavien tapahtumien ja trendien havaitseminen.

Lokienhallinta ja valvonta

Tekniset valvontajärjestelmät auttavat havaitsemaan ja reagoimaan poikkeavuuksiin.

Teknologiat:

- **SIEM-järjestelmät (Security Information and Event Management):** Tietoturvalokien ja hälytysten keskitetty analyysi.
- **Reaaliaikainen valvonta:** Verkon ja järjestelmien jatkuva seuranta.
- **Lokitietojen analyysi:** Poikkeavien tapahtumien ja trendien havaitseminen.

Tietojen eheyden ja saatavuuden hallinta

Näiden mekanismien avulla varmistetaan, että tiedot eivät muutu luvatta ja ovat aina käytettävissä.

Tekniikat:

- **Checksums ja hash-funktiot:** Varmistavat tiedostojen eheyden.
- **Raid-järjestelmät:** Parantavat tietojen saatavuutta ja suojaa laitteistovirheiltä.
- **Kuormantasainjärjestelmät:** Ylläpitävät palvelun saatavuutta korkean kuormituksen aikana.

Hyödyntäminen riskienhallinnassa

Tekniset kontrollit toimivat riskienhallinnassa seuraavilla tavoilla:

1. **Riskejä pienentävät:** Esimerkiksi palomuuri estää ulkoiset hyökkäykset.
2. **Riskejä tunnistavat:** IDS-järjestelmät havaitsevat tunkeutumisyritykset.
3. **Riskejä hallitsevat:** Varmuuskopioinnin avulla järjestelmät voidaan palauttaa hyökkäyksen jälkeen.
4. **Riskejä seuraavat:** SIEM-järjestelmät valvovat ympäristöä jatkuvasti.

Yhdistämällä tekniset kontrollit hallinnollisiin ja fyysisiin mekanismeihin voidaan saavuttaa kattava suojaus organisaation tietoturvariskejä vastaan.

Hallinnolliset kontrollit

Hallinnolliset kontrollit ovat organisaation tasolla tehtyjä suunnitelmia, prosesseja ja sääntöjä, joiden tavoitteena on suojata tietoja ja järjestelmiä. Ne muodostavat pohjan teknisten ja fyysisten kontrollien tehokkaalle käytölle, sillä ne ohjaavat, miten turvallisuutta hallitaan ja miten toimitaan kriisitilanteissa.

Tietoturvapolitiikat ja -ohjeistukset

Tietoturvapolitiikat ovat strategisia dokumentteja, jotka määrittelevät organisaation tietoturvaperiaatteet, tavoitteet ja vastuut.

Keskeiset osa-alueet:

- **Tietoturvapolitiikka:** Korkean tason periaatteet, kuten tietojen luottamuksellisuus, eheys ja saatavuus.
- **Pääsynhallintapolitiikka:** Määrittelee käyttäjien käyttöoikeudet ja roolit.
- **Tietojen luokittelu:** Tiedon jakaminen eri luokkiin, kuten julkinen, luottamuksellinen ja salainen.
- **Etätyöpolitiikka:** Ohjeet turvallisesta työskentelystä kotitoimistoissa (VPN:n ja salattujen laitteiden käyttö).

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietoturvapolitiikat ja -ohjeistukset

- **Henkilökohtaisen laitteen käytön politiikka (BYOD):** Säännöt omien laitteiden turvallisesta käytöstä työympäristössä.

Hyöty riskienhallinnassa:

- Yhtenäiset politiikat vähentävät inhimillisten virheiden riskiä.

- Selkeät ohjeet tukevat nopeaa reagointia kyberuhkiin ja tietomurtoihin.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietoturvakoulutus ja -tietoisuuden lisääminen

Työntekijöiden koulutus ja tietoisuuden lisääminen ovat keskeisiä hallinnollisia keinoja.

Tapoja lisätä tietoisuutta:

- **Phishing-simulaatiot:** Käytännön harjoituksia työntekijöiden valmiuksien parantamiseksi.
- **Tietoturvakoulutukset:** Säännölliset koulutukset kyberuhkista ja tietoturvakäytännöistä.
- **Ohjeet vaaratilanteisiin:** Selkeät toimintaohjeet esimerkiksi haittaohjelmatartuntojen tai tietomurtojen varalle.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tietoturvakoulutus ja -tietoisuuden lisääminen

Hyöty riskienhallinnassa:

- Vähentää merkittävästi ihmisiin kohdistuvien hyökkäysten, kuten tietojenkalastelun (phishing), onnistumisen todennäköisyyttä.

- Parantaa kykyä havaita ja raportoida epäilyttävää toimintaa ajoissa.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Riskienhallintaprosessit

Riskienhallinta on järjestelmällinen lähestymistapa tietoturvariskien tunnistamiseen, arviointiin ja hallintaan.

Riskienhallinnan vaiheet:

1. **Riskien tunnistaminen:** Kartoitus organisaation tietovarannoista, uhkista ja haavoittuvuuksista.

2. **Riskien arviointi:** Todennäköisyyden ja vaikutusten analysointi.

3. **Riskien hallinta:** Toimenpiteiden suunnittelu riskien pienentämiseksi hyväksyttävälle tasolle.

4. **Seuranta ja arviointi:** Riskien ja kontrollien tehokkuuden jatkuva arviointi.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Riskienhallintaprosessit

Hyöty riskienhallinnassa:

- Auttaa priorisoimaan toimenpiteitä ja resursseja suurimpien riskien torjumiseksi.

- Tukee päätöksentekoa, kun valitaan sopivia teknisiä ja fyysisiä kontrolleja.

Auditoinnit ja vaatimustenmukaisuus

Tietoturva-auditoinnit ja lainsäädännön noudattaminen ovat tärkeä osa hallinnollisia kontrollimekanismeja.

Tärkeitä standardeja ja säädöksiä:

- **ISO 27001:** Kansainvälinen tietoturvan hallintajärjestelmän (ISMS) standardi.
- **GDPR (General Data Protection Regulation):** Tietosuoja-asetus, joka säätelee henkilötietojen käsittelyä EU:ssa.
- **NIST Cybersecurity Framework:** Yhdysvaltalainen viitekehys, joka ohjaa tietoturvakäytäntöjä.

Auditoinnit ja vaatimustenmukaisuus

Auditointityypit:

- **Sisäinen auditointi:** Organisaation omien prosessien ja kontrollien arviointi.
- **Ulkoinen auditointi:** Kolmannen osapuolen tekemä arviointi (esim. ISO 27001 -sertifiointi).

Hyöty riskienhallinnassa:

- Varmistaa, että organisaation tietoturvakäytännöt vastaavat vaatimuksia ja parhaita käytäntöjä.
- Havaitsee puutteet ja mahdollistaa niiden korjaamisen ennen kriisitilanteita.

Kriisinhallinta ja jatkuvuussuunnittelu

Organisaation on oltava valmis reagoimaan tehokkaasti kyberuhkiin ja palauttamaan toimintansa nopeasti häiriön jälkeen.

Keskeisiä suunnitelmia:

- **Incident Response Plan:** Toimintaohjeet tietoturvaloukkausten hallintaan.
- **Business Continuity Plan (BCP):** Suunnitelma liiketoiminnan jatkuvuuden varmistamiseksi häiriötilanteessa.
- **Disaster Recovery Plan (DRP):** Teknologian ja tietojärjestelmien palautussuunnitelma.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Kriisinhallinta ja jatkuvuussuunnittelu

Hyöty riskienhallinnassa:

- Vähentää liiketoiminnan keskeytyksestä aiheutuvia tappioita.
- Parantaa organisaation kykyä sopeutua yllättäviin tilanteisiin ja suojata mainettaan.

Kaakkois-Suomen ammattikorkeakoulu

Tietoturvajohtaminen ja vastuut

Organisaation hallintorakenne määrittelee, kuka on vastuussa tietoturvasta ja miten sitä johdetaan.

Keskeiset roolit:

- **CISO (Chief Information Security Officer):** Vastaa strategisesta tietoturvajohtamisesta.
- **Tietoturvatiimi:** Toteuttaa tietoturvatoimenpiteitä ja vastaa päivittäisestä valvonnasta.
- **Liiketoimintajohdon rooli:** Varmistaa, että tietoturva on integroitu osaksi organisaation strategiaa.

Tietoturvajohtaminen ja vastuut

Hyöty riskienhallinnassa:

- Selkeä vastuunjako varmistaa, että tietoturva ei jää huomioimatta.

- Strateginen tietoturvan johtaminen auttaa yhdistämään turvallisuuden liiketoiminnan tavoitteisiin.

Kaakkois-Suomen ammattikorkeakoulu

Kolmansien osapuolien hallinta

Organisaation tulee varmistaa, että sen kumppanit, toimittajat ja muut kolmannet osapuolet noudattavat tietoturvavaatimuksia.

Tapoja hallita kolmansia osapuolia:

- **Sopimukset:** Tietoturvavaatimukset sisällytetään yhteistyösopimuksiin.
- **Toimittaja-auditoinnit:** Arvioidaan toimittajien turvallisuuskäytännöt.
- **Kolmansien osapuolien pääsynhallinta:** Rajoitetaan toimittajien pääsy organisaation järjestelmiin.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Kolmansien osapuolien hallinta

Hyöty riskienhallinnassa:

- Minimoi ulkopuolisista toimijoista aiheutuvat tietoturvariskit.
- Varmistaa, että toimittajaketjun turvallisuus ei heikennä organisaation kokonaisvaltaista suojaa.

Hallinnolliset kontrollit luovat rakenteen, joka ohjaa organisaation tietoturvan hallintaa. Niiden avulla varmistetaan, että tekniset ja fyysiset kontrollit toimivat tehokkaasti ja tietoturva integroituu osaksi liiketoiminnan tavoitteita. Yhdessä ne pienentävät riskejä ja varmistavat organisaation valmiuden kohdata nykyiset ja tulevat uhat.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Fyysiset kontrollit

Fyysiset kontrollit ovat suojatoimenpiteitä, jotka estävät luvattoman pääsyn organisaation fyysisiin tiloihin, laitteistoihin ja infrastruktuuriin. Näiden kontrollien tarkoitus on suojata sekä tietojärjestelmiä että tietoja fyysisiltä uhkilta, kuten tunkeutumiselta, sabotaasilta, ympäristöriskeiltä tai luonnonkatastrofeilta.

Pääsynhallinta fyysisiin tiloihin

Pääsynhallinta estää luvattoman pääsyn kriittisiin tiloihin, kuten serverihuoneisiin, toimistoihin tai muihin tietoturvakriittisiin paikkoihin.

Tapoja hallita pääsyä:

- **Lukitusjärjestelmät:** Mekaaniset lukot, älylukot tai sähköiset lukot.
- **Pääsynvalvonta:** RFID-kortit, PIN-koodit, biometriset tunnisteet (sormenjäljet, kasvotunnistus).
- **Vierailijanhallinta:** Kirjautuminen sisään vierailijana, vierailijakorttien käyttö ja valvonta.
- **Rajoitettu kulku:** Tilojen jako eri turvallisuustasoihin. Esimerkiksi vain tietyillä työntekijöillä on pääsy serverihuoneisiin.

Pääsynhallinta fyysisiin tiloihin

Riskienhallinta:

- Estää luvattomat henkilöt pääsemästä käsiksi laitteistoihin tai tietoihin.

- Tukee tietojen eheyttä ja luottamuksellisuutta.

Kaakkois-Suomen ammattikorkeakoulu

Valvonta ja seuranta

Valvontajärjestelmät mahdollistavat tilojen jatkuvan seurannan ja nopean reagoinnin poikkeavuuksiin.

Tapoja valvoa:

- **Turvakamerat (CCTV):** Videovalvonta auttaa seuraamaan ja tallentamaan tapahtumia.
- **Hälytysjärjestelmät:** Ilmoittavat murtoyrityksistä, tulipalosta tai muista häiriöistä.
- **Reaaliaikainen seuranta:** Valvontakeskukset tai ulkoistetut turvallisuuspalvelut.
- **Sensorit ja anturit:** Liike-, ääni- ja lämpötila-anturit, jotka tunnistavat poikkeavuudet.

Valvonta ja seuranta

Riskienhallinta:

- Pelotevaikutus estää fyysisiä hyökkäyksiä.

- Mahdollistaa poikkeamien nopean havaitsemisen ja käsittelyn.

Kaakkois-Suomen ammattikorkeakoulu

Ympäristöön liittyvien riskien hallinta

Fyysiset kontrollit suojaavat laitteistoja ympäristötekijöiltä, kuten kosteudelta, lämpötilan vaihteluilta tai sähkökatkoilta.

Tärkeitä toimenpiteitä:

- **Ilmastointi ja jäähdytys:** Serverihuoneiden lämpötilan ja kosteuden hallinta estää ylikuumenemista ja kondensaatiota.

- **Ylijännitesuojat:** Suojaavat laitteistoja virtapiikeiltä.

- **UPS (Uninterruptible Power Supply):** Katkeamaton virtalähde varmistaa järjestelmien toiminnan sähkökatkoksen aikana.

- **Tulvasuojaus:** Laitteistojen sijoittaminen tulvariskin ulkopuolelle ja vedenpitävien rakenteiden käyttö.

Ympäristöön liittyvien riskien hallinta

- **Palontorjunta:** Savu- ja palohälyttimet, automaattiset sammutusjärjestelmät (esim. inerttikaasut).

Riskienhallinta:

- Suojaa kriittistä infrastruktuuria ympäristövahingoilta.

- Tukee järjestelmien käytettävyyttä ja toiminnan jatkuvuutta.

Rakenteelliset turvallisuustoimet

Rakenteelliset toimenpiteet estävät fyysisiä uhkia ja suojaavat kriittisiä tiloja.

Rakenteellisia ratkaisuja:

- **Turvallisuushäkit ja kaapit:** Serverien ja tietovarastojen lukitut kaapit ja rack-kotelot.
- **Turvaovet ja -seinät:** Vahvistetut ovet ja seinät, jotka kestävät murtoyrityksiä tai muita hyökkäyksiä.
- **Erityiset suojatilat:** Turvakontit tai datakeskuksille suunnitellut panssaroidut tilat.
- **Kulunohjaus:** Esteet ja portit, jotka estävät luvattoman pääsyn.

Riskienhallinta:

- Hidastaa ja vaikeuttaa fyysistä tunkeutumista.
- Mahdollistaa kriittisten järjestelmien fyysisen suojaamisen myös uhkatilanteissa.

Henkilöstön turvallisuus ja ohjeistus

Fyysinen turvallisuus riippuu myös työntekijöiden koulutuksesta ja ohjeistuksesta.

Keskeiset ohjeistukset:

- **Kulunvalvontaohjeet:** Ohjeet siitä, miten työntekijöiden ja vierailijoiden pääsyä valvotaan.
- **Turvallisuuskoulutus:** Henkilöstön opastus hätätilanteisiin, kuten tulipalot ja evakuoinnit.
- **Laitteiden hallinta:** Ohjeet kriittisten laitteiden siirrosta ja käytöstä.

Riskienhallinta:

- Parantaa henkilöstön valmiuksia reagoida tehokkaasti poikkeustilanteisiin.
- Varmistaa, että kriittisten alueiden turvallisuus otetaan huomioon päivittäisessä toiminnassa.

Varautuminen ja suunnitelmat

Fyysiset kontrollit voivat sisältää varautumisjärjestelyjä hätätilanteita varten.

Keskeiset suunnitelmat:

- **Evakuointisuunnitelmat:** Ohjeistus siitä, miten henkilöstö evakuoidaan turvallisesti.

- **Turvallisuusharjoitukset:** Säännölliset testit varmistavat, että suunnitelmat toimivat.

- **Toipumissuunnitelmat:** Tilat ja resurssit, jotka mahdollistavat kriittisten järjestelmien siirron turvalliseen sijaintiin.

Riskienhallinta:

- Vähentää kriisitilanteiden vaikutuksia henkilöstöön ja järjestelmiin.

- Parantaa organisaation resilienssiä ja valmiutta toiminnan jatkuvuuden varmistamiseen.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Vierailijavalvonta

Organisaation tiloissa käyvät vierailijat voivat aiheuttaa fyysisen turvallisuuden riskejä.

Toimenpiteitä vierailijavalvonnassa:

- **Vierailijoiden rekisteröinti:** Vierailijat kirjataan saapuessa ja heille annetaan kulkuluvat.

- **Saattajat:** Vierailijat liikkuvat tiloissa vain saattajan kanssa.

- **Pääsyn rajoittaminen:** Vierailijoille pääsy vain ei-kriittisiin tiloihin.

Riskienhallinta:

- Estää ulkopuolisten pääsyn arkaluonteisiin tietoihin tai tiloihin.

- Mahdollistaa vierailijoiden liikkeiden seurannan.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Fyysisen turvallisuuden teknologiat

Fyysisten kontrollien tueksi käytetään erilaisia teknologioita, jotka automatisoivat ja tehostavat suojaa.

Keskeiset teknologiat:

- **Älykkäät pääsynhallintajärjestelmät:** Järjestelmät, jotka tunnistavat henkilöt ja hallinnoivat pääsyä reaaliajassa.

- **Geofencing:** Rajaa alueita, joilla tietyt laitteet tai henkilöt voivat liikkua.

- **IoT-antureiden valvonta:** Lämpötila-, liike- tai äänisensorit, jotka tunnistavat poikkeavuudet.

Riskienhallinta:

- Vähentää fyysisen turvallisuuden valvonnan inhimillisiä virheitä.

- Mahdollistaa reaaliaikaisen reagoinnin uhkiin.

Yhteenveto

Fyysiset kontrollit ovat keskeinen osa kokonaisvaltaista tietoturvaa, sillä ne suojaavat infrastruktuuria ja tietoja fyysisiltä uhkilta. Ne täydentävät **teknisiä** ja **hallinnollisia** kontrollimekanismeja ja varmistavat, että organisaation tietoturva on kattava. Yhdistämällä rakenteelliset ratkaisut, teknologiat ja henkilöstön koulutuksen voidaan varmistaa turvallinen ja luotettava ympäristö organisaation toiminnalle.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Tunne huominen.