Ohjelmisto-turvallisuuden johtaminen

- Roolit ja osaamistarpeet

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISSN 2669-8757 (verkkojulkaisu)
ISBN 987-952-425-003-0

Traficomin julkaisuja
1/2026

Julkaisun nimi
Ohjelmistoturvallisuuden johtaminen – Roolit ja osaamistarpeet

Tekijät
Karoliina Mancuso, Solita

Sisällysluettelo

Johdanto

Oppaan tarkoitus

Tämän Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen laatiman oppaan tarkoituksena on vahvistaa ohjelmistoturvallisuuden johtamista organisaatioissa siten, että voidaan turvata sekä yksittäisten toimijoiden että koko yhteiskunnan toiminnan jatkuvuus ja häiriöttömyys digitaalisessa ympäristössä. Opas keskittyy ohjelmistoturvallisuuden sisällyttämiseen osaksi koko ohjelmiston elinkaaren aikaisia prosesseja ja päätöksiä. Lisäksi opas tarjoaa käytännönläheisiä suosituksia erityisesti johdon ja muiden keskeisten toimijoiden tueksi.

Oppaan tavoitteena on tukea organisaatioita ohjelmistoturvallisuuden systemaattisessa johtamisessa koko ohjelmiston elinkaaren ajan. Opas tarjoaa rakenteen, jonka avulla turvallisuus voidaan kytkeä osaksi suunnittelua, päätöksentekoa, hankintoja, kehitystyötä ja ylläpitoa. Tarkoituksena on vahvistaa ennakoivaa otetta, lisätä näkyvyyttä turvallisuusriskeihin ja selkeyttää eri roolien vastuita. Kun ohjelmistoturvallisuutta johdetaan tavoitteellisesti ja johdonmukaisesti, voidaan vähentää haavoittuvuuksia, parantaa luottamusta ohjelmistoihin, tuottaa laadukkaampia ohjelmistoja ja täyttää myös lainsäädännön ja sidosryhmien vaatimuksia.

Kuinka opasta käytetään?

Johdanto-osio tarjoaa taustan ja yhteisen ymmärryksen siitä, mitä turvallinen ohjelmisto tarkoittaa, miksi ohjelmistoturvallisuus on kaikkien vastuulla ja miten turvallisuuden painopisteet muuttuvat ohjelmiston elinkaaren aikana.

Oppaan ydin muodostuu roolikohtaisista osioista, joissa kuvataan kunkin roolin kannalta keskeiset osaamistarpeet sekä käytännön toimet ohjelmistoturvallisuuden varmistamiseksi eri elinkaaren vaiheissa. Voit tarkastella opasta joko oman roolisi näkökulmasta hahmottaaksesi omat tietoturvan osaamistarpeesi tai kokonaisuutena, jolloin saat paremman käsityksen siitä, miten eri toimijat yhdessä varmistavat ohjelmistojen turvallisuuden.

Huomioi, että oppaassa kuvatut roolit ja niihin liitetyt osaamistarpeet eivät ole tyhjentäviä, eikä roolien nimet tai vastuut ole kaikissa organisaatioissa samanlaisia. Roolit ja tehtävien painotukset voivat vaihdella organisaation rakenteen, koon ja toimintatapojen mukaan. Opasta voi soveltaa joustavasti eri tilanteisiin ja täydentää niillä rooleilla, jotka ovat omassa organisaatiossa keskeisiä ohjelmistoturvallisuuden kannalta.

Mitä tarkoittaa turvallinen ohjelmisto?

Hyvin tuotettu ohjelmisto ei ole pelkästään toimiva – se on myös turvallinen.

Turvallinen ohjelmisto on suunniteltu ja toteutettu niin, että sen käyttö, kehitys ja ylläpito huomioivat järjestelmällisesti tietoturvariskit koko ohjelmiston elinkaaren ajan. Se suojaa sekä käyttäjiään että käsiteltävää tietoa, perustuu turvallisen ohjelmistokehityksen periaatteisiin ja mahdollistaa tehokkaan poikkeamien hallinnan.

Turvallisuutta ei saavuteta täydellisellä virheettömyydellä, vaan uhkamallinnuksella, ennakoivalla suunnittelulla ja selkeillä toimintamalleilla tietoturvapoikkeamien ja haavoittuvuuksien tunnistamiseksi, ilmoittamiseksi ja korjaamiseksi.

Turvallinen ohjelmistotuottaja erottautuu läpinäkyvyydellä. Se kertoo avoimesti, miten tietoturva on huomioitu kehityksessä ja ylläpidossa, sekä tarjoaa selkeät kanavat haavoittuvuuksien ilmoittamiseen. Läpinäkyvyys lisää luottamusta ja antaa myös ohjelmiston hankkijalle mahdollisuuden arvioida, miten vastuullisesti ohjelmiston turvallisuutta johdetaan.

Turvallisuus ei ole erillistä lisätyötä, vaan olennainen osa laadukasta ja vastuullista toimintaa.

Ohjelmistoturvallisuus on kaikkien vastuulla

Ohjelmistoturvallisuus ei synny yksittäisen asiantuntijan tai tiimin toimesta, vaan se rakentuu koko organisaation yhteisellä toiminnalla. Johto määrittää suuntaviivat ja resurssit, hankinnoista vastaavat tekevät ratkaisevia valintoja, kehittäjät toteuttavat turvallisuutta käytännössä ja käyttäjät vaikuttavat turvallisuuteen omalla toiminnallaan.

Turvallisuus rakentuu pala palalta arjen päätöksistä, valinnoista ja toimintatavoista. Kun jokainen tuo oman asiantuntemuksensa ja vastuunsa osaksi kokonaisuutta, turvallisuudesta tulee kestävä ja luonteva osa ohjelmistojen elinkaarta. Siksi on tärkeää tunnistaa, miten voi itse vaikuttaa turvallisuuteen, varmistaa oman toiminnan olevan organisaation vaatimusten mukaista ja varmistaa, että tavoitetaso on yhteisesti ymmärretty. Yhtenäinen näkemys turvallisuuden tasosta tukee sujuvaa kehitystä ja varmistaa, että resurssit kohdistuvat oikein.

Kun turvallisuus otetaan huomioon läpi koko ohjelmiston elinkaaren ja otetaan osaksi jokapäiväisiä tehtäviä, riskit pienenevät ja lopputulos on luotettavampi. Turvallisuudesta tulee osa organisaation kulttuuria: tapa ajatella, tehdä päätöksiä ja toimia yhdessä.

Ohjelmiston elinkaari ja tietoturvan painopisteet

Ohjelmiston eri elinkaarivaiheisiin liittyy vaihtelevia tietoturvan painopisteitä ja vaatimuksia. Jokaisessa vaiheessa korostuvat eri turvallisuusteemat, jotka on tärkeää huomioida sekä johtamisessa että käytännön toteutuksessa. Tässä kappaleessa käydään läpi, mitä asioita tulisi erityisesti huomioida kussakin vaiheessa vaatimusten määrittelystä aina käytöstä poistoon asti.

Elinkaaren vaiheet on kuvattu tässä yleisellä tasolla. Kuvaus ei ole tyhjentävä, vaan tarjoaa tiiviin läpileikkauksen ohjelmiston elinkaaren keskeisistä vaiheista tietoturvan näkökulmasta.

Turvallisuus syntyy valinnoista ja johtamisesta jokaisessa vaiheessa – sen vuoksi ohjelmistoturvallisuus on elinkaaren mittainen tehtävä.

1

Vaatimusten määrittely ja suunnittelu

Vaatimusten määrittely ja suunnittelu luovat perustan ohjelmiston hankinnalle tai kehitykselle. Tavoitteena on varmistaa, että ratkaisu vastaa liiketoiminnan tarpeisiin ja tietoturva huomioidaan jo suunnitteluvaiheessa.

2

Hankinta / kehityspäätös

Oli kyseessä oma kehitys tai valmiin ratkaisun hankinta, päätöksenteossa on varmistettava, että turvallisuus-vaatimukset, resurssit ja osaaminen otetaan huomioon alusta asti.

3

Toteutus

Toteutusvaiheessa ohjelmiston lähdekoodi kehitetään ja yhdistetään tarvittaviin komponentteihin. Tavoitteena on tuottaa toimiva, laadukas ja turvallinen ratkaisu, jossa riskit hallitaan jo kehityksen aikana.

4

Rakentaminen

Rakentamisvaiheessa ohjelmisto kootaan turvallisesti ja hallitusti varmistaen luotettavat komponentit ja toistettava prosessi. Tavoitteena on eheä ja vakaa ohjelmisto, joka tukee turvallista käyttöönottoa.

5

Testaus

Testausvaiheessa tietoturva-testaus, kuten haavoittuvuus-skannaukset ja penetraatiotestit, täydentää toiminnallista testausta. Tarkoitus on tunnistaa ja korjata mahdolliset heikkoudet ennen julkaisua.

6

Julkaisu ja käyttöönotto

Julkaisu- ja käyttöönottovaiheessa varmistetaan, että käyttöön otetaan vain hyväksytty ja testattu versio. Käyttöönotto tehdään hallitusti ja turvallisesti huolehtimalla asetuksista, pääsynhallinnasta, riippuvuuksista ja ympäristön turvallisesta konfiguroinnista.

7

Ylläpito ja monitorointi

Ylläpidossa varmistetaan ohjelmiston jatkuva turvallisuus ja toimivuus. Monitorointi havaitsee poikkeamat ja haavoittuvuudet ajoissa, jotta korjaukset voidaan tehdä hallitusti ja minimoida riskit.

8

Käytöstä poisto

Käytöstä poiston yhteydessä varmistetaan tietojen turvallinen käsittely ja järjestelmien purkaminen niin, ettei ympäristöön jää tietoturvariskejä tai haavoittuvia komponentteja.

Ohjelmistotuvallisuuden osaamistarpeet rooleittain

Strateginen ja operatiivinen johto

Tässä osiossa käsitellään, miksi ohjelmistoturvallisuus kuuluu organisaation strategiselle johdolle, millaista ymmärrystä ja osaamista se edellyttää sekä miten johto voi omalla toiminnallaan luoda edellytykset turvallisille ohjelmistoratkaisuille ja niiden hallitulle elinkaarelle.

Osio on kirjoitettu pääosin strategista johtoa ajatellen, mutta sen teemat ja osaamisvaatimukset ovat hyödyllisiä myös operatiivisessa johdossa työskenteleville, kuten tietoturva- ja riskienhallintapäällikölle, sekä muille, jotka vastaavat organisaation turvallisuuden ja vaatimustenmukaisuuden toteutuksesta.

Ohjelmistoturvallisuus on strategiaa.

MIKSI OHJELMISTOTURVALLISUUS KUULUU JOHTAMISEEN?

Ohjelmistoturvallisuus on kilpailutekijä, joka vahvistaa organisaation toimintakykyä, luotettavuutta ja innovointia. Kun johto ymmärtää ohjelmistoturvallisuuden strategisen merkityksen, se voi hyödyntää turvallisuutta liiketoimintaa tukevana voimavarana.

Ohjelmistot ovat yhä useammin liiketoiminnan ytimessä: ne ohjaavat prosesseja, mahdollistavat palvelut ja vaikuttavat suoraan asiakaskokemukseen sekä kilpailukykyyn. Turvalliset ja hallitusti johdetut ohjelmistot lisäävät luottamusta asiakkaiden ja kumppaneiden silmissä, mahdollistavat sujuvan liiketoiminnan, pienentävät riskejä ja tukevat toiminnan jatkuvuutta.

Johto, sekä strateginen että operatiivinen, luo edellytykset turvalliselle ohjelmistokehitykselle ja sen hallinnalle koko elinkaaren ajan. Strateginen johto linjaa suunnan, priorisoinnin ja resurssit ohjelmistoturvallisuudelle. Operatiivinen johto puolestaan varmistaa, että linjaukset jalkautuvat prosesseiksi ja käytännöiksi. Johdon sitoutuminen ohjelmistoturvallisuuteen luo organisaatiokulttuurin, jossa turvallisuus on osa kaikkea päätöksentekoa ja toiminnan suunnittelua.

Riittävä osaaminen ja johdon tuki eivät siis ainoastaan ehkäise riskejä, vaan mahdollistavat liiketoiminnan kestävän kasvun ja varmistavat, että organisaatio voi hyödyntää teknologiaa turvallisesti ja rohkeasti.

Tiivistelmä

JOHDON OSAAMISTARPEET

- Ymmärretään, että ohjelmistoturvallisuus ei ole vain tekninen tehtävä, vaan jatkuva prosessi, joka edellyttää strategista ajattelua, resursointia ja johdon sitoutumista.
- Ymmärretään, miten ohjelmistoturvallisuus vaikuttaa organisaation liiketoimintariskeihin, jatkuvuuteen ja kilpailukykyyn.
- Osataan liittää ohjelmistoturvallisuuden osaksi strategista suunnittelua, riskienhallintaa ja päätöksentekoa.
- Tunnistetaan ohjelmistojen elinkaaren eri vaiheisiin liittyvät riskit.
- Ymmärretään, miten ohjelmistojen turvallisuus rakentuu vaiheittain ja miksi se ei ole erillinen tekninen osa-alue.
- Ymmärretään keskeiset lainsäädännölliset ja sopimukselliset vaatimukset, jotka ohjaavat ohjelmistojen turvallisuutta.
- Tunnistetaan ulkoisten toimittajien ja toimitusketjujen vaikutuksen ohjelmistoturvallisuuteen.
- Ymmärretään, miten asiakasvaatimukset ja sopimukset vaikuttavat ohjelmiston turvallisuuteen ja vastuisiin.
- Osataan arvioida, milloin tietoturvariski on liiketoiminnallisesti merkittävä ja vaatii johdon toimenpiteitä.

OHJELMISTOTURVALLISUUDEN STRATEGINEN PAINOTTAMINEN JA LINJAAMINEN

Johdon tehtävänä on tunnistaa, että ohjelmistoturvallisuus on osa liiketoiminnan jatkuvuutta ja kilpailukykyä. Strateginen johto luo suunnan ja kulttuurin, joissa turvallisuus on olennainen osa päätöksentekoa, resursointia ja riskienhallintaa. Operatiivinen johto varmistaa, että nämä linjaukset toteutuvat käytännön prosesseissa ja toiminnassa.

Ymmärtää ohjelmistoturvallisuuden strategisen merkityksen liiketoiminnalle

Ohjelmistoturvallisuus vaikuttaa suoraan organisaation liiketoimintariskeihin, kilpailukykyyn ja asiakassuhteisiin. Ohjelmistot ovat yhä useammin keskeinen osa palveluita, tuotteita ja prosesseja, ja niiden turvallisuus on olennainen osa organisaation luotettavuutta ja toimintakykyä. Kun johto ymmärtää ohjelmistoturvallisuuden vaikutukset liiketoiminnan jatkuvuuteen, maineeseen ja sääntelyn noudattamiseen, se voi tehdä tietoon perustuvia päätöksiä, jotka tukevat liiketoiminnan kasvua.

Tietoturva ei toteudu sattumalta – se vaatii suunnittelua, johdon sitoutumista ja resursointia.

Kykenee liittämään ohjelmistoturvallisuuden osaksi liiketoimintastrategiaa ja toimintaperiaatteita

Ohjelmistoturvallisuus ei saa olla irrallinen tukitoiminto, vaan sen tulee kiinteä osa päätöksentekoa, riskienhallintaa ja liiketoiminnan kehittämistä. Kun turvallisuus on sisällytetty strategisiin prosesseihin, se tukee organisaation kykyä hallita riskejä ja varmistaa toiminnan jatkuvuus myös häiriötilanteissa. Johdon strateginen ohjaus tekee ohjelmistoturvallisuudesta ennakoivaa ja yhtenäistä, ei reaktiivista tai yksittäisten asiantuntijoiden vastuulle jäävää toimintaa.

Ymmärtää ohjelmistoturvallisuuteen liittyvät riskit ja keskeiset sääntelyvaatimukset

Johdon on ymmärrettävä, miten ohjelmistoturvallisuus liittyy organisaation kokonaisriskeihin, sääntelyvelvoitteisiin (esim. NIS2, CRA) ja liiketoimintatavoitteisiin. Tämä tarkoittaa kykyä arvioida ohjelmistoihin liittyviä riskejä strategisella tasolla ja huomioida ohjelmistoturvallisuus osana päätöksentekoa. On myös varmistettava, että turvallisuutta johdetaan suunnitelmallisesti koko ohjelmiston elinkaaren ajan.

Osaa tehdä tietoon perustuvia päätöksiä ja kohdentaa resurssit vaikuttavasti turvallisuustyöhön

Ohjelmistoturvallisuus vaatii johdonmukaista päätöksentekoa ja oikea-aikaista resurssien kohdentamista. Johdon on kyettävä arvioimaan, milloin ja mihin ohjelmistoturvallisuuteen liittyviin toimiin investoidaan – oli kyseessä henkilöstön osaamisen kehittäminen, turvallisuustyökalujen hankinta tai turvallisuusprosessien kehittäminen. Ilman tätä kykyä turvallisuus voi jäädä reaktiiviseksi ja hajanaiseksi, mikä kasvattaa riskejä ja kustannuksia pitkällä aikavälillä.

Ymmärtää elinkaariajattelun ja ohjelmistojen merkityksen jatkuvuuteen

Ohjelmistot eivät ole kertaluonteisia hankintoja, vaan pitkäaikaisia ja liiketoimintakriittisiä kokonaisuuksia, jotka vaikuttavat organisaation toimintaan koko elinkaarensa ajan. Jos ohjelmistojen jatkuvuutta ja kehittyvää luonnetta ei huomioida riittävästi päätöksenteossa ja johtamisessa, organisaatio voi altistua tekniselle velalle, tietoturvariskeille ja liiketoiminnan keskeytyksille, jotka olisi voitu ehkäistä ennakoivalla suunnittelulla ja pitkäjänteisellä johtamisella.

Ymmärtää toimitusketjujen ja ulkoisten ohjelmistotoimittajien roolin turvallisuudessa

Ohjelmistoturvallisuus ei rajoitu organisaation sisäisiin järjestelmiin, vaan ulottuu koko toimitusketjuun ja erityisesti ulkoisiin ohjelmistotoimittajiin. Johto tarvitsee ymmärrystä siitä, miten kolmansien osapuolten ohjelmistot, komponentit ja palvelut voivat muodostaa merkittäviä riskejä. Toimitusketjujen hallinta on keskeinen osa ohjelmistoturvallisuuden kokonaisuutta, ja johdon on varmistettava, että toimittajilta edellytetään selkeitä turvallisuusvaatimuksia, sopimuksellisia velvoitteita ja jatkuvaa valvontaa. Tämä on erityisen tärkeää niin jatkuvuuden kuin sääntelyn näkökulmasta, sillä esimerkiksi NIS2 edellyttää kykyä hallita myös toimitusketjuun liittyviä riskejä.

Osaa viestiä ohjelmistoturvallisuudesta ja vahvistaa turvallisuuskulttuuria omalla esimerkillään

Johto toimii suunnannäyttäjänä koko organisaatiolle ja sen viestintä vaikuttaa suoraan siihen, miten ohjelmistoturvallisuus ymmärretään ja otetaan vakavasti eri tasoilla. Kun johto viestii selkeästi turvallisuuden merkityksestä ja osoittaa sitoutumista siihen omalla toiminnallaan, se rakentaa turvallisuuskulttuuria, jossa jokainen työntekijä ymmärtää oman roolinsa turvallisuuden varmistamisessa. Tämä ei vaadi teknistä asiantuntemusta, vaan kykyä johtaa arvoilla ja viestiä tavoitteista. Johto voi tukea turvallisuutta tuomalla sen osaksi organisaation arkea ja päätöksentekoa.

Keskeiset toimet:

- Aseta ohjelmistoturvallisuudelle konkreettiset tavoitteet ja mittarit.
- Linjaa ohjelmistoturvallisuus osaksi organisaation strategiaa ja keskeisiä toimintamalleja, kuten kehittämistä, hankintoja ja riskienhallintaa.
- Käsittele ohjelmistoturvallisuutta säännöllisesti johtoryhmässä.
- Varmista, että kaikissa ohjelmiston elinkaaren vaiheissa on aikaa, osaamista ja vastuuhenkilöt turvallisuuden varmistamiseen.
- Huolehdi, että sääntelyvaatimukset (esim. NIS2, CRA) tunnetaan ja huomioidaan toiminnassa.
- Aseta selkeät turvallisuusvaatimukset myös ulkoisille toimittajille ja seuraa niiden toteutumista.
- Suunnittele päivitykset ja ohjelmistojen poistaminen osaksi jatkuvuudenhallintaa.
- Viesti ohjelmistoturvallisuuden merkityksestä ja näytä esimerkkiä sitoutumisesta turvallisuuteen.

TARPEEN MÄÄRITTELY, SUUNNITTELU JA HANKINTAPÄÄTÖS

Johdon tehtävänä on varmistaa, että tietoturva- ja liiketoimintavaatimukset huomioidaan jo ohjelmistojen suunnittelun ja hankinnan alkuvaiheissa. Strateginen johto linjaa tavoitteet ja varmistaa resurssit, jotta turvallisuus sisältyy osaksi vaatimustenmäärittelyä, hankintakäytäntöjä ja toimittajavalintoja. Operatiivinen johto vastaa siitä, että nämä linjaukset toteutuvat käytännössä ja että vaatimukset ovat selkeitä, mitattavia ja vertailukelpoisia koko hankintaprosessin ajan.

Ymmärtää vaatimustenmäärittelyn merkityksen suunnittelu- ja hankintavaiheessa

Vaatimusten määrittely suunnittelun tai hankinnan varhaisessa vaiheessa on keskeistä, jotta turvallisuus ei jää vain tekniseksi yksityiskohdaksi, vaan vastaa myös liiketoimintatarpeisiin. Ohjelmiston hankinnan tai suunnittelun alkuvaiheessa tehdään päätöksiä, jotka vaikuttavat ohjelmiston turvallisuuteen koko sen elinkaaren ajan. Jos liiketoimintakriittiset tarpeet jäävät tunnistamatta tai sääntelyn vaatimukset täyttämättä, seuraukset voivat näkyä myöhemmin kalliina tai jopa mahdottomina korjauksina. Hyvin määritellyt vaatimukset mahdollistavat vertailukelpoiset tarjoukset, realistisen aikataulutuksen ja sen, että toimittaja voi sitoutua selkeästi määriteltyihin turvallisuustavoitteisiin.

Ymmärtää riskienhallinnan merkityksen suunnittelu- ja hankintavaiheessa

Riskienhallinta suunnittelu- ja hankintavaiheessa on edellytys onnistuneelle ja turvalliselle ohjelmistohankkeelle. Näissä varhaisissa vaiheissa tehdään ratkaisuja, jotka vaikuttavat ohjelmiston turvallisuuden lisäksi myös organisaation toiminnan jatkuvuuteen ja kyberturvallisuuden tasoon. Ennakoiva riskienhallinta mahdollistaa turvallisuusvaatimusten oikein kohdentamisen ja että toimittajalta voidaan edellyttää realistisia ja riittäviä turvallisuustoimia tarjouspyynnön ja sopimuksen tasolla.

Ymmärtää sopimusprosessin roolin tietoturvassa

Ulkoisten toimittajien ja kumppaneiden kanssa tehtävät sopimukset määrittävät vastuut, velvoitteet ja mahdollisuudet valvoa turvallisuutta. Sopimus on usein ainoa keino, jolla organisaatio voi sitouttaa toimittajat pitkäaikaisiin turvallisuusvelvoitteisiin, kuten haavoittuvuuksien korjaamiseen, auditointioikeuksiin ja tietoturvaloukkauksiin reagoimiseen. Jos sopimus ei sisällä näitä elementtejä, ongelmiin on vaikea puuttua jälkikäteen ja sopimukset voivat jättää organisaation alttiiksi toimitusketjuriskeille tai sääntelyrikkomuksille.

Tunnistaa yhteistyön tarpeen eri liiketoiminta-alueiden välillä

Ohjelmistoturvallisuus ei ole vain IT:n tai tietoturvatiimin vastuulla. Johdon tulee ymmärtää, että turvallinen ohjelmistohankinta edellyttää yhteistyötä liiketoiminnan, juridiikan, hankinnan, tietoturvan ja teknisten asiantuntijoiden välillä, jotta kaikki näkökulmat ja vaatimukset tulevat huomioiduksi. Ilman johdon tukea eri yksiköt toimivat helposti siiloissa, jolloin kokonaisvastuu jää epäselväksi ja tietoturva voi jäädä katveeseen.

Keskeiset toimet:

- Edellytä, että vaatimustenmäärittelyssä huomioidaan tietoturva ja liiketoimintakriittiset tarpeet.
- Varmista, että organisaatiossa on selkeät riskienhallintaprosessit jo suunnittelun ja hankinnan alkuvaiheeseen.
- Luo selkeät turvallisuusvaatimukset, jotka ohjaavat tarjouspyyntöjä, toimittajavalintoja ja sopimusneuvotteluita.
- Varmista, että organisaatiolla on riittävä asiantuntemus ja resurssit turvallisuusvaatimusten määrittelyyn ja arviointiin.
- Edellytä, että tietoturva sisältyy hankintojen ja kumppanuuksien hallintaan.
- Tarjoa ohjeistusta, koulutusta ja tukea vaatimustenmäärittelyyn osallistuville henkilöille.
- Luo käytännöt, jotka tuovat yhteen eri osastojen asiantuntemuksen jo suunnittelun ja hankinnan varhaisessa vaiheessa.

Turvallisuuden rakentaminen alusta alkaen on kustannustehokasta ja suojaa liiketoimintaa.

OHJELMISTOKEHITYS

Johdon vastuulla on varmistaa, että ohjelmistokehitystä ohjataan suunnitelmallisesti ja turvallisesti koko organisaatiossa. Strateginen johto määrittää tavoitteet ja varmistaa, että kehitysresurssit, osaaminen ja ohjausmallit tukevat turvallisuutta, sääntelyä ja riskienhallintaa. Operatiivinen johto vastaa siitä, että nämä periaatteet näkyvät konkreettisesti kehitysprosesseissa, työnjaossa ja arjen käytännöissä.

Tuntee keskeiset tietoturvan hallintamallit ja sääntelyn vaikutukset kehitystyöhön

Organisaation johdon tulee ymmärtää, miten keskeiset tietoturvan hallintamallit ja sääntely (esim. GDPR, NIS2, CRA, OWASP Top 10, NIST SSDF, ISO/IEC 27001 ja 27034) ohjaavat turvallista ohjelmistokehitystä. Nämä viitekehykset määrittävät vaatimuksia, jotka vaikuttavat ohjelmiston turvallisuuteen, auditointimahdollisuuksiin ja sääntelyvaatimusten täyttämiseen. Johdon on kyettävä arvioimaan, miten sääntely vaikuttaa organisaation vastuisiin ja riskeihin, sekä varmistamaan, että kehitystyö on linjassa vaatimusten kanssa.

Ymmärtää, että uhkat ja turvalliset käytännöt muuttuvat jatkuvasti

Kyberturvallisuuden koko kenttä muuttuu jatkuvasta: uhkat, kehityskäytännöt ja käytettävät työkalut. Johdon tulee mahdollistaa kehitystiimien jatkuva oppiminen ja kouluttautuminen, jotta organisaatio pysyy ajan tasalla uusista uhista ja pystyy reagoimaan niihin tehokkaasti. Tämä edellyttää resursointia, ohjeistusta ja kulttuuria, jossa osaamisen kehittäminen on osa arkea. Ilman jatkuvaa oppimista turvallisuusratkaisut vanhenevat nopeasti ja organisaatio altistuu riskeille, joita ei tunnisteta tai osata hallita.

Ymmärtää asiakasvaatimusten ja sopimusten vaikutuksen kehitystyössä

Asiakasvaatimukset ja sopimukset määrittävät, mitä turvallisuustoimia ohjelmistolta odotetaan ja miten vastuut jakautuvat. Johdon tulee ymmärtää, että sopimuksilla voidaan sitouttaa kehitystiimit ja toimittajat noudattamaan turvallisuusvaatimuksia, kuten haavoittuvuuksien hallintaa, auditointioikeuksia ja reagointia tietoturvaloukkauksiin. Ilman selkeitä sopimusvelvoitteita organisaatio voi altistua toimitusketjuriskeille ja sääntelyrikkomuksille.

Ymmärtää turvallisen ohjelmistokehityksen vaiheet

Turvallinen ohjelmistokehitys ei ole yksittäinen tarkistuspiste vaan jatkuva osa koko kehitysprosessia. Johdon tulee ymmärtää keskeiset vaiheet, kuten vaatimusmäärittely, suunnittelu, uhkamallinnus, turvallinen koodaus, testaus, julkaisu ja ylläpito. Secure by Design -periaate edellyttää, että tietoturva huomioidaan alusta alkaen. Johdon ymmärrys näistä vaiheista mahdollistaa realististen aikataulujen, resurssien ja tavoitteiden asettamisen sekä tukee kehitystiimejä tietoturvan integroinnissa.

Osaa hyödyntää riskienhallintaa päätöksenteossa

Ohjelmistokehitykseen liittyvät riskit voivat vaikuttaa merkittävästi organisaation toimintaan, talouteen ja maineeseen. Johdon tulee kyetä tekemään tietoon perustuvia päätöksiä riskien hyväksymisestä, siirtämisestä tai torjumisesta. Tämä edellyttää ymmärrystä siitä, milloin riski on liiketoiminnallisesti hyväksyttävä ja milloin se vaatii toimenpiteitä. Organisaatiossa tulisi olla selkeät prosessit, joiden avulla ohjelmistokehityksen riskit nousevat tarvittaessa johdon tietoisuuteen. Tämä mahdollistaa ohjelmistokehityksen riskien kytkeytymisen osaksi liiketoiminnan johtamista, jolloin niihin voidaan reagoida oikea-aikaisesti ja liiketoiminnan tavoitteiden mukaisesti.

Oikeat päätökset vaativat oikeaa ymmärrystä.

Keskeiset toimet:

- Varmista, että sääntelyn vaatimukset on tunnistettu ja että ne on sisällytetty kehitysprosessien ja auditointien ohjaukseen.
- Edellytä, että kehitysprojekteissa on käytössä viitekehyksiin perustuvat kontrollit.
- Edellytä, että kehityksessä noudatetaan dokumentoitua prosessia, jossa turvallisuus huomioidaan kaikissa vaiheissa.
- Edellytä, että asiakasvaatimukset kartoitetaan ja dokumentoidaan kattavasti ennen kehitystyön käynnistämistä.
- Varmista, että kehitystiimeillä on käytössään turvallisuutta tukevat menetelmät ja työkalut sekä riittävä osaaminen.
- Tue kehitystiimejä realististen aikataulujen ja resurssien määrittelyssä niin, että turvallisuus voidaan aidosti sisällyttää kehitystyöhön.
- Luo prosessit, joilla ohjelmistokehityksen riskit arvioidaan ja dokumentoidaan säännöllisesti projektien aikana.
- Luo selkeä toimintamalli sille, miten kehitysprojekteissa tunnistetut merkittävät riskit tuodaan johdon tietoon ajoissa.

OHJELMISTON KÄYTTÖÖNOTTO, KÄYTTÖ JA YLLÄPITO

Ohjelmiston käytön aikana johdon tehtävänä on ylläpitää sitoutumista ohjelmistoturvallisuuden tavoitteisiin ja varmistaa, että toteutukseen on riittävät resurssit, osaaminen ja vastuut. Strateginen johto mahdollistaa jatkuvan parantamisen luomalla rakenteet, jotka tukevat seurantaa, kehittämistä ja raportointia koko ohjelmiston elinkaaren ajan. Operatiivinen johto varmistaa, että nämä rakenteet toimivat käytännössä ja että turvallisuus pysyy osana päivittäistä toimintaa ja päätöksentekoa.

Ymmärtää käyttöönottoprosessin tietoturvariskit ja hallintatarpeet

Ohjelmiston käyttöönotto on kriittinen vaihe, jossa tehdään päätöksiä ja toimia, joilla on pitkäkestoisia vaikutuksia tietoturvaan. Tietoturvatestaukset, konfiguraatioiden validointi, käyttöoikeuksien hallinta ja järjestelmän kovennus ovat kriittisiä toimenpiteitä, jotka on sisällytettävä käyttöönottosuunnitelmaan. Lisäksi on varmistettava, että dokumentointi on kattavaa ja että kolmansien osapuolien roolit ja vastuut on selkeästi määritelty. Ilman näitä toimenpiteitä käyttöönottovaihe voi jättää ohjelmiston haavoittuvaksi heti alusta alkaen.

Ymmärtää jatkuvan ylläpidon merkityksen ohjelmiston tietoturvassa

Tietoturva ei pääty ohjelmiston julkaisuun. Johdon tulee ymmärtää, että ohjelmiston turvallisuus vaatii jatkuvaa ylläpitoa, kuten haavoittuvuuksien hallintaa, versiopäivityksiä ja poikkeamien käsittelyä. On tärkeää, että vastuut ja resurssit on määritelty koko elinkaaren ajaksi, ja että organisaatio toimii proaktiivisesti tietoturvan hyväksi. Lisäksi johdon tulee varautua tilanteisiin, joissa ohjelmiston tuki päättyy. Vaihtoehtoisten toimittajien kartoittaminen ja ylläpitosopimusten hallinta ovat tärkeä osa liiketoimintariskien hallintaa.

Osaa varmistaa riittävät resurssit ja prosessit haavoittuvuuksien hallintaan

Haavoittuvuudet ovat väistämättömiä, jonka vuoksi haavoittuvuuksien tunnistamisen, arvioinnin ja korjaamisen on oltavat nopeaa ja systemaattista. Päivittämättä jääneet kirjastot ja komponentit muodostavat merkittäviä riskejä. Ohjelmiston osaluettelo (SBOM, Software Bill of Materials) auttaa hallitsemaan kokonaisuutta ja tunnistamaan, mitä

Jatkuva parantaminen on osa kyberturvallisuuden resilienssiä.

komponentteja ohjelmisto sisältää ja missä kohtaa ne voivat aiheuttaa riskejä. Osana tätä on tärkeää huolehtia myös laajemmasta IT-omaisuuden hallinnasta, jotta tiedetään, mitä ohjelmistoja ja versioita organisaatiossa on käytössä. Jos SBOMia ei ole saatavilla, riskejä voidaan pienentää ylläpitämällä muulla tavoin listaa käytetyistä kirjastoista ja komponenteista, sekä seuraamalla aktiivisesti toimittajien haavoittuvuustiedotteita. Johdon rooli on varmista, että haavoittuvuuksien hallinta on jatkuvaa ja priorisoitua, ja että päivityskäytännöt ja vastuut on määritelty selkeästi.

Tiedostaa valvonnan ja poikkeamienhallinnan merkityksen

Tehokas valvonta ja poikkeamiin reagointi ovat keskeisiä osia ohjelmiston turvallisuutta. Valvontamekanismit, kuten lokitus ja hälytykset, mahdollistavat poikkeamien havaitsemisen ajoissa. Johdon vastuulla on varmistaa, että valvontaa tehdään riittävän tehokkaasti ja systemaattisesti, ja että olemassa olevat mahdollistavat nopean ja koordinoidun reagoinnin. Myös esimerkiksi NIS2-direktiivin mukaiseen raportointivelvoitteeseen tulee olla olemassa selkeät toimintamallit ja ohjeistukset.

Ymmärtää harjoittelun merkityksen poikkeamatilanteissa

Poikkeamienhallinnan toimintamalleja tulee harjoitella säännöllisesti, jotta tiedetään, että toimintamallit todella toimivat kriisitilanteissa. On johdon vastuulla varmistaa, että organisaatiossa järjestetään käytännönläheisiä harjoituksia, jotka kattavat erilaisia uhkaskenaarioita. On hyvä harjoitella tilanteita, joissa esimerkiksi ohjelmistossa on haavoittuvuus tai vikatilanne, ja myös varmuuskopioista palauttamista. Harjoittelun kautta varmistetaan roolien selkeys, päätöksenteon sujuvuus ja yhteistyö eri osastojen välillä. Harjoitukset tuovat myös esiin mahdolliset puutteet nykyisissä toimintamalleissa ja tukevat jatkuvaa parantamista.

Ymmärtää käyttöoikeuksien hallinnan ja tiedon luokittelun periaatteet

Käyttöoikeuksien hallinta ja tiedon luokittelu ovat keskeisessä osassa niin asiakkaiden kuin organisaation tiedon turvaamisessa. Johdon tulee varmistaa, että käyttöoikeudet perustuvat roolipohjaisuuteen, ovat ajantasaisia ja noudattavat ”need to know” -periaatetta. Tiedon luokittelu auttaa ohjaamaan, mitä tietoa suojataan ja miten vahvasti. Tiedon luokittelu ja sen mukainen pääsynhallinta suojaavat kriittisiä tietoja väärinkäytöksiltä ja virheiltä. Ilman selkeää hallintamallia käyttöoikeudet voivat muodostua merkittäväksi riskiksi.

Keskeiset toimet:

- Edellytä, että käyttöönottosuunnitelmat sisältävät:
  - tietoturvatestaukset
  - konfiguraatioiden tarkistukset
  - käyttöoikeuksien hallinnan
  - järjestelmän kovennuksen
  - selkeät vastuut, myös kolmansien osapuolien roolit ja vastuut
  - dokumentointivaatimukset ohjelmiston käyttöönotosta
- Resursoi jatkuva ylläpito, joka kattaa haavoittuvuuksien hallinnan, versiopäivitykset ja poikkeamien käsittelyn koko ohjelmiston elinkaaren ajan.
- Mahdollista haavoittuvuuksien hallinta tarjoamalla riittävät työkalut, osaaminen ja prosessit nopeaan reagointiin.
- Edellytä, että ohjelmiston osaluettelo (SBOM) on käytössä ja että komponenttien päivitykset ovat hallittuja ja seurattuja.
- Mahdollista tehokas valvonta ja poikkeamienhallinta osana jokapäiväistä operatiivista toimintaa.
- Varmista, että on olemassa prosessit, joiden avulla raportointivelvollisuudet täytetään.
- Resursoi säännölliset poikkeamaharjoitukset, jotka parantavat organisaation reagointikykyä ja yhteistyötä eri osastojen välillä. Osallistu myös itse harjoituksiin.
- Edellytä, että käyttöoikeuksien hallintaan ja tiedon luokitteluun on politiikat, jotka perustuvat selkeisiin periaatteisiin ja tukevat riskienhallintaa sekä sääntelyvaatimuksia.

Hallittu käytöstä poisto on tärkeä osa tietoturvallisuutta ja jatkuvuudenhallintaa.

OHJELMISTON KÄYTÖSTÄ POISTO

Johdon vastuulla on varmistaa, että organisaatiolla on selkeät prosessit ohjelmistojen hallittuun käytöstä poistoon. Strateginen johto linjaa periaatteet ja varmistaa, että poistamiseen, tietojen käsittelyyn ja toimittajavelvoitteisiin liittyvät menettelyt tukevat jatkuvuudenhallintaa ja tietoturvaa myös ohjelmiston elinkaaren viimeisessä vaiheessa. Operatiivinen johto vastaa prosessien käytännön toteutuksesta, dokumentoinnista ja siitä, että poistaminen tapahtuu turvallisesti ja sääntelyn mukaisesti.

Ymmärtää ohjelmiston käytön päättämiseen liittyvät riskit

Ohjelmistojen käytöstä poistaminen on kriittinen vaihe, joka vaatii suunnitelmallisuutta ja riskien tunnistamista. Käytöstä poistettavat järjestelmät voivat sisältää arkaluonteista tietoa, riippuvuuksia muihin palveluihin tai liiketoimintakriittisiä toimintoja, joiden hallitsematon katkaiseminen voi aiheuttaa merkittäviä häiriöitä. Käytöstä poisto voi liittyä esimerkiksi toimittajasuhteen päättymiseen, teknologian vanhenemiseen tai siirtymiseen uuteen järjestelmään. Käytöstä poiston yhteydessä tulee arvioida, mitä riskejä tähän liittyy (esim. tiedon menetykset, siirtymävaiheen haavoittuvuudet) ja varmistaa, että ne hallitaan.

Ymmärtää tietojen poistamisen ja säilyttämisen vaatimukset

Tietojen poistaminen ja säilyttäminen eivät ole pelkästään teknisiä tehtäviä, vaan liiketoimintaa ja tietoturvaa koskevia vastuukysymyksiä. Ohjelmistot keräävät ja käsittelevät usein arkaluonteista tai henkilötietolain alaista tietoa, jonka käsittelylle on määritelty tarkat säilytysajat ja poistovaatimukset esimerkiksi tietosuojalainsäädännössä tai asiakassopimuksissa. Liian pitkään säilytetyt tarpeettomat tiedot voivat muodostaa tietoturvariskin, ja toisaalta liian aikaisin poistettu tieto voi aiheuttaa liiketoiminnallisia tai juridisia ongelmia. On tärkeää, että organisaatiolla on selkeät politiikat ja prosessit tietojen luokitteluun, säilytysaikojen määrittelyyn ja tietojen poistamiseen, ja että nämä ovat linjassa toimialan vaatimusten, lainsäädännön ja asiakkaiden odotusten kanssa.

Ymmärtää sopimusten ja toimittajahallinnan merkityksen käytöstä poistoon

Ohjelmiston käytöstä poistoon liittyvät sopimukset ja toimittajahallinta ovat keskeisiä tietoturvan hallinnan välineitä. Käytöstä poiston yhteydessä korostuvat erityisesti toimittajien vastuut ja tiedonhallinnan velvoitteet. Jos ohjelmisto on ollut ulkoisen kumppanin hallinnassa, on varmistettava, että sopimuksissa on selkeästi määritelty, miten tiedot poistetaan, miten poistaminen dokumentoidaan ja miten organisaatio voi tarvittaessa varmistaa toimenpiteiden toteutumisen. Ilman näitä sopimusperusteisia velvoitteita organisaatio voi jäädä tilanteeseen, jossa tietoja ei poisteta asianmukaisesti tai jää epäselväksi, kuka vastaa tietoturvasta elinkaaren viimeisessä vaiheessa.

Keskeiset toimet:

- Luo käytöstä poiston prosessit ja varmista, että ne ovat linjassa organisaation tietoturvapolitiikan ja sääntelyvaatimusten kanssa.
- Määritä käytöstä poistoon liittyvät vastuut selkeästi: kuka vastaa tietojen poistamisesta, dokumentoinnista ja mahdollisista auditoinneista.
- Varmista, että käytöstä poiston prosessit kattavat myös kumppanit ja toimittajat.
- Edellytä, että käytöstä poistoon laaditaan aina erillinen suunnitelma, jossa tunnistetaan liiketoiminta- ja tietoturvariskit.
- Luo organisaatioon politiikat ja prosessit tietojen luokitteluun, säilytysaikojen määrittelyyn ja turvalliseen poistamiseen.
- Ohjaa resurssit ohjelmiston tietoturvalliseen alasajoon.
- Varmista, että sopimuksissa huomioidaan käytöstä poiston aikaiset tietoturvavelvoitteet ja vastuut.
- Edellytä, että toimittajahallinta ulottuu myös ohjelmiston elinkaaren loppuun asti.

Ohjelmistoturvallisuus alkaa hankintavaiheessa tehdyistä päätöksistä.

Ohjelmistohankinnoista vastaava

Tässä osiossa käsitellään, millaista tietoturvaosaamista valmiiden ohjelmistojen hankinnoista vastaavalta edellytetään ohjelmiston eri elinkaaren vaiheissa ja miten hän voi omalla toiminnallaan edistää ohjelmistoturvallisuutta.

MIKSI OHJELMISTO-TURVALLISUUS KUULUU OHJELMISTOHANKINNOISTA VASTAAVALLE?

Kun ohjelmisto otetaan käyttöön osana organisaation toimintaa, sen turvallisuus vaikuttaa suoraan toiminnan jatkuvuuteen, tietojen suojaan ja asiakaskokemukseen. Ilman tietoturvan huomioimista jo hankinnan alkuvaiheessa organisaatio voi altistua riskeille, joita on myöhemmin vaikea tai kallista korjata.

Kun tietoturva otetaan järjestelmällisesti huomioon jo hankintavaiheessa, se luo perustan turvalliselle ohjelmistolle koko sen elinkaaren ajaksi. Hankintavastaava määrittelee vaatimukset, valitsee toimittajat ja neuvottelee sopimukset. Kaikki nämä ovat keskeisiä vaiheita, joissa luodaan pohja sille, että myöhemmissä vaiheissa mukana olevat roolit, kuten järjestelmävastaavat ja palveluomistajat, voivat toimia turvallisesti.

Ohjelmistohankinnoista vastaavan tehtävänä on varmistaa, että turvallisuusnäkökulmat sisällytetään koko hankintaprosessiin, alkaen tarpeiden määrittelystä ja toimittajien arvioinnista aina sopimusehtoihin ja elinkaaren hallintaan saakka. Tämä ei edellytä syvällistä teknistä osaamista, vaan ymmärrystä siitä, miten turvallisuusvaatimukset kytkeytyvät hankintapäätöksiin ja miten ne voidaan varmistaa yhteistyössä teknisten asiantuntijoiden kanssa.

Tiivistelmä

OHJELMISTOHANKINNOISTA VASTAAVAN OSAAMISTARPEET

- Ymmärtää ohjelmistoturvallisuuden merkityksen liiketoiminnassa, riskienhallinnassa ja jatkuvuudessa.
- Tunnistaa sääntelyn, tietosuojan ja toimitusmallien vaikutukset hankintaan.
- Ymmärtää, miten ohjelmiston turvallisuus muodostuu.
- Osaa määritellä ja konkretisoida tietoturvavaatimukset hankintadokumentteihin ja sopimuksiin.
- Osaa arvioida toimittajan tietoturvakyvykkyyttä ja turvallisuuskäytäntöjä.
- Osaa asettaa perustellut tietoturvavaatimukset toimittajalle ja tunnistaa toimittajan rooli ja vastuut tietoturvan toteutumisessa.
- Ymmärtää yhteistyön merkityksen eri asiantuntijoiden kanssa hankintaprosessissa.
- Osaa varmistaa tietoturvavaatimusten toteutumisen ennen käyttöönottoa.
- Osaa tunnistaa käyttöönoton tietoturvariskit ja varmistaa turvallinen siirtymä tuotantoon.
- Tietää, miten turvallisuus otetaan huomioon ohjelmiston elinkaaren aikana ja huolehtii tietoturvan siirtymisestä osaksi jatkuvaa hallintaa.

Kun turvallisuus huomioidaan alussa, säästytään ongelmilta lopussa.

TARPEEN MÄÄRITTELY JA SUUNNITTELU

Ohjelmistohankinnoista vastaavan tehtävänä on varmistaa, että liiketoiminnan tavoitteet, riskienhallinta ja tietoturvavaatimukset kulkevat käsi kädessä jo suunnittelun ja tarpeen määrittelyn vaiheissa, jolloin luodaan perusta koko ohjelmiston turvallisuudelle.

Ymmärtää ohjelmistoturvallisuuden vaikutuksen liiketoimintaan

Ohjelmistot ovat yhä useammin kriittinen osa liiketoimintaa, jolloin niiden turvallisuudella on suora vaikutus organisaation toiminnan jatkuvuuteen, asiakastyytyväisyyteen ja maineeseen. Ohjelmistoturvallisuus vaikuttaa suoraan organisaation kykyyn tuottaa palveluita luotettavasti ja suojata asiakasdataa. On tärkeää tiedostaa, että ohjelmistoturvallisuus ei ole pelkästään teknisiä ratkaisuja, vaan osa kokonaisvaltaista riskienhallintaa, joka kattaa myös prosessit, vastuut, osaamisen ja yhteistyön ohjelmiston koko elinkaaren ajan.

Osaa tunnistaa sääntelyn ja tietosuojan vaatimukset osana tarpeen määrittelyä

Ohjelmiston turvallisuusvaatimukset nousevat paitsi liiketoiminnan tarpeista myös lainsäädännöstä, viranomaisohjeista ja asiakkaiden odotuksista. Hankintavaiheessa on tärkeää tunnistaa, mitä sääntelyä ohjelmiston on noudatettava (esimerkiksi GDPR, NIS2-direktiivi, CRA ja mahdollinen alan erityissääntely). Kun vaatimukset tunnistetaan ajoissa ja niitä hyödynnetään hankintaprosessin ohjaamisessa, varmistetaan, että ohjelmisto palvelee alkuperäistä käyttötarkoitustaan ilman tarpeettomia rajoituksia tai myöhempiä muutostarpeita.

Ymmärtää riskienhallinnan merkityksen suunnittelun ja hankinnan alkuvaiheessa

Turvallisuuteen liittyviä riskejä voidaan hallita tehokkaimmin, kun ne tunnistetaan varhain. Riskienhallinta on keskeinen osa turvallisuuden suunnittelua, ja riskien tunnistaminen ja arviointi jo alkuvaiheessa auttaa kohdentamaan resursseja oikein. Riskienhallinta ohjaa valitsemaan ja priorisoimaan oikeat suojausmekanismit ja lisäksi tukee päätöksentekoa toimittajien arvioinnissa ja sopimusehdoissa.

Osaa laatia alustavat turvallisuusvaatimukset hankittavalle ohjelmistolle

Alustavat turvallisuusvaatimukset muodostavat perustan tarjouspyynnöille ja toimittajavalinnoille. Hankintavastaavan tulee osata määritellä riittävän selkeästi, mitä tietoturvalta odotetaan, jotta toimittajat voivat vastata vaatimuksiin. Tarvitaan myös kyky tunnistaa, mitkä vaatimukset ovat ehdottomia ja missä voidaan joustaa tuotteen ominaisuuksien rajoissa. Hyvin määritellyt vaatimukset ja selkeät vastuut tilaajan ja toimittajan välillä auttavat varmistamaan, että turvallisuus ei jää toimittajan tulkinnan varaan.

Tietää turvallisuuteen vaikuttavista teknisistä ja hallinnollisista ratkaisuista

Vaikka hankintavastaavan ei tarvitse hallita teknisiä yksityiskohtia, hänen tulee ymmärtää keskeiset ratkaisut, jotka vaikuttavat ohjelmiston turvallisuuteen. Tämä kattaa sekä tekniset ratkaisut, kuten palomuurit, haavoittuvuusskannerit, käyttöoikeuksien hallinnan ja salauksen, että hallinnolliset käytännöt, kuten käyttöoikeuspolitiikat, auditoinnit ja toimittajien turvallisuusarvioinnit. Lisäksi on tärkeää tunnistaa, miten valittu toimitusmalli, esimerkiksi pilvipalvelu, paikallinen asennus tai monitoimittajaympäristö, vaikuttaa tietoturvavastuisiin ja toteutustapoihin. Näiden kokonaisuuksien ymmärtäminen auttaa laatimaan parempia vaatimuksia ja arvioimaan toimittajien kyvykkyyttä jo ennen käyttöönottoa.

Ymmärtää eri osastojen yhteistyön merkityksen

Ohjelmistohankinta on monialainen prosessi, jossa tarvitaan eri osastojen asiantuntemusta, jotta kaikki tietoturvaan vaikuttavat näkökulmat tulevat huomioiduksi. Turvallisuusvaatimusten määrittelyssä tarvitaan yhteistyötä esimerkiksi IT:n, tietoturva-, tietosuoja-, lakiasiain- ja liiketoimintayksiköiden välillä. Ilman yhteistyötä voi syntyä puutteita, jotka johtavat turvallisuusaukkoihin, sääntelyriskien toteutumiseen ja kalliisiin korjaustoimenpiteisiin. Yhteistyö varmistaa, että hankinta tukee koko organisaation tavoitteita.

Keskeiset toimet:

- Tunnista hankinnan kohteen kriittisyys ja sen vaikutus turvallisuusvaatimusten tasoon.
- Käynnistä riskienarviointi ja tunnista keskeiset tietoturvariskit, jotka voivat vaikuttaa hankintaan tai myöhemmin ohjelmiston käyttöön.
- Varaa riittävästi osaamista ja aikaa sääntely- ja turvallisuusvaatimusten valmisteluun.
- Selvitä ja dokumentoi ohjelmistoon sovellettava sääntely ja tietosuojavaatimukset yhteistyössä asiantuntijoiden kanssa.
- Laadi alustavat tietoturva- ja tietosuojavaatimukset osaksi hankintasuunnitelmaa ja määrittelydokumentteja.
- Varmista, että turvallisuusvaatimukset ovat ymmärrettäviä ja mitattavia, jotta ne voidaan sisällyttää sopimuksiin ja arvioida toimittajien kyvykkyyttä.
- Tee yhteistyötä eri asiantuntijoiden ja liiketoimintayksiköiden kanssa, jotta kaikki näkökulmat tulevat huomioiduksi.
- Arvioi toimittajien turvallisuuskyvykkyyttä myös hallinnollisten käytäntöjen, kuten auditointien ja poikkeamienhallinnan, näkökulmasta.

TOIMITTAJAN ARVIOINTI JA VALINTA

Ohjelmistohankinnoista vastaavan on osattava arvioida toimittajien tietoturvakyvykkyyttä, toimitusmallien riskejä ja elinkaaren aikaista tukea kokonaisuutena. Tässä vaiheessa varmistetaan, että valittu toimittaja pystyy tuottamaan ja ylläpitämään ohjelmistoa turvallisesti sekä täyttämään organisaation vaatimukset koko sopimuskauden ajan.

Ymmärtää toimittajan tietoturvakyvykkyyden merkityksen

Hankintavastaavan tulee ymmärtää, mitä toimittajan tietoturvakyvykkyys tarkoittaa kokonaisuutena. Kyvykkyys ei rajoitu tekniseen osaamiseen, vaan siihen sisältyvät toimittajan sisäiset prosessit, auditointikäytännöt, jatkuvuudenhallinnan suunnitelmat sekä kyky toimia sääntelyn ja tietosuojan edellyttämällä tasolla. Tietoturvastandardit, kuten ISO/IEC 27001, tarjoavat hyvän viitekehyksen, mutta laadukas ja turvallinen toiminta on mahdollista myös ilman sertifikaatteja, jos tietoturvakäytännöt ovat systemaattisia ja läpinäkyviä. Lisäksi on tärkeää arvioida, miten toimittaja osoittaa sitoutumisensa turvallisuuteen käytännössä. Näiden osa-alueiden ymmärtäminen auttaa muodostamaan realistisen kuvan siitä, onko toimittajalla kyky tuottaa ja ylläpitää turvallista ohjelmistoa koko sen elinkaaren ajan.

Osaa arvioida toimittajan kyvykkyyttä täyttää ohjelmiston turvallisuusvaatimukset

Hankintavastaavan tulee arvioida, kykeneekö toimittaja vastaamaan ohjelmistoratkaisun tietoturvavaatimuksiin. Tämä edellyttää oikeiden kysymysten esittämistä tarjouspyynnöissä ja arviointikriteereissä sekä toimittajan käytäntöjen tarkastelua: turvallisen kehityksen periaatteiden noudattaminen, haavoittuvuuksien hallinta, poikkeamatilanteisiin reagointi ja kolmansien osapuolten komponenttien hallinta. Arvioinnissa voidaan hyödyntää myös julkisesti saatavilla olevia lähteitä, kuten haavoittuvuustietokantoja (esim. CVE), jotka tarjoavat konkreettista tietoa toimittajan ohjelmistojen turvallisuushistoriasta ja reagointikyvystä. Arvioinnissa on tärkeää huomioida myös toimittajan tausta, referenssit, taloudellinen tilanne ja kokemus vastaavanlaisten ratkaisujen toimittamisesta. Näiden tietojen avulla voidaan muodostaa luotettava kokonaiskuva toimittajan kyvystä toteuttaa turvallinen ohjelmisto käytännössä.

Tietoturva ei ole lupaus vaan osoitettavaa osaamista.

Osaa tunnistaa riskit toimittajan toimitusmallissa ja miten se vaikuttaa vastuunjakoon

Toimittajan toimitusmalli vaikuttaa suoraan siihen, miten vastuut ja riskit jakautuvat organisaation ja toimittajan välillä. Hankintavastaavan tulee tunnistaa, millaisia riskejä liittyy esimerkiksi pilvipalveluihin, ulkoistettuihin ratkaisuihin tai monitoimittajaympäristöihin. On tärkeää ymmärtää, missä kohtaa toimittaja vastaa tietoturvasta ja missä kohtaa vastuu siirtyy organisaatiolle. Tämä auttaa varmistamaan, että riskit eivät jää epäselviksi tai hallitsemattomiksi, ja että sopimuksissa voidaan myöhemmin määritellä vastuut selkeästi.

Ymmärtää toimittajariippuvuuden ja elinkaaren aikaisen tuen merkityksen turvallisuudelle

Toimittajan valinta vaikuttaa ohjelmiston turvallisuuteen koko sen elinkaaren ajan, ja hankintavaiheessa onkin arvioitava, kuinka pitkäaikainen ratkaisu on kyseessä. Hankintavastaavan tulee ymmärtää, miten toimittajan tarjoama tekninen ratkaisu tukee organisaation tietoturvapolitiikkaa ja miten riippuvuus toimittajasta voi vaikuttaa tuleviin muutoksiin, ylläpitoon ja tukeen. Jos toimittaja ei pysty tarjoamaan pitkäaikaista tukea tai ei reagoi nopeasti uusiin uhkiin, ohjelmiston turvallisuus voi heikentyä ajan myötä. Siksi on tärkeää arvioida toimittajan kykyä ylläpitää ja kehittää ratkaisua turvallisesti myös vuosien päästä.

Myös riippuvuus yhdestä toimittajasta voi lisätä riskejä, jos toimittajan tuki, päivitykset tai liiketoiminta loppuvat tai heikkenevät. On hyvä tunnistaa, onko ohjelmisto helposti siirrettävissä toiselle toimittajalle tai ylläpidettävissä itsenäisesti, jos toimittajasuhde päättyy.

Osaa hyödyntää asiantuntijoita ja vertailla vaihtoehtoja turvallisuusnäkökulmasta

Ei voida olettaa, että kaikilla hankintavastaavilla olisi syvällistä tietoturvaosaamista. On tärkeää tunnistaa, milloin tarvitaan mukaan organisaation tietoturva-asiantuntijoita tai ulkopuolista asiantuntemusta, esimerkiksi teknisten ratkaisujen arviointiin tai riskien mallintamiseen. Tämä korostuu erityisesti laajoissa tai liiketoimintakriittisissä hankinnoissa.
Hankintavastaavan tulee ymmärtää, miten eri toimittajien ratkaisut eroavat toisistaan turvallisuusnäkökulmasta ja varmistaa, että arviointiin käytetään riittävää asiantuntemusta. Vaikka teknisten ja hallinnollisten tietoturvatietojen tulkinta voi vaatia erityisosaamista, hankintavastaava vastaa siitä, että turvallisuusnäkökulma ohjaa valintaa hinnan ja toiminnallisuuksien rinnalla.

Keskeiset toimet:

- Arvioi toimittajan tietoturvakyvykkyyttä kokonaisuutena ja systemaattisesti, mukaan lukien prosessit, sertifikaatit, auditoinnit ja sääntelyn noudattaminen.
- Selvitä toimittajan maine, tausta, taloudellinen tilanne ja kokemus vastaavista ratkaisuista.
- Varmista, että toimittaja hallitsee haavoittuvuudet ja reagoi poikkeamatilanteisiin tehokkaasti.
- Tunnista ja dokumentoi toimitusmallin tietoturvariskit ja vastuunjaon vaikutukset tietoturvaan, erityisesti pilvi- ja ulkoistusratkaisuissa.
- Arvioi ja dokumentoi toimittajariippuvuuden vaikutukset elinkaaren aikaisen turvallisuuteen.
- Varmista, että mukana on tarvittaessa organisaation omia tai ulkopuolisia tietoturva-asiantuntijoita.
- Varmistaa, että turvallisuus sisältyy valintakriteereihin eikä jää pelkkien teknisten ominaisuuksien tai kustannusten varaan.
- Dokumentoi valintaperusteet ja turvallisuuteen liittyvät päätökset.

SOPIMUKSEN LAADINTA

Ohjelmistohankinnoista vastaavan tehtävänä on varmistaa, että toimittajan vastuut, raportointivelvoitteet ja riskienhallintamekanismit määritellään selkeästi ja mitattavasti. Näin luodaan sopimuksellinen perusta, joka tukee tietoturvan toteutumista koko ohjelmiston elinkaaren ajan.

Osaa konkretisoida tietoturvavaatimukset sopimukseen

Hankintavastaavan tulee osata muuttaa tietoturvavaatimukset selkeiksi, mitattaviksi ja sopimuksellisesti velvoittaviksi ehdoiksi. Hankintavastaavan on ymmärrettävä, miten organisaation omien tietoturvavaatimusten, sovellettavien standardien ja sääntelyn (esim. GDPR, CRA, NIS2) tulee ohjata sopimussisältöä. Lisäksi tulee määritellä dokumentointivelvoitteet, joilla varmistetaan, että toimittaja raportoi tietoturvan toteutumisesta läpinäkyvästi ja säännöllisesti. Sopimukseen on myös syytä sisällyttää mekanismi, jolla tietoturvaehdot voidaan päivittää, jos sääntely, riskit tai vaatimukset muuttuvat ohjelmiston elinkaaren aikana.

Osaa määritellä toimittajan tietoturvavelvoitteet

Sopimuksessa on tärkeää kuvata toimittajan vastuut koko ohjelmiston elinkaaren ajalle. Tämä kattaa tietoturvan ylläpidon, päivitykset, haavoittuvuuksien hallinnan, tietoturvaloukkausten käsittelyn ja virheiden korjaamisen. Hankintavastaavan tulee osata neuvotella myös auditointioikeuksista, alihankkijoiden hallinnasta ja sopimusrikkomusten seuraamuksista. Selkeä vastuunjako auttaa varmistamaan, että tietoturva ei jää epäselväksi tai toimittajan harkinnan varaan.

Osaa hallita tietoturvariskejä sopimusehtojen kautta

Sopimuksella voidaan hallita tietoturvariskejä, mutta se edellyttää ymmärrystä siitä, miten toimittajan tietoturvakäytännöt ja kypsyystaso vaikuttavat kokonaisriskiin. Hankintavastaavan tulee osata arvioida, millaisia riskejä sopimuksella voidaan rajata, siirtää tai hallita, ja miten nämä kirjataan sopimukseen selkeästi ja vaikuttavasti.

Kyky toimia yhteistyössä sidosryhmien kanssa sopimuksen laadinnassa

Tietoturvaehdot vaativat tiivistä yhteistyötä sopimusjuristien, tietoturva-asiantuntijoiden ja toimittajan kanssa. Hankintavastaavan tulee osata kommunikoida tietoturvavaatimukset selkeästi ja varmistaa, että ne kirjataan sopimukseen yksiselitteisesti ja ilman tulkinnanvaraa. Hyvä yhteistyö varmistaa, että sopimus tukee organisaation tietoturvatavoitteita ja on juridisesti pätevä.

Keskeiset toimet:

- Määrittele tietoturvavaatimukset selkeästi ja mitattavasti sopimukseen.
- Käytä standardeja, sääntelyvaatimuksia ja organisaation tietoturvaperiaatteita ohjaamaan sopimussisältöä.
- Kirjaa toimittajan vastuut ohjelmiston koko elinkaaren ajalta.
- Sisällytä sopimukseen auditointioikeudet, alihankkijoiden hallinta ja seuraamukset rikkomuksista.
- Arvioi tietoturvariskit ja hallitse riskejä sopimusehtojen kautta.
- Tee tiivistä yhteistyötä eri asiantuntijoiden kanssa sopimuksen muotoilussa.

Hyvä valmistelu tekee tietoturvasta todennettavaa, ei toivottavaa.

TOIMITUKSEN JA KÄYTTÖÖNOTON VALMISTELU

Ohjelmistohankinnoista vastaavan tehtävänä on varmistaa, että tietoturvaa koskevat velvoitteet ja menettelyt on määritelty ja siirretty selkeästi toimitus- ja käyttöönottovaiheeseen. Näin varmistetaan, että sovitut vaatimukset toteutuvat hallitusti ja että tietoturva jatkuu saumattomasti osana ohjelmiston ylläpitoa ja jatkokehitystä.

Osaa varmistaa tietoturvavaatimusten toteutumisen ennen käyttöönottoa

Käyttöönoton valmistelussa tulee varmistaa, että sopimusvaiheessa sovitut tietoturvavaatimukset on kytketty konkreettisesti toimitussuunnitelmaan ja toteutettu käytännössä. Tämä edellyttää dokumentaation, testitulosten ja selvitysten läpikäyntiä sekä mahdollisesti käyttöönottotarkastuksen toteuttamista. Hankintavastaavan tulee myös varmistaa, että toimitukseen sisältyvät ajantasaiset ohjeet, hallintaprosessit ja lokienhallinnan käytännöt, jotka tukevat turvallista käyttöönottoa. Tarkastuslistojen hyödyntäminen auttaa varmistamaan, että mikään kriittinen vaatimus ei jää huomiotta.

Tunnistaa käyttöönoton tietoturvariskit

Käyttöönottoon liittyy monia teknisiä ja organisatorisia riskejä, jotka on tunnistettava ennen tuotantokäyttöä. Näihin kuuluvat esimerkiksi oletusasetusten hallinta, käyttöoikeuksien ja pääsynvalvonnan tarkistaminen, haavoittuvuuksien tunnistaminen sekä integraatiot muiden järjestelmien kanssa. Riskien arviointi, testaus ja tarvittaessa auditointi ennen tuotantoon siirtymistä on olennaista, jotta tarvittavat turvatoimet voidaan suunnitella ja tietovuodot tai luvattomat muutokset ehkäistä tehokkaasti. Koska käyttöönoton yhteydessä voi ilmetä tietoturvapoikkeamia, on poikkeamien hallintaan jo tässä vaiheessa oltava selkeät prosessit, vastuut ja eskalointipolut.

Ymmärtää turvallisen käyttöönottoprosessin periaatteet

Turvallinen käyttöönotto edellyttää suunnitelmallisuutta, selkeitä vastuita ja riittäviä valvontamekanismeja. Hankintavastaavan tulee varmistaa, että käyttöönottoprosessi on tietoturvan näkökulmasta hallittu ja että tarvittavat resurssit ja osaaminen ovat käytettävissä. Lisäksi on tärkeää huolehtia tietoturvan siirtymisestä osaksi jatkuvaa hallintaa siirtämällä vastuut selkeästi nimetyille henkilöille tai rooleille, kuten tuoteomistajille, ylläpitotiimille tai muulle jatkovastuulliselle taholle.

Ymmärtää ylläpidon ja jatkuvuuden tietoturvaedellytykset

Hankintavastaavan ei tarvitse suunnitella ylläpidon teknisiä yksityiskohtia, mutta hänen on tärkeää huolehtia tietoturvavastuiden siirtymisestä osaksi jatkuvaa hallintaa. Hankintavastaavan on varmistettava, että toimittajalla on käytössään toimivat prosessit päivitysten hallintaan, haavoittuvuuksien seurantaan ja käyttöönoton jälkeiseen tukeen. Lisäksi on huolehdittava, että järjestelmässä on käytössä riittävät valvontamekanismit ja että tietoturvaan liittyvä dokumentaatio siirtyy selkeästi osaksi tuotannon hallintaa ja on ylläpitotiimin saatavilla. Näin varmistetaan tietoturvan saumaton jatkuvuus ja seuranta.

Keskeiset toimet:

- Kytke sopimuksessa sovitut tietoturvavaatimukset toimitussuunnitelmaan.
- Varmista dokumentaation ja tarkastusten avulla, että tietoturvavaatimukset on toteutettu sovitusti.
- Tunnista ja arvioi käyttöönottoon liittyvät tietoturvariskit.
- Varmista riittävän osaamisen ja tuen turvalliseen käyttöönottoon.
- Siirrä tietoturvavastuut selkeästi osaksi jatkuvaa hallintaa.

Ohjelmistokehityksen tilaaja

Tässä osiossa käsitellään, millaista tietoturvaosaamista ohjelmistokehityksen tilaajalta edellytetään ohjelmiston elinkaaren eri vaiheissa ja miten hän voi omalla roolillaan käytännössä edistää ohjelmistoturvallisuutta.

MIKSI OHJELMISTOTURVALLISUUS KUULUU OHJELMISTON TILAAJALLE?

Ohjelmiston turvallisuus ei synny sattumalta eikä sitä voi lisätä jälkikäteen, vaan se rakennetaan osaksi ohjelmistoa alusta asti. Tilaajalla on keskeinen vastuu siitä, millaisia vaatimuksia kehitystyölle asetetaan ja miten turvallisuutta ohjataan koko kehitysprosessin ajan.

Tilaaja määrittää suunnan myös tietoturvassa.

Tiivistelmä

TILAAJAN OSAAMISTARPEET

- Ymmärtää ohjelmistoturvallisuuden merkityksen liiketoiminnassa, riskienhallinnassa ja jatkuvuudessa.
- Tunnistaa sääntelyn ja tietosuojan vaikutukset ohjelmistoon ja ohjelmistokehitykseen.
- Ymmärtää, miten ohjelmiston turvallisuus muodostuu.
- Osaa määritellä selkeät turvallisuusvaatimukset kehitykselle ja varmistaa niiden toteutumisen.
- Osaa arvioida toimittajan tietoturvakyvykkyyttä, ja tuntee toimittajavalinnan ja sopimusneuvottelun keskeiset turvallisuusnäkökulmat.
- Osaa asettaa perustellut tietoturvavaatimukset toimittajalle ja tunnistaa toimittajan rooli ja vastuut tietoturvan toteutumisessa.
- Ymmärtää riskienhallinnan merkityksen tilausprosessissa ja osaa käyttää sitä päätöksenteon tukena.
- Ymmärtää yhteistyön merkityksen eri asiantuntijoiden kanssa tilaus- ja kehitysprosessin aikana.
- Tunnistaa käyttöönoton tietoturvariskit ja osaa valmistella ja valvoa turvallista toimitusta ja käyttöönottoa.
- Osaa siirtää tietoturvan osaksi jatkuvaa hallintaa.

Tilaaja ohjaa turvallisuutta.

Kun ohjelmisto tilataan organisaation tarpeisiin kehitettäväksi, tilaaja vaikuttaa suoraan siihen, mitä ratkaisuja toteutetaan, miten tietoa käsitellään ja kuinka turvallisuus otetaan huomioon suunnittelussa, toteutuksessa, testauksessa ja käyttöönotossa. Tilaajan osaaminen ja päätökset määrittävät pitkälti sen, syntyykö järjestelmästä aidosti turvallinen ja elinkaaren mittaisiin tarpeisiin vastaava.

Tilaajan ei tarvitse ratkaista teknisiä yksityiskohtia itse, mutta hänen on osattava asettaa olennaiset tietoturvavaatimukset, huolehdittava jatkuvuudesta, tunnistettava vastuunjako ja varmistettava, että toimittaja ymmärtää turvallisuustavoitteet. Myös sopimuksilla ja yhteistyön rakenteilla on suuri merkitys: ne ohjaavat kehityksen laatua ja mahdollistavat tarvittavat muutokset, auditoinnit ja ylläpidon.

Tilaaja ei siis vain pyydä ohjelmistoa. Hän määrittää, millaiseen riski- ja laatutasoon organisaatio sitoutuu. Turvallisuus syntyy yhdessä suunnittelemalla, valvomalla ja vaatimalla.

TARPEEN MÄÄRITTELY JA SUUNNITTELU

Ohjelmistokehityksen tilaajan tehtävänä on varmistaa, että tietoturva sisältyy suunnitteluun ja vaatimustenmäärittelyyn jo ennen kehitystyön käynnistämistä. Tilaajan on tunnistettava liiketoiminnan, sääntelyn ja riskienhallinnan näkökulmasta keskeiset tietoturvavaatimukset ja huolehdittava, että ne ohjaavat kehityksen ratkaisuja ja toimittajavalintoja alusta asti.

Ymmärtää ohjelmistoturvallisuuden vaikutuksen liiketoimintaan

Ohjelmistot ovat yhä useammin kriittinen osa liiketoimintaa, jolloin niiden turvallisuudella on suora vaikutus organisaation jatkuvuuteen, asiakastyytyväisyyteen ja maineeseen. Ohjelmistoturvallisuus vaikuttaa suoraan organisaation kykyyn tuottaa palveluita luotettavasti ja suojata asiakasdataa. On tärkeää ymmärtää, että ohjelmistoturvallisuus ei ole vain tekninen kysymys, vaan olennainen osa kokonaisvaltaista riskienhallintaa, joka ulottuu kehitysprosessiin, vastuunjakoon, osaamiseen ja yhteistyöhön koko ohjelmiston elinkaaren ajan.

Osaa tunnistaa sääntelyn ja tietosuojan vaatimukset osana tarpeen määrittelyä

Ohjelmiston turvallisuusvaatimukset nousevat paitsi liiketoiminnan tarpeista myös lainsäädännöstä, viranomaisohjeista ja asiakkaiden odotuksista. Ennen kehitystyön alkamista on tunnistettava, mitä sääntelyä ohjelmiston on noudatettava (esimerkiksi GDPR, NIS2-direktiivi, CRA ja mahdollinen alan erityissääntely). Näiden vaatimusten huomioiminen varhaisessa vaiheessa varmistaa, että kehitystyö etenee oikeilla reunaehdoilla ja ilman myöhempiä korjaustarpeita.

Ymmärtää riskienhallinnan merkityksen suunnittelun ja kehityksen alkuvaiheessa

Turvallisuusriskit tulee tunnistaa ja arvioida jo suunnitteluvaiheessa, jotta ne voidaan hallita tehokkaasti. Tilaajan tulee ymmärtää, miten riskien arviointi vaikuttaa suunnitteluratkaisuihin, teknologioiden valintaan ja resurssien kohdentamiseen. Riskienhallinta tukee päätöksentekoa ja ohjaa suojausmekanismien valintaa koko kehitysprosessin ajan.

Osaa laatia alustavat turvallisuusvaatimukset hankittavalle ohjelmistolle

Tilaajan tulee määritellä selkeät ja mitattavat tietoturvavaatimukset, jotka sisältyvät suoraan suunnitteluun ja ohjeaavat kehitystyötä alusta alkaen. Vaatimusten tulee kattaa keskeiset osa-alueet, kuten arkkitehtuuri, käyttöoikeuksien hallinta, lokitus, haavoittuvuuksien hallinta ja tietosuoja. Hyvin määritellyt vaatimukset varmistavat, että tietoturva ei jää kehittäjän tulkinnan varaan, ja että sen toteutuminen voidaan todentaa esimerkiksi testauksen, katselmointien ja dokumentaation avulla. Tilaajan tulee varmistaa, että tietoturvavaatimukset eivät jää pelkästään kirjallisiksi tavoitteiksi, vaan ne toimivat konkreettisina hyväksymiskriteereinä ohjelmiston kehitystyön arvioinnissa

Ymmärtää turvallisen ohjelmistokehityksen periaatteet

Tilaajan ei tarvitse hallita ohjelmointityön yksityiskohtia, mutta hänen on tärkeää ymmärtää turvallisen ohjelmistokehityksen keskeiset periaatteet. Tämä kattaa suunnittelun, koodauksen, testauksen ja julkaisun vaiheet, joihin tietoturva tulee sisällyttää järjestelmällisesti. Tilaajan on osattava vaatia, että kehityksessä noudatetaan turvallisen kehityksen periaatteita, kuten vähimmän oikeuden periaatetta, syvyyssuuntaista suojausta, syötteiden validointia, lokitusta sekä haavoittuvuuksien ja riippuvuuksien hallintaa. Lisäksi tilaajan tulee ymmärtää kehitysmallien, kuten DevSecOpsin, merkitys: tietoturva ei ole erillinen vaihe, vaan osa jatkuvaa kehitysprosessia, jossa turvallisuusautomaatio, testaus ja valvonta integroidaan osaksi CI/CD-putkea. Näiden periaatteiden ymmärtäminen auttaa ohjaamaan kehitystä niin, että lopputulos on turvallinen ja elinkaaren mittaisiin vaatimuksiin vastaava.

Tietää turvallisuuteen vaikuttavista teknisistä ja hallinnollisista ratkaisuista

Vaikka tilaajan ei tarvitse hallita kaikkia teknisiä yksityiskohtia, hänen tulee ymmärtää keskeiset turvallisuusratkaisut, joita kehityksessä voidaan hyödyntää, kuten salaus, tietoturvatestaukset, pääsynhallintajärjestelmät ja jatkuva haavoittuvuuksien skannaus. Lisäksi on tärkeää tunnistaa hallinnolliset käytännöt, kuten tietoturvakatselmoinnit, auditoinnit ja toimittajan tietoturvaprosessit. Näiden tuntemus auttaa tilaajaa tekemään perusteltuja valintoja kehitysratkaisujen ja toimittajien välillä.

Osaa toimia yhteistyössä eri asiantuntijoiden kanssa

Kehityshankkeen onnistuminen edellyttää tiivistä yhteistyötä eri sidosryhmien välillä. Turvallisuusvaatimusten määrittelyyn tarvitaan panos esimerkiksi IT:ltä, tietoturva- ja tietosuojatiimeiltä, lakiasioista sekä liiketoimintayksiköiltä. Tilaajan on varmistettava, että nämä näkökulmat yhdistyvät yhtenäiseksi vaatimuskokonaisuudeksi, jolloin vältetään tietoturva-aukot ja varmistetaan ohjelmiston soveltuvuus liiketoiminnan tarpeisiin.

Keskeiset osaamistarpeet:

- Tunnista ohjelmistoturvallisuuden liiketoimintavaikutukset ja sisällytä ne hankinnan tavoitteisiin.
- Selvitä soveltuva sääntely, tietosuojavaatimukset ja alan standardit jo suunnitteluvaiheessa.
- Arvioi ja dokumentoi keskeiset turvallisuusriskit ja huomioi ne suunnittelussa.
- Määritä selkeät, mitattavat ja kattavat tietoturvavaatimukset niin ohjelmistolle kuin kehitystyölle.
- Edellytä turvallisen ohjelmistokehityksen periaatteiden noudattamista ja että tietoturvavaatimukset toimivat kehitystyön hyväksymiskriteereinä.
- Selvitä ohjelmiston ja sen kehityksen kannalta keskeiset tekniset ja hallinnolliset turvallisuusratkaisut.
- Tee yhteistyötä eri asiantuntijoiden kanssa ja kokoa näkemykset yhtenäiseksi vaatimuskokonaisuudeksi.

Oikea toimittaja suojaa muutakin kuin koodia – se suojaa liiketoimintaa.

TOIMITTAJAN ARVIOINTI JA VALINTA

Ohjelmistokehityksen tilaajan tehtävänä on varmistaa, että toimittajan tietoturvakyvykkyys, riskienhallinta ja kehitysprosessit vastaavat organisaation vaatimuksia. Tilaajan on osattava arvioida toimittajan toimintatapoja ja pitkäaikaisia valmiuksia turvallisuuden näkökulmasta, jotta valittu kumppani tukee ohjelmiston turvallista kehitystä ja ylläpitoa koko sen elinkaaren ajan.

Ymmärtää toimittajan tietoturvakyvykkyyden merkityksen

Tilaajan tulee hahmottaa, mitä toimittajan tietoturvakyvykkyys tarkoittaa kokonaisuutena. Kyvykkyys ei rajoitu tekniseen osaamiseen, vaan sisältää myös sisäiset prosessit, tietoturvastandardien noudattamisen (esim. ISO/IEC 27001), auditointikäytännöt, jatkuvuudenhallinnan sekä kyvyn toimia sääntelyn ja tietosuojan edellyttämällä tasolla. Lisäksi on tärkeää arvioida toimittajan organisaatiokulttuuria ja sitoutumista turvallisuuteen – onko tietoturva aidosti osa toimintaa vai pelkkä muodollisuus? Tämä kokonaiskuva auttaa arvioimaan, pystyykö toimittaja tuottamaan ja ylläpitämään turvallista ohjelmistoa koko sen elinkaaren ajan.

Ymmärtää toimittajan riskiprofiilin merkityksen valinnassa

Toimittajaan liittyvät tietoturvariskit tulee tunnistaa ja arvioida ennen sopimuksen solmimista. Riskiprofiili muodostuu muun muassa toimittajan käyttämistä teknologioista, kolmansien osapuolten komponenttien ja palveluiden riippuvuuksista, pilvipalveluiden arkkitehtuurista, tiedon sijainnista ja käsittelykäytännöistä sekä toimittajan historiasta tietoturvapoikkeamien osalta. Näiden tekijöiden ymmärtäminen tukee perusteltua päätöksentekoa, auttaa välttämään turvallisuuteen liittyviä yllätyksiä myöhemmissä vaiheissa ja varmistaa, että valittu toimittaja tukee organisaation riskinsietokykyä ja liiketoiminnan jatkuvuutta.

Osaa arvioida kehitystyön tietoturvakäytännöt ja suojausratkaisut

Tilaajan on pystyttävä arvioimaan, miten tietoturva on sisällytetty toimittajan kehitysprosessiin. Tämä kattaa muun muassa turvallisen kehityksen periaatteiden noudattamisen, testaus- ja päivityskäytännöt, haavoittuvuuksien hallinnan, CI/CD-putken turvallisuusautomaation sekä kolmansien osapuolten komponenttien hallinnan. Arvioinnissa on huomioitava myös tekniset ja hallinnolliset suojausratkaisut, datan salaus, pääsynhallinta, haavoittuvuustestaus, auditoinnit, katselmoinnit ja riskienhallinta. Näin voidaan tunnistaa konkreettisesti, miten tietoturva näkyy konkreettisina ja todennettavina toimintatapoina kehityksen eri vaiheissa.

Osaa arvioida toimittajan dokumentaation ja raportoinnin laatua

Tilaajan tulee osata arvioida, miten toimittaja dokumentoi tietoturvakäytännöt, raportoi riskeistä ja osoittaa vaatimusten täyttymistä. Hyvin tuotettu dokumentaatio tukee läpinäkyvyyttä, mahdollistaa valvonnan ja toimii perustana hyväksynnälle, auditoinneille ja jatkuvalle kehitykselle. Dokumentaation laatu kertoo myös toimittajan kyvystä hallita tietoturvaa järjestelmällisesti ja osoittaa sen toteutumista käytännössä.

Ymmärtää toimittajariippuvuuden ja pitkäaikaisen tuen merkityksen turvallisuudelle

Toimittajan valinta vaikuttaa ohjelmiston tietoturvaan koko sen elinkaaren ajan. On tärkeää arvioida, miten kehitettävä ohjelmisto tukee oman organisaation tietoturvapolitiikkaa ja kuinka riippuvuus toimittajasta vaikuttaa muutoksiin, ylläpitoon ja tukeen. Jos toimittaja ei pysty tarjoamaan pitkäaikaista tukea, julkaisemaan säännöllisiä päivityksiä tai reagoimaan nopeasti uusiin haavoittuvuuksiin, ohjelmiston tietoturva heikentyy ajan kuluessa. Lisäksi on syytä selvittää, voiko ohjelmiston ylläpitoa jatkaa itsenäisesti tai siirtää toiselle toimittajalle, jos alkuperäisen toimittajan tuki tai liiketoiminta lakkaa.

Osaa hyödyntää asiantuntijoita ja vertailla vaihtoehtoja turvallisuusnäkökulmasta

Koska kaikilla tilaajilla ei ole syvällistä tietoturvaosaamista, on tärkeää tunnistaa, milloin tarvitaan organisaation tietoturva-asiantuntijoita tai ulkopuolista apua esimerkiksi teknisten ratkaisujen arviointiin tai riskien mallintamiseen. Tämä korostuu erityisesti laajoissa ja liiketoimintakriittisissä ohjelmistohankinnoissa.

Keskeiset osaamistarpeet:

- Arvioi toimittajan tietoturvakyvykkyys kokonaisuutena, mukaan lukien prosessit, sertifioinnit, auditointikäytännöt ja organisaation sitoutuminen turvallisuuteen.
- Tunnista ja arvioi toimittajaan liittyvät tietoturvariskit.
- Varmista, että kehitystyön tietoturvakäytännöt ja suojausratkaisut kattavat koko kehitysprosessin ja ovat dokumentoituja.
- Arvioi toimittajan dokumentaation ja raportoinnin laatu ja varmista, että tietoturvakäytännöt ja riskienhallinta on kuvattu selkeästi ja läpinäkyvästi.
- Varmista toimittajan kyky tarjota pitkäaikaista tukea ja ylläpitoa.
- Selvitä mahdollisuus ohjelmiston itsenäiseen ylläpitoon tai siirtoon toiselle toimittajalle.
- Hyödynnä organisaation asiantuntijoita tai ulkopuolista apua tarvittaessa, ja vertaile vaihtoehtoja tietoturvan näkökulmasta.

SOPIMUKSEN LAADINTA

Ohjelmistokehityksen tilaajan tehtävänä on varmistaa, että tietoturvavaatimukset konkretisoidaan sopimuksessa selkeiksi ja velvoittaviksi ehdoiksi. Tilaajan on huolehdittava, että vastuut, raportointivelvoitteet ja riskienhallintakeinot kattavat koko ohjelmiston elinkaaren, jotta tietoturva pysyy hallittuna kehityksestä ylläpitoon asti.

Osaa konkretisoida tietoturvavaatimukset sopimukseen

Tilaajan tulee osata muotoilla tietoturvavaatimukset selkeiksi, mitattaviksi ja sopimuksellisesti velvoittaviksi ehdoiksi, jotka ohjaavat kehitystyötä alusta alkaen. Tämä tarkoittaa ymmärrystä siitä, miten organisaation omat vaatimukset, sovellettavat standardit ja sääntely (esim. GDPR, CRA, NIS2) vaikuttavat sopimussisältöön. Lisäksi tulee määritellä dokumentointi- ja raportointivelvoitteet, joiden avulla toimittaja osoittaa tietoturvan toteutumisen jo kehitystyön aikana läpinäkyvästi ja säännöllisesti. Sopimukseen on myös syytä sisällyttää mekanismi, jolla tietoturvaehdot voidaan päivittää, jos sääntely, riskit tai vaatimukset muuttuvat ohjelmiston elinkaaren aikana.

Sopimus ohjaa ja varmistaa turvallisen toiminnan koko sopimussuhteen ajan.

Osaa määritellä toimittajan tietoturvavelvoitteet koko elinkaarelle

Sopimuksessa tulee kuvata toimittajan vastuut tietoturvan osalta koko ohjelmiston elinkaaren ajan. Tämä kattaa kehitystyön aikaisen tietoturvan toteuttamisen, päivityskäytännöt, haavoittuvuuksien hallinnan, poikkeamien käsittelyn ja virheiden korjaamisen. Tilaajan tulee osata neuvotella myös auditointioikeuksista, alihankkijoiden hallinnasta ja sopimusrikkomusten seuraamuksista. Selkeä vastuunjako varmistaa, että tietoturva ei jää epäselväksi tai toimittajan harkinnan varaan.

Sopimuksella voidaan myös varmistaa, että ohjelmisto ja sen dokumentaatio toteutetaan siten, että tarvittaessa ohjelmisto on siirrettävissä toiselle toimittajalle tai omaan ylläpitoon ilman kohtuutonta riskiä tietoturvan heikkenemisestä.

Osaa hallita tietoturvariskejä sopimusehtojen avulla

Tilaajan tulee ymmärtää, miten sopimusehdoilla voidaan rajata, siirtää tai hallita tietoturvariskejä, jotka liittyvät toimittajan kyvykkyyteen, kehityskäytäntöihin ja järjestelmän ylläpitoon. Tämä edellyttää kykyä arvioida toimittajan tietoturvakäytäntöjen kypsyystasoa ja kirjata sopimukseen ehtoja, jotka suojaavat organisaatiota esimerkiksi toimittajan laiminlyönneiltä, viivästyksiltä tai tietoturvapoikkeamilta.

Kyky toimia yhteistyössä sidosryhmien kanssa sopimuksen laadinnassa

Tietoturvaehdot edellyttävät tiivistä yhteistyötä sopimusjuristien, tietoturva-asiantuntijoiden ja toimittajan kanssa. Tilaajan tulee osata kommunikoida vaatimukset selkeästi ja varmistaa, että ne kirjataan sopimukseen yksiselitteisesti ilman tulkinnanvaraa. Hyvä yhteistyö varmistaa, että sopimus tukee tietoturvan toteutumista kehitystyössä ja sen jälkeen.

Keskeiset toimet:

- Määrittele tietoturvavaatimukset selkeästi ja mitattavasti sopimukseen.
- Käytä standardeja, sääntelyvaatimuksia ja organisaation tietoturvaperiaatteita ohjaamaan sopimussisältöä.
- Kirjaa toimittajan vastuut ohjelmiston koko elinkaaren ajalta.
- Sisällytä sopimukseen auditointioikeudet, alihankkijoiden hallinta ja seuraamukset rikkomuksista.
- Arvioi tietoturvariskit ja hallitse riskejä sopimusehtojen kautta.
- Tee tiivistä yhteistyötä eri asiantuntijoiden kanssa sopimuksen muotoilussa.

Seuraa, arvioi ja reagoi.

Suunnitelmallisuus ja selkeät vastuut turvaavat ohjelmiston siirtymän tuotantoon.

KEHITYSTYÖN OHJAUS JA SEURANTA

Ohjelmistokehityksen tilaajan tehtävänä on varmistaa, että tietoturva pysyy kehitystyön keskiössä ja etenee suunniteltujen vaatimusten mukaisesti. Tilaajan on seurattava tietoturvan toteutumista, ohjattava poikkeamien käsittelyä ja ylläpidettävä yhteistyötä kehitystiimin ja asiantuntijoiden kanssa, jotta tietoturva kehittyy jatkuvasti osana ohjelmiston laatua.

Osaa seurata ja arvioida tietoturvan toteutumista suhteessa vaatimuksiin

Tilaajan tulee osata verrata kehitystyön etenemistä sovittuihin tietoturvavaatimuksiin ja ymmärtää, että tietoturva ei ole staattinen tila, vaan kehittyvä osa ohjelmiston laatua. Tämä edellyttää kykyä tulkita katselmointien tuloksia, testiraportteja ja muuta dokumentaatiota sekä tunnistaa poikkeamat suunnitellusta. Tietoturvan toteutumista ei voi arvioida pelkästään lopputuloksesta, vaan sitä on seurattava jatkuvasti kehitystyön aikana.

Ymmärtää turvalliset kehityskäytännöt

Tilaajan on tunnistettava keskeiset turvallisen ohjelmistokehityksen periaatteet, kuten suojattu koodaus, riippuvuuksien hallinta, versionhallinta ja CI/CD-putken turvallisuus. Tämä tarkoittaa kykyä ymmärtää, miten tietoturva näkyy konkreettisesti kehitystyön arjessa, esimerkiksi koodikatselmuksissa, testauksessa, haavoittuvuuksien hallinnassa ja automaattisissa tarkistuksissa. Tilaajan ei tarvitse itse hallita teknisiä yksityiskohtia, mutta hänen on osattava tulkita raportteja, kysyä oikeita kysymyksiä ja tunnistaa poikkeamat suunnitellusta toteutuksesta.

Osaa reagoida tietoturvapoikkeamiin ja muutostarpeisiin

Kehitystyön aikana on väistämätöntä, että esiin nousee virheitä, haavoittuvuuksia ja muutostarpeita. Tilaajan tulee varmistaa, että poikkeamat raportoidaan sovitusti, tieto kulkee oikeille tahoille ja korjaavat toimenpiteet käynnistyvät viivytyksettä. Lisäksi on tärkeää, että havaittuja haavoittuvuuksia ja virheitä seurataan aktiivisesti ja osallistutaan niiden priorisointiin. Tilaajan on myös osattava arvioida, miten uudet vaatimukset, muuttuvat riskit tai lainsäädännön velvoitteet vaikuttavat kehitykseen, ja ohjattava tarvittavat muutokset hallitusti osaksi projektia.

Kyky toimia yhteistyössä kehitystiimin ja asiantuntijoiden kanssa

Tietoturvan toteutuminen edellyttää jatkuvaa vuoropuhelua eri toimijoiden välillä. Tilaajan on osattava kommunikoida tietoturvaan liittyvät havainnot, kysymykset ja vaatimukset selkeästi kehitystiimille, tietoturva-asiantuntijoille ja muille sidosryhmille. Rakentava yhteistyö auttaa tunnistamaan ongelmat ajoissa, ratkaisemaan ne tehokkaasti ja varmistamaan, että tietoturva on luonteva osa koko kehitystyötä.

Keskeiset toimet:

- Seuraa jatkuvasti kehityksen etenemistä suhteessa tietoturvavaatimuksiin.
- Varmista turvallisten kehityskäytäntöjen toteutuminen.
- Reagoi poikkeamiin ja muutostarpeisiin nopeasti ja hallitusti.
- Kommunikoi tietoturvaan liittyvät havainnot ja vaatimukset selkeästi eri sidosryhmille.

TOIMITUKSEN JA KÄYTTÖÖNOTON VALMISTELU

Ohjelmistokehityksen tilaajan tehtävänä on varmistaa, että toimitus täyttää sovitut tietoturvavaatimukset ja että käyttöönotto toteutetaan hallitusti ja suunnitelmallisesti. Tilaajan on huolehdittava, että tietoturvaan liittyvät vastuut, dokumentaatio ja prosessit siirtyvät selkeästi ylläpidon vastuulle, jotta tietoturva säilyy jatkuvana myös kehitysvaiheen jälkeen.

Osaa varmistaa, että toimitus vastaa sovittuja tietoturvavaatimuksia

Tilaajan on kyettävä varmistamaan, että toimitettava ohjelmisto täyttää sovitut tietoturvavaatimukset ja että tämä voidaan osoittaa katselmointien, testien ja dokumentaation avulla. Käyttöönottoon liittyvien ohjeiden, hallintaprosessien ja lokienhallinnan käytäntöjen on oltava ajantasaisia ja selkeitä, jotta ohjelmisto voidaan ottaa turvallisesti käyttöön. Tarkastuslistojen hyödyntäminen auttaa varmistamaan, että mikään kriittinen vaatimus ei jää huomiotta.

Tunnistaa käyttöönoton tietoturvariskit

Tilaajan tulee ymmärtää, miten ohjelmiston siirtyminen tuotantoympäristöön vaikuttaa tietoturvaan. On hyvä tunnistaa keskeiset käyttöönottoon liittyvät riskit, kuten väärin määritellyt käyttöoikeudet, puutteellinen konfiguraatio ja suojaamattomat integraatiot. Käyttöönoton yhteydessä voi ilmetä tietoturvapoikkeamia, joten poikkeamien hallintaan on jo tässä vaiheessa oltava olemassa selkeä toimintamalli, vastuuhenkilöt ja eskalointipolut. Tilaajan rooli on varmistaa, että siirtymä tuotantoon on suunniteltu ja toteutettu turvallisesti, jotta kehitysvaiheen tietoturva jatkuu saumattomasti tuotannossa.

Ymmärtää turvallisen käyttöönottoprosessin periaatteet

Turvallinen käyttöönotto edellyttää suunnitelmallisuutta, selkeitä vastuita ja riittäviä valvontamekanismeja. Tilaajan tulee varmistaa, että käyttöönottoprosessi on tietoturvan näkökulmasta hallittu ja että tarvittavat resurssit ja osaaminen ovat käytettävissä. On keskeistä huolehtia, että tietoturvaan liittyvä tieto (vaatimukset, katselmointien tulokset, testiraportit ja käyttöönottosuunnitelmat ym.) siirtyy osaksi tuotannon hallintaa ja on helposti ylläpitotiimin käytettävissä. Näin varmistetaan, ettei tietoturva katkea kehitysvaiheen päättyessä.

Ymmärtää ylläpidon ja jatkuvuuden tietoturvaedellytykset

Tietoturvan jatkuvuuden varmistaminen edellyttää, että tilaaja huolehtii vastuiden siirtymisestä selkeästi käyttö- ja ylläpitovaiheen vastuullisille tahoille, kuten tuoteomistajalle tai ylläpitotiimille. Tämä edellyttää dokumentaation, sopimusten ja prosessien huolellista tarkistamista. Tilaajan on myös varmistettava, että toimittajalla on käytössään toimivat prosessit päivitysten hallintaan, haavoittuvuuksien seurantaan ja käyttöönoton jälkeiseen tukeen. Lisäksi tuotantoympäristöön on rakennettava riittävät valvontamekanismit, kuten lokitus, hälytykset ja auditointikäytännöt, jotka mahdollistavat tietoturvan jatkuvan arvioinnin ja siihen reagoinnin. Näin tietoturva jatkuu johdonmukaisesti koko ohjelmiston elinkaaren ajan.

Keskeiset toimet:

- Varmista katselmointien, testien ja dokumentaation avulla, että ohjelmisto täyttää sovitut tietoturvavaatimukset.
- Tunnista ja arvioi käyttöönottoon liittyvät tietoturvariskit.
- Varmista riittävä osaaminen ja tuki turvalliseen käyttöönottoon.
- Siirrä tietoturvavastuut selkeästi osaksi jatkuvaa hallintaa.

Projektipäällikkö

Tässä osiossa käsitellään, millaista tietoturvaosaamista ohjelmistoprojektien projektipäälliköiltä, tai muilta kehitystyötä ohjaavilta rooleilta, edellytetään projektin eri vaiheissa, ja miten he voivat omalla toiminnallaan edistää ohjelmistoturvallisuutta.

Projektipäällikkö sitoo riskienhallinnan ja yhteistyön yhdeksi turvalliseksi projektiksi.

MIKSI OHJELMISTOTURVALLISUUS KUULUU PROJEKTIPÄÄLLIKÖLLE?

Projektipäällikkö vastaa ohjelmistoprojektin sujuvasta etenemisestä, ja hänen tehtävänään on varmistaa, että tietoturva otetaan huomioon kaikissa projektin vaiheissa. Turvallisuus ei ole pelkästään teknisiä ratkaisuja, vaan se edellyttää suunnitelmallisuutta, riskienhallintaa ja yhteistyötä eri sidosryhmien kanssa. Tietoturvanhallinta koskee myös itse projektin toteutusta: esimerkiksi pääsyoikeudet, luottamuksellisen tiedon käsittely, dokumentointi ja turvalliset työtavat vaativat suunnittelua, ohjeistusta ja valvontaa.

Projektipäällikön tulee ymmärtää ohjelmistoturvallisuuden merkitys organisaation liiketoiminnalle ja riskeille. Hän varmistaa, että turvallisuusvaatimukset on määritelty selkeästi, resurssit ovat riittävät ja aikataulut realistiset. Projektipäällikkö edistää turvallisuuskulttuuria, ohjaa riskienhallintaa ja varmistaa, että kaikki projektin osapuolet noudattavat sovittuja tietoturvakäytäntöjä. Projektipäällikkö huolehtii myös, että projektin turvallisuuspoikkeamiin reagoidaan nopeasti.

Tiivistelmä

PROJEKTIPÄÄLLIKÖN OSAAMISTARPEET

- Ymmärtää, että tietoturva ei ole vain teknisiä ratkaisuja, vaan osa projektin toimintakulttuuria ja arjen päätöksentekoa.
- Osaa tunnistaa ja määrittää projektin tietoturvatarpeet.
- Osaa sisällyttää tietoturvan osaksi projektisuunnitelmaa ja aikataulutusta.
- Osaa arvioida ja hallita projektin tietoturvariskejä koko projektin ajan.
- Ymmärtää ohjelmistoturvallisuuden merkityksen, tietää ohjelmiston eri elinkaaren vaiheet ja niiden vaikutukset turvallisuuteen.
- Ymmärtää sopimusten tietoturvavaatimukset ja osaa muuntaa ne konkreettisiksi toimenpiteiksi, joilla vaatimusten toteutuminen varmistetaan.
- Osaa varmistaa turvallisten työtapojen toteutumisen projektin arjessa ja edistää tietoturvatietoisuutta.
- Osaa ylläpitää ajantasaista ja jäljitettävää tietoturvadokumentaatiota.
- Kykenee johtamaan tietoturvayhteistyötä eri osapuolten välillä.
- Osaa varmistaa turvallisen siirtymän tuotantoon ja tietojen luovutuksen.
- Ymmärtää siirtää tietoturvavastuut selkeästi jatkovastuullisille tahoille.
- Osaa arvioida tietoturvan tilan projektin päättyessä, dokumentoida opit ja hyödyntää niitä seuraavissa projekteissa.

Yhteistyö toimittajien, kehitystiimin ja muiden sidosryhmien kanssa on keskeistä, jotta turvallisuustoimenpiteet integroituvat saumattomasti osaksi projektia. Projektipäällikkö kannattaakin ottaa mukaan mahdollisimman varhaisessa vaiheessa. Projektipäällikön osallistuminen suunnitteluun, toimittajan arviointiin ja sopimuksen laadintaan auttaa häntä tunnistamaan tulevan projektin tietoturvatarpeet ja varmistamaan, että ne huomioidaan ajoissa.

Vaikka projektipäällikkö vastaa vain projektin aikaisesta tietoturvasta, hänen on silti hyvä ymmärtää ohjelmiston koko elinkaari. Tämä auttaa varmistamaan, että projektissa tehdyt ratkaisut tukevat ohjelmiston turvallista ylläpitoa, jatkokehitystä ja tietoturvan hallintaa.

Projektipäällikkö laatii tietoturvan yhteisen pelikirjan.

PROJEKTIN SUUNNITTELU JA TARPEIDEN MÄÄRITTELY

Projektipäällikön tulee varmistaa, että tietoturva on sisällytetty projektin hallintaan, tavoitteisiin ja johtamiseen alusta alkaen. Tietoturvavaatimukset, riskit ja vastuut on tunnistettava ja sovitettava yhteen eri osapuolten toiminnan kanssa, jotta projekti tukee ohjelmiston turvallista toteutusta.

Osaa tunnistaa ja määrittää projektin tietoturvavaatimukset

Projektipäällikön varhainen osallistuminen hankinnan suunnittelu- ja määrittelyvaiheessa on tärkeää, jotta projektin tietoturvatarpeet tunnistetaan ja määritellään ajoissa. Projektipäällikön on ymmärrettävä hankkeen sisältö ja taustat riittävän syvällisesti, sillä nämä tiedot muodostavat pohjan tietoturvasuunnitelmalle. Projektin tietoturvavaatimuksia määriteltäessä on osattava huomioida, kuinka salaista tai kriittistä tietoa projektin aikana käsitellään, ja varmistettava, että tiedot ja käytettävät järjestelmät suojataan tarkoituksenmukaisesti.

Projektipäällikön on tunnettava organisaation tietoturvakäytännöt ja -vaatimukset, sekä osattava soveltaa sovellettavia standardeja ja säädöksiä projektin vaatimusten määrittelyssä. Tietoturvavaatimukset ohjaavat koko projektin toteutusta, joten ne on kirjattava selkeästi ja mitattavasti, eikä määrittelyyn saa jäädä tulkinnanvaraa. Projektipäälliköllä on oltava kyky tuoda yhteen eri toimijat, kuten ohjelmistotoimittaja, kehitystiimi, liiketoiminta ja tietoturvavastaava, jotta kaikilla on yhteinen käsitys tietoturvan tavoitteista ja reunaehdoista.

Ymmärtää ohjelmistoturvallisuuden merkityksen ohjelmiston elinkaaren eri vaiheissa

Projektipäällikön tulee ymmärtää, että ohjelmistoturvallisuus ulottuu koko ohjelmiston elinkaarelle – suunnittelusta käyttöönottoon, ylläpitoon, jatkokehitykseen ja käytöstä poistoon. Tämän vuoksi projektipäälliköllä tulee olla selkeä käsitys ohjelmiston eri elinkaaren vaiheista. Kokonaiskuva auttaa varmistamaan, että projektissa tehtävät ratkaisut tukevat ohjelmiston pitkäaikaista turvallisuutta, organisaation riskienhallintaa ja liiketoimintatavoitteita. Samalla se vähentää riskiä siitä, että projektissa syntyy ratkaisuja, jotka vaikeuttavat tietoturvan hallintaa tulevaisuudessa.

Osaa sisällyttää tietoturvan projektisuunnitelmaan

Projektin alkuvaiheessa luodaan perusta tietoturvakulttuurille, joka vaikuttaa siihen, miten tietoturva toteutuu koko projektin ajan. Projektipäällikön tulee varmistaa, että tietoturva sisältyy projektisuunnitelmaan kokonaisuutena – aikatauluihin, resursointiin ja tehtävälistoihin. Tämä edellyttää, että projektipäällikkö ymmärtää, mitkä tietoturvatehtävät kuuluvat muiden roolien vastuulle projektin aikana. Tietoturvatehtävät, niihin liittyvät vastuut ja tarkastuspisteet on sovittava ja jalkautettava selkeästi, jotta tietoturva ei jää irralliseksi osaksi vaan kulkee mukana projektin arjessa.

Osaa arvioida ja hallita projektin tietoturvariskejä

Projektipäällikön on kyettävä tunnistamaan ja arvioimaan projektin tietoturvariskit jo suunnitteluvaiheessa. Näihin kuuluvat esimerkiksi pääsyoikeuksien hallinta, luottamuksellisen tiedon käsittely ja järjestelmien konfigurointiin liittyvät haavoittuvuudet. Projektipäällikön tulee suunnitella hallintatoimenpiteet riskeihin varautumiseksi ja varmistaa, että eskalointimallit ja vastuuhenkilöt on määritelty mahdollisia projektin aikaisia poikkeamia varten.

Ymmärtää sopimusten tietoturvavelvoitteet

Projektipäällikön tulee osallistua sopimusten ja yhteistyömallien suunnitteluun siten, että tietoturvavelvoitteet ja vastuut ovat selkeästi määritelty jo ennen projektin käynnistymistä. Tämä auttaa varmistamaan, että toimittajan ja muiden osapuolten roolit tietoturvan toteuttamisessa ovat yksiselitteiset ja että projektin tietoturva ei jää epäselvyyksien varaan.

Keskeiset toimet:

- Osallistu hankinnan suunnitteluun ja määrittelyyn, jotta projektin tietoturvavaatimukset huomioidaan heti alussa.
- Tunnista ja määrittele projektille selkeät ja mitattavat tietoturvavaatimukset.
- Kokoa eri sidosryhmät yhteen ja varmista yhteinen ymmärrys tietoturvatavoitteista ja reunaehdoista.
- Sisällytä tietoturva osaksi projektisuunnitelmaa: aikataulut, resurssit, tehtävät, vastuut ja tarkastuspisteet.
- Tunnista projektin tietoturvariskit ja suunnittele niihin hallintatoimenpiteet.
- Huomioi projektissa ohjelmiston koko elinkaaren tietoturvatarpeet.

Tietoturvan tulee näkyä arjessa, ei vain suunnitelmissa.

PROJEKTIN AIKANA

Projektipäällikön tehtävänä on varmistaa, että tietoturva toteutuu käytännössä projektin kaikissa vaiheissa ja pysyy osana arjen toimintaa. Vastuualueisiin kuuluu riskienhallinnan, dokumentoinnin ja sidosryhmien yhteistyön johtaminen siten, että tietoturva pysyy hallittuna, ajantasaisena ja yhteisesti ymmärrettynä koko projektin ajan.

Osaa varmistaa tietoturvan toteutumisen käytännössä

Projektipäällikön tehtävänä on varmistaa, että turvalliset työtavat, kuten pääsyoikeuksien hallinta, dokumentoinnin käytännöt ja tiedon käsittely, sovitaan ja jalkautetaan heti projektin alussa. Projektipäällikkö vastaa siitä, että nämä toimintatavat toteutuvat käytännössä koko projektin ajan ja noudattavat organisaation ohjeita sekä sovittuja käytäntöjä. Tietoturvatehtävien, vastuiden ja tarkastuspisteiden etenemistä on seurattava säännöllisesi, ja tarvittaessa tietoturvavaatimuksia päivitetään projektin edetessä. Myös muutokset on dokumentoitava asianmukaisesti. Lisäksi projektipäällikkö raportoi säännöllisesti tietoturvan toteutumisesta projektin johdolle ja sidosryhmille sekä varmistaa, että vaatimukset näkyvät konkreettisina ratkaisuina projektin arjessa, ei pelkästään suunnitelmissa.

Osaa hallita projektin tietoturvariskejä

Projektin tietoturvariskit tulee tunnistaa, arvioida ja hallita koko projektin ajan. Projektipäällikön on varmistettava, että riskienhallinta on jatkuvaa ja järjestelmällistä, ja että riskilistaa päivitetään säännöllisesti yhteistyössä asiantuntijoiden ja sidosryhmien kanssa. Riskienhallinnan tulee kattaa tekniset, organisatoriset ja toiminnalliset näkökulmat, kuten työasemat, pääsyoikeudet, tiedon käsittely, järjestelmäintegraatiot ja ulkoiset riippuvuudet. Projektipäällikkö vastaa siitä, että riskienhallintatoimenpiteet ovat linjassa organisaation käytäntöjen ja sääntelyvaatimusten kanssa. Mikäli riskit ylittävät ennalta määritellyt hyväksyttävyyden rajat tai voivat vaikuttaa merkittävästi liiketoimintaan, projektipäällikön tulee eskaloida ne viipymättä ylemmälle johdolle päätöksenteon tueksi.

Varmistaa dokumentoinnin ja jäljitettävyyden

Projektipäällikön vastuulla on varmistaa, että kaikki tietoturvaan liittyvä dokumentaatio, kuten testiraportit, katselmointien tulokset ja päätökset, kootaan ja ylläpidetään huolellisesti. Dokumentaation tulee olla ajantasaista, jäljitettävää ja helposti saatavilla esimerkiksi auditointeja, katselmointeja tai siirtymävaiheita varten. Hyvin hoidettu dokumentointi tukee myös poikkeamien hallintaa ja jatkuvuuden varmistamista.

Tunnistaa turvallisuusvaatimusten toteutumista uhkaavat tilanteet

Projektipäällikön tulee aktiivisesti seurata tietoturvan toteutumista ja tunnistaa tilanteet, jotka voivat vaarantaa sovittujen vaatimusten toteutumisen. Hän arvioi poikkeamia ja riskejä yhdessä asiantuntijoiden kanssa ja huolehtii siitä, että niihin reagoidaan järjestelmällisesti ja nopeasti. Projektissa tulee varmistaa, että tarvittavat korjaavat toimenpiteet tunnistetaan, päätetään ja viedään käytäntöön ilman viivettä. Projektipäällikkö vastaa myös siitä, että sidosryhmät saavat ajantasaisen tiedon projektin tietoturvatilanteesta ja että tarkastuspisteet, testaukset ja katselmoinnit toteutetaan sovitussa aikataulussa.

Osaa ylläpitää tietoturvatietoisuutta projektitiimissä

Tietoturvatietoisuuden ylläpitäminen on olennainen osa projektin johtamista. Projektipäällikön tulee varmistaa, että kaikki osapuolet noudattavat sovittuja käytäntöjä, ja tukea tiimin kykyä tunnistaa tietoturvariskejä ja havaita poikkeamia. Projektipäällikkö huolehtii siitä, että tietoturva pysyy mukana arjen päätöksenteossa ja työskentelytavoissa, ja että turvallisuuskulttuuri juurtuu koko projektin ajaksi.

Osaa johtaa sidosryhmien tietoturvayhteistyötä

Projektipäällikön tehtävänä on varmistaa, että tietoturva ymmärretään ja huomioidaan kaikissa projektin päätöksissä ja työvaiheissa. Projektipäällikkö viestii vaatimukset ja riskit selkeästi eri sidosryhmille, määrittelee roolit ja vastuut, ja ylläpitää yhteistyötä toimittajien, kehitystiimin, liiketoiminnan ja tietoturvavastaavien välillä. Hyvin johdettu yhteistyö varmistaa, että tietoturva ei jää yksittäisten henkilöiden vastuulle, vaan on koko projektin yhteinen tehtävä.

Keskeiset toimet:

- Jalkauta turvalliset työtavat heti projektin alussa ja edistä projektitiimin tietoisuutta tietoturvasta.
- Seuraa tietoturvatehtävien, vastuiden ja tarkastuspisteiden etenemistä.
- Päivitä tietoturvavaatimuksia projektin edetessä ja dokumentoi muutokset huolellisesti.
- Tunnista ja arvioi projektin tietoturvariskejä jatkuvasti.
- Varmistaa, että tietoturvadokumentaatio on ajantasaista, jäljitettävää ja helposti saatavilla.
- Reagoi nopeasti poikkeamiin ja huolehdi korjaavien toimenpiteiden toteutuksesta.
- Johda sidosryhmien välistä tietoturvayhteistyötä.

TUOTANTOON SIIRTO JA KÄYTTÖÖNOTTO

Projektipäällikön tehtävänä on varmistaa, että tuotantoon siirtyminen toteutetaan hallitusti ja tietoturva huomioiden. Vastuualueisiin kuuluu riskien arviointi, tarkistusten ja hyväksyntöjen koordinointi sekä tietoturvavastuiden siirtäminen selkeästi jatkovastuullisille tahoille, jotta ohjelmiston turvallisuus säilyy myös projektin päätyttyä.

Ymmärtää tuotantoon siirtoon liittyvät tietoturvariskit

Projektipäällikön tulee tunnistaa, miten ohjelmiston siirtyminen tuotantoympäristöön voi aiheuttaa tietoturvariskejä, jotka poikkeavat kehitysvaiheen riskeistä. Tyypillisiä riskejä ovat esimerkiksi väärin määritellyt käyttöoikeudet, puutteelliset konfiguraatiot, suojaamattomat rajapinnat ja keskeneräiset integraatiot. Lisäksi riskejä voi syntyä, jos tietoturvaan liittyvä tieto ei siirry kattavasti ylläpitotiimille tai jos vastuut jäävät epäselviksi. Projektipäällikön on varmistettava, että siirtymävaiheeseen liittyvät riskit arvioidaan huolellisesti, hallintatoimet suunnitellaan etukäteen ja mahdolliset poikkeamat voidaan havaita ja käsitellä nopeasti. Mikäli riski voi vaikuttaa merkittävästi tuotantoympäristön turvallisuuteen tai liiketoimintaan, se tulee eskaloida viipymättä ylemmälle johdolle.

Osaa varmistaa turvallisen siirtymän tuotantoon

Projektipäällikkö tulee huolehtia siitä, että siirtymä tuotantoon etenee suunnitelmallisesti ja tietoturva huomioiden. Tämä tarkoittaa, että hän varmistaa hyväksymistestien, tietoturvatarkastusten ja katselmusten valmistumisen ja dokumentoinnin ennen käyttöönottoa. Projektipäällikkö seuraa, että sovitut tarkistuspisteet käydään läpi, löydetyt puutteet korjataan ja käyttöönottopäätös tehdään vain silloin, kun tietoturva on todettu riittäväksi. On varmistettava, että kaikki tietoturvaan liittyvä tieto (kuten vaatimukset, testitulokset, katselmoinnit ja dokumentaatio ym.) siirtyy ylläpitotiimin käyttöön ja on helposti saatavilla. Lisäksi on koordinoitava käyttöön liittyvä koulutus ja perehdytys.

Osaa siirtää tietoturvavastuut selkeästi jatkovastuullisille tahoille

Projektin päättyessä tietoturvavastuut siirtyvät ylläpidolle, palvelutoimittajalle tai muille jatkovastuullisille tahoille. Projektipäällikön tulee varmistaa, että tämä siirto on selkeä ja dokumentoitu. Hän huolehtii, että jatkovastuullisilla on tarvittavat tiedot tietoturvavaatimuksista, toteutetuista ratkaisuista ja riskeistä. Käytännössä tämä tarkoittaa esimerkiksi käyttö- ja ylläpito-ohjeiden täydentämistä, dokumentaation luovuttamista ja vastuuroolien määrittelyä niin, ettei tietoturva katkea projektin päättyessä.

Ymmärtää tuotantoympäristön tietoturvavaatimukset

Projektipäällikön tulee ymmärtää, millaisia tietoturvamekanismeja tuotantoympäristössä tarvitaan, kuten lokitus, hälytykset, auditointikäytännöt ja haavoittuvuuksien seuranta. Projektipäällikkö ei välttämättä itse ole tekninen asiantuntija, mutta hänen on osattava varmistaa, että asiantuntijat toteuttavat vaatimukset ja että niiden toteutuminen dokumentoidaan ja hyväksytään.

Osaa varmistaa jatkuvuuden ja reagointikyvyn

Projektipäällikön tulee varmistaa, että tuotantoympäristössä on valmiudet tietoturvapoikkeamien havaitsemiseen ja niihin reagoimiseen. Tämä tarkoittaa, että häiriö- ja poikkeamatilanteiden toimintamallit on määritelty ja sovittu etukäteen, ja että vastuut niiden hoitamiseen on selkeästi jaettu. Lisäksi on varmistettava, että varmistus- ja palautuskäytännöt toimivat, ja että ylläpito-organisaatiolla on riittävä tieto ja valmiudet reagoida nopeasti tietoturvapoikkeamiin. Näin projektista luovutettu järjestelmä on paitsi toimintavalmis myös turvallinen ja hallittavissa pitkällä aikavälillä.

Keskeiset toimet:

- Tunnista ja arvioi tuotantoon siirron riskit ja suunnittele hallintatoimet.
- Varmista, että hyväksymistestit, tietoturvatarkastukset ja katselmoinnit on tehty ja dokumentoitu ennen käyttöönottoa.
- Varmista, että tietoturvavaatimukset, riskilista, testitulokset, katselmoinnit ja muu tietoturvadokumentaatio siirtyy ylläpitotiimille.
- Koordinoi riittävä käyttöönottoon liittyvä koulutus ja perehdytys.
- Dokumentoi ja siirrä tietoturvavastuut selkeästi vastuullisille tahoille.
- Varmista, että tuotantoympäristössä on käytössä tarvittavat tietoturvamekanismit.
- Varmista, että poikkeamien hallintamallit ja vastuut on määritelty.

Tietoturva ei siirry tuotantoon itsestään.

PROJEKTIN LOPETUS

Projektipäällikön tehtävänä on varmistaa, että tietoturva arvioidaan, dokumentoidaan ja siirretään hallitusti osaksi jatkuvaa toimintaa projektin päättyessä. Projektin lopetus on vaihe, jossa myös varmistetaan vaatimusten täyttyminen, vastuiden selkeys ja opittujen kokemusten hyödyntäminen tulevien projektien tietoturvan kehittämisessä.

Osaa arvioida tietoturvan tilan projektin päättyessä

Projektin lopussa tulee tehdä tietoturvan tilan arviointi, jossa tarkastellaan, onko kaikki vaatimukset täytetty, poikkeamat käsitelty ja riskit hallinnassa. Projekti voidaan lopettaa vasta, kun sovitut tietoturvavaatimukset on täytetty ja dokumentoitu. Tämä tarkoittaa, että kaikki tietoturvatestit, katselmukset ja mahdolliset auditoinnit on suoritettu, ja niiden tulokset on hyväksytty. Projektipäällikön tehtävänä on varmistaa, että arviointi dokumentoidaan ja että sen pohjalta voidaan tarvittaessa käynnistää jatkotoimenpiteitä tuotannon puolella.

Osaa dokumentoida ja luovuttaa tietoturvaan liittyvät tiedot

Projektin lopetuksessa tietoturvaosaaminen näkyy erityisesti dokumentoinnissa ja tiedon siirrossa. Projektipäällikkö huolehtii, että kaikki tietoturvaan liittyvä materiaali – testiraportit, riskilistaukset, hyväksymistodistukset, ohjeistukset ja sovitut toimintamallit – siirtyy selkeästi vastuullisille. Projektipäälliköllä tulee olla taito erottaa, mikä tieto on kriittistä jatkuvuuden kannalta, ja varmistaa sen löydettävyys myöhemmin.

Ymmärtää tietoturvavastuiden siirtymisen merkityksen

Projektipäällikön on huolehdittava, että tietoturvavastuut eivät jää epäselviksi. Tämä edellyttää kykyä käydä läpi ja sopia yhdessä organisaation ja toimittajien kanssa, kuka vastaa jatkossa esimerkiksi lokiseurannasta, haavoittuvuuksien hallinnasta tai poikkeamien käsittelystä. Keskeistä on varmistaa jatkuvuus ja estää “vastuun katoaminen” projektin päättyessä. Tietoturvavastuiden siirron tulee olla suunniteltu ja dokumentoitu huolellisesti.

Arvioi, opi, kehitä – tietoturva kasvaa projektista toiseen.

Osaa poistaa tarpeettomat tiedot ja käyttöoikeudet turvallisesti

Projektin aikana syntynyt ylimääräinen tieto, kuten testidatat, väliaikaiset tiedostot ja vanhentuneet dokumenttiversiot, tulee poistaa tai siirtää turvallisesti. Tämä koskee esimerkiksi testidataa, väliaikaisia käyttöoikeuksia, kehitysympäristöjen sisältöjä ja projektikohtaisia tiedostoja. Samalla on tärkeää varmistaa, että kehitysaikaiset asetukset, kuten lokitustasot, tarkistetaan ja mukautetaan tuotantokäyttöön sopiviksi, jotta vältetään tahattomat tietovuodot.

Tiedon poistaminen tulee tehdä suunnitellusti ja dokumentoidusti, organisaation ohjeiden ja säädöstelyvaatimusten mukaisesti. Projektipäällikön on varmistettava, että projektin päättyessä käyttöoikeudet tarkistetaan ja tarpeettomat pääsyoikeudet poistetaan. Näin ehkäistään riski, että entiset projektin jäsenet tai toimittajat pääsisivät myöhemmin luvattomasti käsiksi järjestelmiin tai tietoihin.

Osaa hyödyntää tietoturvan jälkiarviointia oppimisen ja kehittämisen välineenä

Projektin lopetusvaiheessa projektipäällikön tulee varmistaa, että tietoturvaan liittyvistä kokemuksista, onnistumisista ja poikkeamista tehdään johtopäätökset ja ne dokumentoidaan tulevia projekteja varten. Projektipäällikön on osattava fasilitoida jälkiarviointi, jossa tarkastellaan projektin tietoturvan toteutumista kokonaisuutena, tunnistetaan kehityskohteet ja vahvistetaan toimivia käytäntöjä. Tämä arviointi tukee organisaation oppimista ja jatkuvaa parantamista.

Keskeiset toimet:

- Arvioi projektin tietoturvan tila ja varmista, että kaikki vaatimukset on täytetty, poikkeamat käsitelty ja tulokset dokumentoitu.
- Varmista, että kaikki tietoturvatestit, katselmukset ja auditoinnit on suoritettu ja dokumentoitu hyväksytysti.
- Dokumentoi ja siirrä kaikki tietoturvaan liittyvä materiaali selkeästi jatkovastuullisille.
- Siirrä tietoturvavastuut selkeästi ja dokumentoidusti.
- Poista tai siirrä turvallisesti kaikki tarpeettomat tiedot ja käyttöoikeudet organisaation ohjeiden mukaisesti.
- Fasilitoi tietoturvan jälkiarviointi, dokumentoi opit ja hyödynnä niitä tulevissa projekteissa.

Tuoteomistaja, palvelupäällikkö tai muu operatiivinen vastuuhenkilö

Tässä osiossa käsitellään, millaista tietoturvaosaamista tuoteomistajalta, palvelupäälliköltä tai muulta operatiiviselta vastuuhenkilöltä edellytetään ohjelmiston elinkaaren eri vaiheissa ja miten hän voi omalla toiminnallaan käytännössä edistää ohjelmistoturvallisuutta. Selkeyden vuoksi jatkossa käytetään termiä ”tuoteomistaja” viittaamaan kaikkiin näihin rooleihin.

Tuoteomistaja on jatkuva tietoturvan puolestapuhuja.

MIKSI OHJELMISTOTURVALLISUUS KUULUU TUOTEOMISTAJALLE?

Tuoteomistaja vastaa ohjelmistotuotteen turvallisuudesta sen koko elinkaaren ajan liiketoiminnan ja käyttäjien näkökulmasta. Hän ohjaa tuotteen kehitystä varmistamalla, että tietoturva on osa tuotekehityksen prioriteetteja ja että turvallisuusvaatimukset näkyvät selkeästi tuotteen kehitysjonossa.

Tuoteomistaja toimii tiiviissä yhteistyössä kehitystiimin kanssa ja varmistaa, että tietoturva toteutuu konkreettisina toimintoina ja ominaisuuksina tuotteessa. Hän hallinnoi riskejä, priorisoi turvallisuuteen liittyvät korjaukset ja kehityskohtaiset muutokset sekä vastaa, että lainsäädännön ja muiden vaatimusten edellyttämät turvallisuusominaisuudet otetaan huomioon.

Tuoteomistaja on jatkuva tietoturvan puolestapuhuja tuotteen elinkaaressa, seuraa aktiivisesti turvallisuustilannetta ja reagoi nopeasti uusiin uhkiin tai haavoittuvuuksiin, varmistaen tuotteen luotettavuuden, jatkuvuuden ja käyttäjien tietoturvan.

Tiivistelmä

TUOTEOMISTAJAN OSAAMISTARPEET

- Osaa tunnistaa sääntelyn, tietosuojan ja liiketoiminnan vaatimukset ja muuntaa ne selkeiksi toimenpiteiksi ja hyväksymiskriteereiksi.
- Osaa hallita ohjelmiston tietoturvariskit ohjelmiston kaikissa elinkaaren vaiheissa.
- Ymmärtää tietoturvavaatimusten vaikutuksen resursointiin, aikatauluihin ja budjettiin.
- Osaa arvioida toimittajien tietoturvakäytännöt, hallita toimitusketjuriskit ja sisällyttää turvallisuutta ja jatkuvuutta tukevat vaatimukset sopimuksiin.
- Osaa varmistaa, että käyttöönottovaiheessa tietoturvavaatimukset toteutuvat ja käyttäjät saavat tarvittavan tuen turvalliseen käyttöön.
- Ymmärtää haavoittuvuuksien hallinnan merkityksen ja osaa priorisoida korjaukset liiketoimintariskien perusteella.
- Osaa hallita ohjelmiston ja komponenttien päivityksiä suunnitelmallisesti ja dokumentoidusti.
- Ymmärtää lokituksen ja valvonnan roolin poikkeamien havaitsemisessa.
- Osaa hallita käyttöoikeuksia tietoturvaperiaatteiden mukaisesti koko elinkaaren ajan.
- Osaa seurata ja päivittää sopimuksia ja palvelutasoja tietoturvan näkökulmasta.
- Ymmärtää jatkuvuuden ja palautumisen perusperiaatteet ja niiden toteuttamisen ylläpidossa.
- Osaa edistää tietoturvan jatkuvaa parantamista osana tuote- ja palvelukehitystä.

Selkeät toimenpiteet syntyvät tarkasti määritellyistä vaatimuksista.

TARPEIDEN MÄÄRITTELY JA SUUNNITTELU

Tuoteomistajan tehtävänä on varmistaa, että tietoturva sisältyy ohjelmiston suunnitteluun ja vaatimusten määrittelyyn liiketoiminnan tavoitteiden rinnalla. Tietoturvaa koskevat vaatimukset, riskit ja resurssit on tunnistettava ajoissa ja muutettava konkreettisiksi hyväksymiskriteereiksi, jotka ohjaavat ohjelmiston kehitystä ja käyttöä koko sen elinkaaren ajan.

Ymmärtää ohjelmistoturvallisuuden vaikutuksen liiketoimintaan

Ohjelmistot ovat yhä useammin kriittinen osa liiketoimintaa, jolloin niiden turvallisuudella on suora vaikutus organisaation jatkuvuuteen, asiakastyytyväisyyteen ja maineeseen. Ohjelmistoturvallisuus vaikuttaa suoraan organisaation kykyyn tuottaa palveluita luotettavasti ja suojata asiakasdataa. On tärkeää tiedostaa, että ohjelmistoturvallisuus ei ole pelkästään teknisiä ratkaisuja, vaan osa kokonaisvaltaista riskienhallintaa, joka kattaa myös prosessit, vastuut, osaamisen ja yhteistyön ohjelmiston koko elinkaaren ajan.

Osaa tunnistaa sääntelyn ja tietosuojan vaatimukset osana tarpeen määrittelyä

Ohjelmiston turvallisuusvaatimukset nousevat sekä liiketoiminnan tarpeista että lainsäädännöstä, viranomaisohjeista ja asiakkaiden odotuksista. Ennen ohjelmiston hankintaa tai kehitystyötä on tärkeää tunnistaa, mitä sääntelyä ohjelmiston on noudatettava (esimerkiksi GDPR, NIS2-direktiivi, CRA ja mahdollinen alan erityissääntely) ja ottaa vaatimukset huomioon koko ohjelmiston elinkaaren ajan. Tuoteomistajan on kyettävä määrittelemään, miten nämä vaatimukset näkyvät konkreettisesti arjen toiminnoissa - esimerkiksi miten henkilötietoja käsitellään ja suojataan, kuinka tietojen poistopyyntö toteutetaan tai miten lokitiedot säilytetään sääntelyn mukaisesti. Vaatimukset tulee muuntaa selkeiksi toimenpiteiksi ja hyväksymiskriteereiksi, jotta ohjelmisto täyttää sekä sääntelyn että asiakkaiden odotukset myös pitkäaikaisessa käytössä ja ylläpidossa.

Osaa tunnistaa ja arvioida ohjelmiston riskit

Tuoteomistajan tulee tunnistaa, mitkä ohjelmiston toiminnot tai tiedot ovat kriittisiä liiketoiminnalle ja käyttäjille, sekä mitkä niistä ovat houkuttelevia hyökkäyskohteita. Riskien tunnistaminen ja arviointi auttavat tekemään tietoon perustuvia päätöksiä, kuten priorisoimaan suojausta sinne, missä vaikutukset ovat suurimmat. Tämä osaaminen tukee myös hyväksymiskriteerien määrittelyä. Esimerkiksi jos riski liittyy luvattomaan pääsyyn tietoihin, hyväksymiskriteeriksi voidaan kirjata vahva tunnistautuminen. Jos riski liittyy ulkoisiin riippuvuuksiin, hyväksymiskriteeriksi voidaan vaatia niiden dokumentointi ja päivitysten hallinta. Näin riskit muuttuvat konkreettisiksi ja mitattaviksi vaatimuksiksi, jotka ohjaavat ohjelmiston tuvallisuutta kehityksessä ja ylläpidossa.

Osaa tunnistaa turvallisuusvaatimusten vaikutuksen resursointiin

Tietoturvavaatimukset vaikuttavat paitsi kehityksen laajuuteen, kustannuksiin ja aikatauluihin, myös ohjelmiston jatkuvaan ylläpitoon ja käyttöön. Tuoteomistajan on osattava arvioida, mitä resursseja – aikaa, rahaa ja osaamista – tietoturvan toteuttaminen ja ylläpitäminen edellyttävät. Tämä voi tarkoittaa esimerkiksi lisäkehitystä vahvan tunnistautumisen toteuttamiseksi, asiantuntijaresurssien varaamista auditointeihin tai riittävän budjetin suunnittelua ohjelmiston elinkaaren aikaisiin päivityksiin ja tietoturvaseurantaan. Tuoteomistajan tehtävänä on varmistaa, että tietoturvavaatimukset sisällytetään työjonoon sekä vuosikelloon, ja että turvallisuustyölle on varattu realistiset resurssit.

Osaa tehdä yhteistyötä asiantuntijoiden kanssa

Tuoteomistajan ei tarvitse olla tekninen tietoturva-asiantuntija, mutta hänen tulee tunnistaa tilanteet, joissa tarvitaan syvempää osaamista. Yhteistyö tietoturva-asiantuntijoiden, arkkitehtien ja kehittäjien kanssa on tärkeää jo suunnitteluvaiheessa, sillä silloin tehdään ratkaisuja, joilla on pitkäaikaisia vaikutuksia ohjelmiston turvallisuuteen. Tuoteomistajan tulee osata dokumentoida tietoturvavaatimukset selkeästi ja viestiä ne eri sidosryhmille, sekä käydä rakentavaa keskustelua kehittäjien ja arkkitehtien kanssa siitä, miten vaatimukset voidaan toteuttaa teknisesti ja liiketoiminnallisesti järkevällä tavalla.

Keskeiset toimenpiteet:

- Tunnista ja dokumentoi ohjelmiston turvallisuusvaatimukset sääntelyn ja asiakasodotusten pohjalta.
- Käytä vaatimuksia ohjaamaan hankintaa ja suunnittelua alusta alkaen.
- Priorisoi ja käännä vaatimukset selkeiksi toimenpiteiksi ja hyväksymiskriteereiksi.
- Tunnista ohjelmiston kriittiset toiminnot ja tiedot sekä arvioi niihin liittyvät riskit.
- Resursoi riittävästi aikaa, rahaa ja osaamista tietoturvan kehittämiseen ja ylläpitoon.
- Tee aktiivisesti yhteistyötä tietoturva-asiantuntijoiden, arkkitehtien ja kehittäjien kanssa.
- Dokumentoi tietoturvavaatimukset selkeästi.

TOIMITTAJAN VALINTA JA KEHITYKSEN VALMISTELU

Toimittajan valinnan ja kehityksen valmistelun vaiheessa tuoteomistaja huolehtii siitä, että liiketoiminnan ja tietoturvan tavoitteet kulkevat rinnakkain. On tunnistettava tietoturvavaatimukset, toimitusketjun riskit ja sopimukselliset velvoitteet, ja vietävä ne osaksi hankinta- ja suunnitteluprosessia. Näin varmistetaan, että valittu ratkaisu on turvallinen ja tukee organisaation pitkäaikaisia tavoitteita.

Osaa tuoda esiin liiketoiminnan ja käyttäjien kriittiset tarpeet

Tuoteomistajan tehtävä on varmistaa, että liiketoiminnan ja käyttäjien näkökulmat tulevat huomioiduiksi toimittajan valinnan ja kehityksen valmistelun aikana. Tämä tarkoittaa turvallisuuteen liittyvien vaatimusten tunnistamista ja niiden muuntamista selkeiksi toimenpiteiksi, jotka ohjaavat hankintaa ja kehitystä. Tuoteomistaja toimii siltana eri asiantuntijoiden ja sidosryhmien välillä, jotta tietoturvanäkökulmat sisältyvät päätöksentekoon alusta lähtien. Näin varmistetaan, että ohjelmiston tietoturva on kiinteä osa kokonaisuutta eikä irrallinen lisä myöhemmässä vaiheessa.

Ymmärtää toimittajan tietoturvakäytäntöjen merkityksen

Toimittajan tietoturvakäytännöt ja prosessit määrittävät ohjelmiston turvallisuustason pitkällä aikavälillä. Tuoteomistajan on tärkeää ymmärtää, miten toimittaja varmistaa turvallisuuden kehityksessä ja toimituksessa, miten päivityksiä julkaistaan ja miten ohjelmiston riippuvuuksia hallitaan. Syvällistä teknistä asiantuntemusta ei tarvita, mutta keskeiset kysymykset, joilla selvitetään toimittajan kyvykkyys, on tunnettava. Näin tuoteomistaja pystyy arvioimaan, täyttävätkö ehdotetut ratkaisut pitkällä aikavälillä liiketoiminnan ja tietoturvan kannalta kriittiset vaatimukset.

Osaa arvioida toimitusketjun riskejä

Ohjelmistoihin liittyvät riskit eivät rajoitu pelkästään toimittajaan, vaan ne ulottuvat myös alihankkijoihin ja käytettyihin komponentteihin. Tuoteomistajan tulee ymmärtää, että toimitusketju voi sisältää esimerkiksi avoimen lähdekoodin riippuvuuksia, joiden hallinta edellyttää läpinäkyvyyttä ja dokumentointia, kuten SBOMia (Software Bill of Materials). Valmiin ohjelmiston hankinnassa tuoteomistajan on tunnistettava keskeiset tarkistuskohteet ja ero yksittäisen tuotteen hankinnan ja palveluna toimitettavan ohjelmiston riskienhallinnassa. Lisäksi on arvioitava, mitä resursseja jatkuva yhteistyö toimittajan kanssa edellyttää molemmilta osapuolilta.

Ymmärtää sopimuksen merkityksen tietoturvan jatkuvuudessa

Sopimus on keskeinen väline, jolla varmistetaan tietoturvan toteutuminen ohjelmiston koko elinkaaren ajan, myös käyttöönoton jälkeen. Tuoteomistajan on tärkeää tunnistaa, mitkä tietoturvaan liittyvät asiat tulee sisällyttää tarjouspyyntöihin, arviointikriteereihin ja lopulta sopimukseen. Tämä voi tarkoittaa esimerkiksi SLA-vaatimuksia, vastuiden määrittelyä, auditointioikeuksia sekä dokumentaation ja prosessien sisällyttämistä hyväksymiskriteereihin. Lisäksi sopimuksen on tuettava turvallisuuden hallintaa ylläpidon ja muutosten aikana. Tuoteomistajan kyettävä arvioimaan, miten nämä vaatimukset vaikuttavat budjettiin ja aikatauluun, jotta resursointi on realistista ja turvallisuus voidaan turvata myös pitkällä aikavälillä.

Tuoteomistaja yhdistää liiketoiminnan, asiakkaat ja turvallisuuden.

Hyväksy vain turvallinen alku ohjelmiston käytölle.

Keskeiset toimet:

- Tuo esiin liiketoiminnan ja käyttäjien kriittiset tarpeet ja varmista, että ne huomioidaan toimittajan arvioinnissa.
- Konkretisoi tietoturvaan liittyvät vaatimukset selkeiksi toimenpiteiksi ohjaamaan tarjouspyyntöjä ja toimittajan valintaa.
- Arvioi toimittajan tietoturvakäytännöt ja prosessit.
- Tunnista toimitusketjun riskit.
- Varmista, että sopimuksiin sisällytetään tietoturvavaatimukset koko ohjelmiston elinkaaren ajalta.
- Arvioi vaatimusten vaikutukset resursointiin: budjetti, aikataulu ja osaaminen.

KÄYTTÖÖNOTTO

Käyttöönotossa tuoteomistaja varmistaa, että ohjelmisto voidaan ottaa turvallisesti käyttöön ja että sovitut tietoturvavaatimukset toteutuvat käytännössä. Valmistelu edellyttää yhteistyötä asiantuntijoiden ja käyttäjien kanssa, jotta ratkaisu on teknisesti ja toiminnallisesti valmis tukemaan turvallista ja hallittua käyttöä heti alusta alkaen.

Osaa varmistaa, että sovitut tietoturvavaatimukset toteutuvat käytännössä

Käyttöönoton yhteydessä tuoteomistajan on varmistettava, että aiemmin sovitut tietoturvavaatimukset todella täyttyvät ennen ohjelmiston siirtämistä tuotantoon. Tämä edellyttää hyväksymiskriteerien läpikäyntiä ja varmistamista, että keskeiset osa-alueet kuten käyttäjähallinta, lokitus, varmuuskopiointi ja tietojen suojaaminen ovat kunnossa. Tuoteomistaja hyödyntää asiantuntijoiden apua käyttöönottotarkastuksissa, tietoturvatestauksessa ja tarvittaessa auditoinneissa, jotta ratkaisu täyttää vaatimukset myös käytännössä. Lisäksi on tärkeää, että roolit ja vastuut tietoturvan näkökulmasta on selkeästi määritelty ja dokumentoitu ennen ohjelmiston käyttöönottoa.

Ymmärtää käyttäjien ja organisaation valmiudet

Ohjelmiston tietoturva ei toteudu pelkästään teknisten ratkaisujen kautta, vaan myös käyttäjien toiminnan kautta. Käyttöönoton onnistuminen edellyttää, että käyttäjät osaavat toimia turvallisesti uuden ohjelmiston kanssa. Tuoteomistajan on osattava arvioida, millaista ohjeistusta, koulutusta ja tukitoimia tarvitaan, jotta tietoturva toteutuu myös käytännön käytössä. Tuoteomistaja osallistuu käyttöönottosuunnitelman laatimiseen ja varmistaa, että dokumentaatio ja koulutus tukevat turvallista käyttöä eri käyttäjäryhmille. Näin vähennetään virheiden ja väärinkäytösten riskiä heti alusta lähtien.

Osaa arvioida ja hallita käyttöönottovaiheen riskit

Käyttöönotto on aina kriittinen vaihe, jossa voi ilmetä teknisiä, toiminnallisia tai tietoturvaan liittyviä riskejä. Tuoteomistajan on tunnistettava mahdolliset siirtymävaiheen riskit, kuten puutteet konfiguraatiossa, käyttöoikeuksissa tai integraatioissa, ja varmistettava, että ne hallitaan ennen laajaa käyttöönottoa. Tämä edellyttää tiivistä yhteistyötä sekä teknisten asiantuntijoiden että liiketoiminnan edustajien kanssa. Riskienhallinta tässä vaiheessa auttaa ehkäisemään tietoturvapoikkeamia ja käyttökatkoja.

Ymmärtää jatkuvuuden merkityksen heti käyttöönotossa

Tietoturva ei pääty käyttöönottoon, vaan sen on jatkuttava saumattomasti osana ylläpitoa ja käyttöä. Tuoteomistajan on varmistettava, että ylläpidon ja tuen prosessit käynnistyvät heti ohjelmiston käyttöön oton yhteydessä. Tämä tarkoittaa, että muun muassa päivitykset, tietoturvaseuranta ja tukipalvelut ovat valmiina toimimaan heti käyttöönoton yhteydessä. Näin luodaan pohja ohjelmiston turvalliselle ja luotettavalle käytölle koko sen elinkaaren ajan.

Keskeiset toimet:

- Varmista, että kaikki sovitut tietoturvavaatimukset ja hyväksymiskriteerit ovat täyttyneet ennen tuotantoon siirtoa.
- Dokumentoi ja selkeytä roolit ja vastuut tietoturvan osalta.
- Arvioi käyttäjien ja organisaation valmiudet turvalliseen käyttöön tarvittavan ohjeistuksen ja koulutuksen järjestämiseksi.
- Osallistu käyttöönottosuunnitelman laadintaan ja varmista riittävä dokumentaatio.
- Tunnista ja hallitse käyttöönottovaiheen riskit.
- Käynnistä ylläpidon ja tuen prosessit heti käyttöönotossa.

KÄYTTÖ JA YLLÄPITO

Käytön ja ylläpidon aikana tuoteomistaja vastaa siitä, että ohjelmiston tietoturva pysyy ajantasaisena ja kehittyy muuttuvien tarpeiden ja uhkien mukana. Työhön kuuluu haavoittuvuuksien hallinta, päivitysten ja valvonnan koordinointi, poikkeamien käsittely sekä yhteistyö toimittajien ja sidosryhmien kanssa. Tavoitteena on varmistaa, että ohjelmiston käyttö on turvallista, sääntelyn mukaista ja tukee liiketoiminnan jatkuvuutta koko elinkaaren ajan.

Ymmärtää haavoittuvuuksien hallinnan merkityksen ohjelmiston turvallisuudelle

Haavoittuvuudet ohjelmistossa tai sen komponenteissa voivat vaarantaa koko palvelun turvallisuuden tai liiketoiminnan jatkuvuuden, joten on tärkeää, että haavoittuvuuksia seurataan ja että ne korjataan viivytyksettä. Haavoittuvuuksien hallinta ei ole vain tekninen tehtävä, vaan vaatii liiketoimintalähtöistä priorisointia ja yhteistyötä toimittajien kanssa. Tuoteomistajan on osattava seurata haavoittuvuustiedotteita (esim. CVE), arvioida niiden vaikutuksia ja varmistaa, että korjaukset toteutetaan hallitusti. On tärkeää ymmärtää, miten haavoittuvuudet vaikuttavat palvelun käytettävyyteen ja asiakasluottamukseen, ja miten korjaustoimet priorisoidaan liiketoimintariskien perusteella.

Osaa hallita päivityksiä ja korjauksia

Ohjelmiston ja sen komponenttien ajantasaisuus on keskeinen osa tietoturvaa. Tuoteomistajan tulee ymmärtää päivityskäytäntöjen vaikutus tietoturvaan, käytettävyyteen ja toiminnallisuuksiin. Päivitysten hallinta edellyttää suunnitelmallisuutta, dokumentointia ja yhteistyötä toimittajien kanssa. Tuoteomistajan tehtävänä on varmistaa, että päivitykset toteutetaan hallitusti ja että niihin liittyvät riskit ja vaikutukset on arvioitu etukäteen.

Ymmärtää lokituksen ja valvonnan roolin poikkeamien havaitsemisessa

Lokitus ja valvonta ovat perusta poikkeamien havaitsemiselle ja selvittämiselle. Tuoteomistajan tulee ymmärtää, mitä lokitietoja kerätään, miksi niitä tarvitaan ja miten ne tukevat häiriöiden ja hyökkäysten tunnistamista. Hänen vastuullaan on varmistaa, että tarvittavat lokitiedot kerätään. Lisäksi tuoteomistajalla tulee olla perustiedot hyökkäysten ja häiriöiden tunnistamisesta,

Jatkuva parantaminen on tuoteomistajan tärkein tietoturvateko.

ymmärrys käyttömallien poikkeamien seurannasta sekä kyky tulkita valvontaraportteja ja eskaloida ne oikeille tahoille. Tämä osaaminen varmistaa, että poikkeamat havaitaan ajoissa ja niihin voidaan reagoida tehokkaasti.

Osaa toimia tietoturvapoikkeamatilanteessa

Tietoturvapoikkeamat vaativat nopeaa ja järjestelmällistä toimintaa. Tuoteomistajan tulee tuntea organisaation prosessit ja oma roolinsa poikkeamien käsittelyssä sekä varmistaa, että eskalointi- ja ilmoituskanavat toimivat. Osaaminen kattaa myös ulkoiset raportointivelvoitteet, kuten NIS2- ja CRA-sääntelyn mukaiset ilmoitukset. Lisäksi tuoteomistajan on kyettävä johtamaan reagointia liiketoimintanäkökulmasta, dokumentoimaan tapahtumat ja raportoimaan ne selkeästi.

Osaa hallita käyttöoikeuksia tietoturvaperiaatteiden mukaisesti

Käyttöoikeuksien hallinta on olennainen osa ohjelmiston turvallisuutta. Tuoteomistajan tulee ymmärtää vähimmän oikeuden periaate ja roolipohjaisen käyttöoikeuksien hallinnan vaikutus tietoturvaan. Tuoteomistajan tehtävänä on varmistaa, että käyttöoikeudet ovat ajan tasalla, niitä tarkastetaan säännöllisesti ja että roolit vastaavat organisaation tarpeita koko ohjelmiston elinkaaren ajan.

Tuntee tietosuojan ja sääntelyn vaatimukset

Tuoteomistajan tulee tuntea ohjelmiston käsittelemän datan luonne ja siihen liittyvät suojausvaatimukset. Tuoteomistajan on ymmärrettävä henkilötietojen käsittelyn ja suojaamisen periaatteet sekä osattava varmistaa, että ohjelmisto noudattaa tietosuojalainsäädäntöä (esim. GDPR). Lisäksi on huomioitava muu ohjelmistoon tai palveluun soveltuva sääntely, kuten kyberturvallisuutta koskevat yleiset vaatimukset (esim. NIS2, CRA) sekä toimialakohtaiset säädökset ja standardit (esim. terveydenhuolto, rahoitusala). Tuoteomistajan vastuulla on varmistaa, että sääntelyvaatimukset on tunnistettu ja muutettu selkeiksi toimenpiteiksi, sekä tunnistaa ja arvioida koulutustarpeet, jotta sääntelyn vaatimukset pystytään täyttämään.

Osaa tunnistaa ja hallita ohjelmiston tietoturvariskejä

Riskienhallinta on jatkuva prosessi ohjelmiston käytössä ja ylläpidossa. Tuoteomistajan tulee kyetä tunnistamaan ohjelmiston ja palvelun tietoturvariskit sekä arvioimaan niiden vaikutuksia. Riskienhallinta tukee päätöksentekoa, kuten suojaustoimenpiteiden priorisointia. Tuoteomistajan on osattava eskaloida riskejä ja tehdä yhteistyötä sidosryhmien kanssa – erityisesti silloin, kun toimittajan riskit voivat vaikuttaa omaan palveluun.

Ohjelmistot sisältävät usein ulkopuolisia komponentteja, kuten kirjastoja ja palveluita. Tuoteomistajan tulee ymmärtää näihin liittyvät tietoturvariskit, seurata niiden päivityksiä ja tehdä yhteistyötä toimittajien kanssa. Jos ohjelmisto on kytköksissä muihin järjestelmiin, tuoteomistajan on hyvä ymmärtää rajapintojen riskien ja riippuvuuksien hallintaa.

Osaa seurata sopimuksia ja palvelutasoja tietoturvan näkökulmasta

Tuoteomistajan tulee ymmärtää, miten ylläpitoon ja tietoturvaan liittyvät vastuut jakautuvat eri osapuolille. On osattava seurata velvoitteiden ja palvelutasojen täyttymistä, käynnistää toimenpiteitä tarvittaessa ja muuntaa omat velvoitteet konkreettisiksi toimenpiteiksi. Lisäksi tuoteomistajan on hallittava sopimuksen elinkaarta tietoturvan näkökulmasta: huomioitava ylläpidon aikana esiin nousevat muutostarpeet esimerkiksi sääntelyn, riskien tai palvelun muutosten perusteella, arvioitava niiden vaikutus sopimuksiin ja palvelutasoihin sekä varmistettava, että sopimuksia päivitetään vastaamaan muuttuvia tietoturvavaatimuksia.

Tuntee jatkuvuuden ja palautumisen perusperiaatteet

Tuoteomistajan tulee ymmärtää, miten ohjelmiston käytön jatkuvuus ja palautuminen on järjestetty. Tämä kattaa muun muassa varmuuskopioinnin, palautustes-

tit ja kyvyn arvioida liiketoimintavaikutuksia häiriötilanteissa. Vaikka tekninen toteutus ei ole tuoteomistajan vastuulla, hänen tulee varmistaa, että jatkuvuuden hallinta on huomioitu ylläpidossa ja että siihen liittyvät toimenpiteet ovat asianmukaisesti suunniteltuja ja toteutettuja.

Tuoteomistajan vastuulla on varmistaa, että jatkuvuuteen ja palautumiseen liittyvät vastuut on dokumentoitu ja tiedossa eri osapuolilla. Lisäksi hänen tulee koordinoida tai varmistaa harjoitusten toteutuminen, kuten palautumisharjoitukset ja häiriötilanneskenaariot, jotta toimintamallit ovat testattuja ja henkilöstö on tietoinen rooleistaan. Dokumentaation tulee olla ajan tasalla ja helposti saatavilla, jotta jatkuvuuden hallinta on tehokasta ja todennettavissa.

Osaa valmistautua auditointeihin ja hyödyntää niiden tuloksia

Auditoinnit ja tarkastukset ovat osa ohjelmiston tietoturvan varmistamista. Tuoteomistajan tulee osata valmistautua auditointeihin ja varmistaa, että tarvittavaa dokumentaatiota ylläpidetään. On osattava tehdä yhteistyötä sisäisten ja ulkoisten tarkastajien kanssa, ymmärrettävä tarkastusten tulokset ja koordinoitava korjaavat toimenpiteet. Näin auditoinnit tukevat ohjelmiston jatkuvaa kehittämistä ja tietoturvan varmistamista.

Osaa viestiä ja raportoida tietotuvasta eri sidosryhmille

Tuoteomistajan tulee kyetä viestimään tietoturvaan liittyvistä asioista selkeästi ja ymmärrettävästi eri sidosryhmille. Tämä tarkoittaa kykyä tuottaa kohdennettuja tietoturvaraportteja päätöksenteon tueksi, viestiä käyttäjille tietoturvakäytännöistä ja ohjeista, sekä keskustella teknisistä vaatimuksista IT-tiimin kanssa. Johdon suuntaan viestinnän tulee tukea strategista päätöksentekoa ja riskienhallintaa. Tuoteomistajan rooliin kuuluu myös osallistuminen kriisiviestintään ja viranomaisraportointiin esimerkiksi tietoturvapoikkeamien yhteydessä. Viestinnän tulee perustua ajantasaiseen ja luotettavaan tietoon, olla suunnitelmallista ja säännöllistä, sekä tukea eri osapuolten ymmärrystä omista vastuistaan tietoturvan toteuttamisessa.

Ymmärtää tiedonhallinnan vaatimukset ja käytännöt

Tuoteomistajan tulee tuntea ohjelmiston käsittelemän tiedon luonne, suojaustaso ja säilytysaikavaatimukset. On varmistettava, että tiedon käsittely, säilytys, arkistointi ja poisto toteutuvat organisaation ohjeistuksen ja soveltuvan sääntelyn mukaisesti. Tämä edellyttää käytännön ymmärrystä tiedon elinkaaren hallinnasta, esimerkiksi siitä, miten tietoa luokitellaan, milloin se poistetaan tai siirretään arkistoon. Lisäksi tulee varmistaa, ettei tarpeetonta tai vanhentunutta tietoa jää järjestelmiin. Tuoteomistajan tulee huolehtia siitä, että nämä vaatimukset on huomioitu ohjelmiston toiminnallisuuksissa ja ylläpidossa.

Osaa edistää tietoturvan jatkuvaa parantamista

Tietoturva ei ole kertaluonteinen tehtävä, vaan jatkuvaa kehittämistä. Tuoteomistajan tulee kyetä tunnistamaan kehityskohteita esimerkiksi palautteiden ja auditointien perusteella, arvioida käytäntöjä säännöllisesti ja seurata alan muutoksia. Tuoteomistajan tulee tehdä yhteistyötä tietoturvatiimin ja sidosryhmien kanssa kehitystoimissa ja sisällyttää tietoturva jatkuvaan tuote- ja palvelukehitykseen. Lisäksi tuoteomistajan tulee arvioida toteutettujen toimenpiteiden vaikuttavuutta mittareiden avulla ja tunnistaa koulutuksen tarpeet organisaatiossa.

Keskeiset toimenpiteet:

- Seuraa ja priorisoi haavoittuvuuksia liiketoimintariskien perusteella ja varmista korjausten toteutuminen hallitusti.
- Varmista, että ohjelmiston ja komponenttien päivitykset toteutetaan suunnitelmallisesti ja dokumentoidusti.
- Huolehdi, että tarvittavat lokitiedot kerätään ja valvontaraportit tulkitaan ja eskaloidaan oikein.
- Tunnista roolisi ja vastuusi poikkeaminen käsittelyssä ja varmista raportointivelvoitteiden täyttyminen.

- Tarkasta ja päivitä käyttöoikeudet säännöllisesti vähimmän oikeuden periaatteen mukaisesti.
- Varmista, että sääntelyvaatimukset on tunnistettu ja muutettu konkreettisiksi toimenpiteiksi.
- Tunnista ja arvioi ohjelmiston tietoturvariskit sekä eskaloi ne tarvittaessa. Tee yhteistyötä sidosryhmien kanssa riskien vähentämiseksi.
- Seuraa kolmannen osapuolen komponenttien ja riippuvuuksin tietoturvaa.
- Huolehdi, että sopimuksiin ja palvelutasoihin liittyvät tietoturvavelvoitteet toteutuvat ja päivittyvät.
- Varmista jatkuvuuden ja palautumisen huomioiminen ylläpidossa ja harjoitusten toteutuminen.
- Varaudu auditointeihin varmistamalla, että dokumentaatio on ajan tasalla ja hyödynnä auditointituloksia tietoturvan kehittämisessä.
- Viesti tietoturvasta selkeästi tarvittaville sidosryhmille ja tiedä vastuusi kriisiviestinnässä.
- Huolehdi tiedon käsittelystä, luokittelusta, säilytyksestä ja poistosta sääntelyn mukaisesti koko ohjelmiston elinkaaren ajan.
- Tunnista kehityskohteet, arvioi tietoturvakäytäntöjen vaikuttavuutta mittareiden avulla ja sisällytä tietoturva jatkuvaan kehitykseen.

KÄYTÖSTÄ POISTO

Käytöstä poiston vaiheessa tuoteomistajan vastuulla on varmistaa, että ohjelmiston alasajo toteutetaan hallitusti ja tietoturvavaatimusten mukaisesti. Tähän kuuluu tietojen turvallinen poistaminen tai anonymisointi, pääsyoikeuksien poistaminen, ulkoisten riippuvuuksien hallinta sekä dokumentointi ja viestintä, jotka varmistavat prosessin jäljitettävyyden ja sääntelyn noudattamisen.

Ymmärtää tietoturvan vaatimukset ohjelmiston käytöstä poiston vaiheessa

Tuoteomistajan tulee tuntea ohjelmiston käytöstä poiston tietoturvavaatimukset. Henkilötiedot ja luottamuksellinen data tulee poistaa tai anonymisoida turvallisesti organisaation käytäntöjen ja sääntelyn mukaisesti, kuten GDPR:n vaatimukset huomioiden. Tuoteomistajan tulee tunnistaa sovellettavat säilytysajat ja arkistointivelvoitteet, sekä varmistaa, että mahdolliset arkistointitarpeet ja lainsäädännölliset velvoitteet täyttyvät ennen tietojen lopullista poistoa.

Hallitsee käytöstä poiston riskit ja jälkiseurannan

Tuoteomistajan tulee tunnistaa ohjelmiston elinkaaren lopun tietoturvan erityispiirteet ja niihin liittyvät riskit, kuten unohtuneet integraatiot, vanhat pääsyoikeudet ja puutteellisesti dokumentoidut rajapinnat. Poistoprosessit on suunniteltava huolellisesti, jotta ne minimoivat tietovuodon, väärinkäytön ja muut mahdolliset tietoturvaloukkaukset. Tuoteomistaja vastaa poistotoimenpiteiden seurannasta ja varmistaa, että jälkiseuranta ja auditointilokit ovat kunnossa. Näin voidaan todentaa, että elinkaaren lopetus on suoritettu turvallisesti ja että tarvittavat lokitiedot säilytetään sääntelyn mukaisesti.

Ymmärtää pääsyoikeuksien hallinnan merkityksen käytöstä poiston yhteydessä

Tuoteomistajan tulee ymmärtää identiteetin- ja pääsynhallinnan (IAM) vaikutukset käytöstä poiston turvallisuuteen. On varmistettava, että kaikki käyttöoikeudet, API-avaimet, salasanat ja tunnukset poistetaan tai mitätöidään. Lisäksi on tarkistettava, ettei entisillä käyttäjillä tai kolmansilla osapuolilla ole enää pääsyä järjestelmään, tietoihin tai integraatioihin. Erityisroolit, kuten ylläpito, tuki ja integraatiot, on tunnistettava ja niiden oikeudet poistettava asianmukaisesti.

Tuntee kolmansien osapuolten hallinnan tietoturvavaatimukset

Tuoteomistajan on osattava tunnistaa ohjelmistoon liittyvät ulkoiset riippuvuudet, kuten pilvipalvelut, integraatiot ja alihankkijat, ja varmistaa niiden asianmukainen alasajo käytöstä poiston yhteydessä. On huolehdittava, että myös kolmansilta osapuolilta pois-

tetaan pääsyoikeudet, data käsitellään ja poistetaan turvallisesti ja sopimusten mukaisesti, ja että palveluntarjoajilta saadaan tarvittavat todistukset tietojen tuhoamisesta. Lisäksi tuoteomistajan on varmistettava, että sopimuksiin sisältyvät tietoturvavelvoitteet toteutuvat myös ohjelmiston käytön päättymisen jälkeen, mukaan lukien dokumentointi, ilmoitukset ja mahdolliset jälkiseurannan vaatimukset.

Osaa dokumentoida ja viestiä tietoturvatoimenpiteet käytöstä poiston yhteydessä

Tuoteomistajan vastuulla on varmistaa, että kaikki ohjelmiston käytöstä poiston tietoturvaan liittyvät päätökset, toimenpiteet ja vastuut dokumentoidaan riittävällä tarkkuudella. On ymmärrettävä, miten dokumentointi toteutetaan siten, että auditointi ja jäljitettävyys säilyvät, ja että lokitiedot ovat suojattuja ja saatavilla tarvittavan ajan. Lisäksi on huolehdittava siitä, että käytöstä poistoon liittyvät vastuut ovat selkeästi määritelty, ja että kaikki osapuolet tietävät, kuka vastaa tietojen lopullisesta poistamisesta. Tuoteomistajan on myös viestiä sidosryhmille selkeästi, mitä toimenpiteitä on tehty ja miksi.

Keskeiset toimet:

- Tunnista poistettavat tiedot.
- Arvioi elinkaaren lopun tietoturvariskit ja suunnittele poistoprosessit niiden minimoimiseksi.
- Tarkasta säilytysajat sekä sopimus- ja arkistointivelvoitteet suunnittelun yhteydessä.
- Seuraa poistotoimenpiteiden toteutumista ja varmista auditointilokien säilytys.
- Varmista, että kaikki käyttöoikeudet ja tunnukset on poistettu tai mitätöity.
- Tunnista kolmansien osapuolten riippuvuudet ja varmista, että ne on kaikki katkaistu hallitusti.
- Varmista sopimusvelvoitteiden täyttyminen ja pyydä tarvittaessa palveluntarjoajilta todistukset tietojen poistosta.
- Dokumentoi kaikki poistoon liittyvät tietoturvapäätökset ja -toimenpiteet.
- Viesti selkeästi ja ajantasaisesti sidosryhmille.

Poista oikein – suojaa tiedot loppuun asti.

Sopimusjuristi

Tässä osiossa käsitellään, millaista tietoturvaosaamista ohjelmistojen hankinnassa tai palvelusopimusten laadinnassa mukana olevilta juristeilta edellytetään sopimuksen elinkaaren eri vaiheista ja miten hän voi omalla toiminnallaan edistää ohjelmistoturvallisuutta. Osiossa lähestytään aihetta sopimuksen elinkaaren kautta.

Juristin osaamisella sääntely ja riskienhallinta muuttuvat konkreettisiksi sopimusehdoiksi.

MIKSI OHJELMISTOTURVALLISUUS KUULUU SOPIMUSJURISTILLE?

Sopimusjuristi varmistaa, että organisaation ohjelmistohankintoihin liittyvät sopimukset tukevat tietoturvallisuutta ja ovat lainmukaisia. Hän tuntee keskeiset tietosuoja- ja tietoturvasäädökset sekä osaa sisällyttää ne selkeästi ja kattavasti sopimusehtoihin.

Juristin tehtävä on muotoilla sopimukset niin, että vastuut, velvoitteet ja riskit ovat selkeitä ja tasapainossa molempien osapuolten kannalta. Hän huolehtii, että sopimuksiin sisältyy riittävät turva- ja valvontamekanismit, kuten vaatimukset tietoturvapäivityksistä, haavoittuvuuksien hallinnasta sekä palvelutasosta.

Sopimusjuristi osallistuu neuvotteluihin ja varmistaa, että sopimukset mahdollistavat organisaation turvallisuusvaatimusten toteutumisen koko ohjelmiston elinkaaren ajan. Hän seuraa sopimusten ajantasaisuutta ja tukee tarvittaessa niiden päivittämistä vastaamaan muuttuvia turvallisuusuhkia ja sääntelyvaatimuksia.

Rooli on keskeinen organisaation riskienhallinnan ja vaatimustenmukaisuuden varmistamisessa sekä toiminnan luotettavuuden tukemisessa juridisesta näkökulmasta.

Tiivistelmä

SOPIMUSJURISTIN OSAAMISTARPEET

- Ymmärtää sopimuksen roolin ohjelmistoturvallisuuden mahdollistajana ja riskienhallinnan välineenä.
- Hallitsee tietoturvaan liittyvän keskeisen sääntelyn ja osaa muotoilla vaatimukset selkeiksi sopimusehdoiksi.
- Osaa yhdistää liiketoiminnan tavoitteet ja tietoturvavaatimukset sopimuksessa.
- Tunnistaa sopimuksella hallittavat riskit ja osaa käyttää sopimusta niiden pienentämiseen, siirtämiseen tai jakamiseen.
- Osaa neuvotella ja perustella tietoturvavaatimukset sekä tunnistaa kriittiset ehdot.
- Varmistaa sopimuksen ajantasaisuuden ja muutosmekanismit muuttuvissa olosuhteissa.
- Osaa käsitellä poikkeamia ja sopimusrikkomuksia tietoturvan näkökulmasta.
- Arvioi sopimuksen toteutumista, tunnistaa päättymisen velvoitteet ja valmistaa tarvittaessa turvallisen uusimisen.

Sopimusjuristi tekee tietoturvasta sitovan.

SOPIMUKSEN SUUNNITTELU JA VALMISTELU

Sopimuksen suunnittelu- ja valmisteluvaiheessa juristin tehtävänä on varmistaa, että tietoturva huomioidaan osana sopimuksen rakennetta ja tavoitteita. Sopimus ei ainoastaan määritä kaupallisia ehtoja, vaan luo perustan ohjelmiston turvallisuudelle, vastuunjaolle ja riskienhallinnalle koko elinkaaren ajaksi.

Ymmärtää tietoturvan roolin sopimuksessa

Sopimusjuristin rooli ohjelmistoturvallisuuden varmistamisessa alkaa jo sopimuksen suunnittelu- ja valmisteluvaiheessa. On ymmärrettävä, että sopimus ei ole vain kaupallinen asiakirja vaan sillä luodaan edellytykset myös ohjelmistoturvallisuudelle, liiketoiminnan jatkuvuudelle ja palvelun saatavuudelle. Sopimus on konkreettinen väline, jolla määritellään vastuut, velvoitteet ja riskienhallintakeinot tietoturvan varmistamiseksi. Sopimuksen tulee kattaa koko ohjelmiston elinkaari, mukaan lukien kehitys, käyttöönotto, ylläpito ja mahdollinen alasajo. Juristin on hahmotettava, miten sopimus tukee organisaation ja ohjelmiston tietoturvaa kokonaisvaltaisesti.

Ymmärtää sääntelyn vaatimukset ja niiden vaikutuksen ohjelmistoihin

Juristin tulee hallita soveltuvat lait ja määräykset, kuten hankintalaki, GDPR, NIS2, CRA sekä toimialakohtainen sääntely. Osaaminen tarkoittaa kykyä tunnistaa, mitkä sääntelyvaatimukset koskevat käsillä olevaa sopimusta ja miten ne muokkaavat sen sisältöä. Juristin tehtävä on tulkita sääntelyn velvoitteet ja muotoilla niistä konkreettisia, juridisesti kestäviä sopimusehtoja, joissa vastuunjako ja tietosuojavaatimukset on selkeästi määritelty.

Ymmärtää liiketoiminnan ja tietoturvan yhteiset tavoitteet

Sopimusjuristin on osattava yhdistää sopimuksessa liiketoiminnan tavoitteet ja tietoturvavaatimukset. On osattava kääntää tietoturvavaatimukset liiketoimintalähtöisiksi sopimusehdoiksi ja varmistaa, että sopimus tukee molempia näkökulmia. Käytännössä tämä edellyttää tiivistä yhteistyötä eri asiantuntijoiden, kuten tietoturva-asiantuntijoiden, tuoteomistajien ja palvelupäälliköiden, kanssa.

Osaa valmistella tietoturvavaatimuksia sopimukseen

Tietoturvavaatimukset on pystyttävä muotoilemaan realistisiksi, mitattaviksi, juridisesti selkeiksi sekä toteuttamiskelpoisiksi. Näitä voivat olla esimerkiksi auditointioikeudet, poikkeamien raportointivelvoitteet, salaukseen ja varmuuskopiointiin liittyvät ehdot, vastuiden määrittely sekä dokumentointivelvoitteet. Juristi huolehtii siitä, että vastuut, tiedonkäsittelyehdot, dokumentointivelvoitteet ja palvelutasovaatimukset muotoillaan sopimukseen selkeästi, sääntelyn mukaisesti ja sopimuksen tavoitteita tukevalla tavalla. Hyvin laaditut ehdot eivät ainoastaan suojaa organisaatiota, vaan myös helpottavat myöhempää sopimuksen seurantaa ja hallintaa.

Ymmärtää, miten ohjelmiston riskejä voidaan pienentää sopimuksella

Sopimusjuristin on ymmärrettävä, miten sopimuksella voidaan pienentää ohjelmistoon liittyviä riskejä, kuten palvelukatkoksia, tietovuotoja ja toimitusketjujen haavoittuvuuksia. Sopimusriskejä syntyy puolestaan mm. epäselvistä vastuista ja puutteellisista velvoitteista. Juristin tehtävänä on arvioida, miten sopimuksen rakenne ja ehdot voivat hallita näitä riskejä. Sopimuksella voidaan hallita näitä riskejä esimerkiksi määrittämällä selkeät sanktiot, rajaamalla tai jakamalla vastuuta sekä sisällyttämällä mekanismeja, jotka mahdollistavat sopimuksen joustavan päivittämisen muuttuvassa uhkakentässä. Näin sopimuksesta tulee olennainen väline riskienhallinnassa.

Keskeiset toimet:

- Varmista, että sopimuksen tietoturvavaatimukset kattavat koko ohjelmiston elinkaaren.
- Tunnista ja sisällytä sääntelyn velvoitteet selkeiksi ja sitoviksi sopimusehdoiksi.
- Muotoile tietoturvavaatimukset selkeiksi, mitattaviksi ja toteutumiskelpoisiksi.
- Varmista, että vastuut ja velvoitteet on kirjattu selkeästi, ja sisällytä sopimukseen auditointi- ja raportointivelvoitteet sekä valvontaoikeudet.
- Hyödynnä asiantuntijoiden osaamista tietoturvaan liittyvien ehtojen muotoilussa.
- Sisällytä sopimukseen mekanismit, joilla sopimusta voidaan tarvittaessa päivittää muuttuvien uhkien ja vaatimusten mukaan.

Juristi kääntää vaatimukset sopimuskielelle, jotta tietoturva ei jää epäselväksi.

SOPIMUSNEUVOTTELUT JA HYVÄKSYNTÄ

Neuvotteluvaiheessa sopimusjuristi toimii tasapainottajana liiketoiminnan tavoitteiden ja tietoturvavaatimusten välillä. Jokainen neuvottelussa tehty päätös vaikuttaa siihen, miten hyvin ohjelmiston turvallisuus ja vastuut toteutuvat tulevaisuudessa. Sopimusjuristin tehtävänä on varmistaa, että tietoturvaa koskevat ehdot ovat selkeitä, sitovia ja toteuttamiskelpoisia.

Ymmärtää neuvottelujen vaikutuksen tietoturvaan

Sopimusjuristin on ymmärrettävä, että neuvotteluvaiheessa tehdyt ratkaisut ja kompromissit määrittävät pitkälti, millä tasolla ohjelmistoturvallisuus toteutuu. On ymmärrettävä, että epäselvät tai liian väljät ehdot voivat heikentää tietoturvaa koko ohjelmiston elinkaaren ajaksi. Sopimusjuristin tulee osata löytää ratkaisut, joissa tietoturva ja liiketoiminnan tavoitteet pysyvät tasapainossa, ja samalla varmistaa, että sopimus tukee organisaation riskienhallintaa ja luotettavuutta pitkällä aikavälillä.

Osaa neuvotella tietoturvavaatimuksista

Sopimusjuristi toimii tietoturvan puolestapuhujana ja varmistaa, että vaatimukset pysyvät esillä koko neuvotteluprosessin ajan, eivätkä jää muiden tavoitteiden varjoon. Vaatimukset on osattava kääntää juridisesti selkeiksi ja liiketoimintalähtöisiksi sopimusehdoiksi, jotka ovat toteuttamiskelpoisia ja mitattavia. Lisäksi on kyettävä neuvottelemaan tasapainoiset ehdot, jotka suojaavat organisaatiota mutta ovat myös hyväksyttäviä vastapuolelle.

Osaa arvioida tietoturvan ja liiketoiminnan kompromissit

Sopimusjuristin tulee tunnistaa, miten neuvotteluissa tehtävät kompromissit ja painotukset voivat vaikuttaa ohjelmiston tietoturvaan ja riskienhallintaan. On osattava arvioida, mitkä sopimusehdot ovat kriittisiä tietoturvan ja tietosuojan kannalta ja missä voidaan joustaa ilman, että turvallisuus vaarantuu. Kriittisiä sopimusehtoja voivat olla esimerkiksi tietoturvapäivitysten aikataulut, tietosuojavelvoitteet sekä poikkeamien ilmoittamista ja käsittelyä koskevat menettelyt. Sopimusjuristin tulee ymmärtää, että kustannukset, aikataulut tai markkinatilanne voivat tuoda paineita heikentää tietoturvaa, mutta kriittisistä vaatimuksista ei voida tinkiä.

Osaa varmistaa sääntelyn vaatimusten toteutumisen

Juristin tehtävänä on huolehtia, että sopimuksen ehdot täyttävät soveltuvan sääntelyn (esim. GDPR, NIS2, CRA) ja että vaatimukset on ilmaistu sitovasti ja riittävän selkeästi. Erityistä huomiota tulee kiinnittää tietosuojavelvoitteisiin, viranomaisraportointiin liittyviin ehtoihin sekä siihen, että osapuolten vastuut on määritelty yksiselitteisesti ja sääntelyn mukaisesti. Juristi varmistaa, että sääntely ei jää sopimuksessa yleisluontoiseksi viittaukseksi, vaan konkretisoituu toteuttamiskelpoisiksi sopimusehdoiksi, ja että sopimus mahdollistaa myös sääntelymuutosten huomioimisen.

Hallitsee riskien pienentämisen, siirtämisen ja jakamisen keinot

Sopimusjuristin tulee tunnistaa tilanteet, joissa riskien siirto, rajoittaminen tai jakaminen on tarpeen, ja osata neuvotella niistä sopimukseen toimivat ratkaisut. Sopimuksessa tulee huomioida myös toimitusketjuriskit. Sopimusjuristin tulee ymmärtää, miten vastuunrajoitukset, vahingonkorvaukset, sanktiot ja vakuutukset voivat toimia riskienhallinnan välineinä, ja että uhkakenttä ja riskit voivat muuttua sopimuksen elinkaaren aikana. On varmistettava, että sopimus mahdollistaa joustavat muutokset ja päivitykset, jolloin sopimuksesta tulee aktiivinen työkalu organisaation riskienhallinnan ja jatkuvuuden tueksi.

Osaa hyödyntää muita asiantuntijoita

Sopimusjuristi ei voi hallita kaikkia teknisiä ja operatiivisia yksityiskohtia, joten hänen tulee osata hyödyntää asiantuntijoita neuvotteluissa. Tämä tarkoittaa esimerkiksi teknisten asiantuntijoiden osallistamista ehdotusten toteutettavuuden arviointiin, tietoturva-asiantuntijoiden konsultointia haavoittuvuuksien hallinnan ja päivitysvelvoitteiden määrittelyssä sekä tuoteomistajien ja palvelupäälliköiden mukaan ottamista liiketoimintavaatimusten ja käytännön toteutuksen yhteensovittamiseksi. Tämä varmistaa, että sopimusehdot perustuvat sekä tekniseen että liiketoiminnalliseen ymmärrykseen ja ovat realistisia toteuttaa.

Osaa varmistaa tietoturvan sopimuksen hyväksymisessä

Hyväksymisvaiheessa sopimusjuristin tehtävänä on tarkistaa, että lopulliset ehdot tukevat sovittuja tietoturvavaatimuksia eikä niihin ole neuvottelujen aikana jäänyt puutteita tai epäselvyyksiä. On varmistettava, että sopimus on sääntelyn mukainen, että kriittiset turvallisuusehdot (kuten päivitysvelvoitteet ja poikkeamien raportointi) ovat mukana, ja että organisaation asiantuntijat ovat hyväksyneet lopullisen sisällön. Lisäksi on huolehdittava, että hyväksymisprosessista jää selkeä jälki, joka osoittaa sopimuksen tietoturvaehdot tarkistetuksi ja hyväksytyksi ennen allekirjoitusta.

Maailma muuttuu, sopimuksen on kehityttävä sen mukana.

Keskeiset toimet:

- Pidä tietoturva mukana jokaisessa neuvotteluvaiheessa.
- Muotoile tietoturvavaatimukset juridisesti selkeiksi, mitattaviksi ja toteuttamiskelpoisiksi sopimusehdoiksi.
- Tunnista kriittiset tietoturvaehdot, joista ei voida joustaa.
- Varmista, että sopimus täyttää kaikki soveltuvat sääntelyvaatimukset ja että vastuut on määritelty yksiselitteisesti.
- Hyödynnä sopimusta riskienhallinnan työkaluna neuvottelemalla selkeät vastuut, sanktiot sekä raportointivelvoitteet.
- Hyödynnä asiantuntijoita, jotta sopimusehdot perustuvat sekä tekniseen että liiketoiminnalliseen ymmärrykseen.
- Huolehdi, että sopimus mahdollistaa muutokset ja päivitykset muuttuvien uhkien ja sääntelyvaatimusten varalta.
- Varmista, että kaikki tietoturvaa koskevat ehdot on tarkistettu ja hyväksytty ennen sopimuksen allekirjoitusta.

SOPIMUKSEN HALLINNOINTI

Sopimuksen hallinnointi on jatkuva prosessi, jossa varmistetaan, että sopimusehdot tukevat tietoturvan toteutumista koko sen elinkaaren ajan. Sopimusjuristin tulee osata tulkita sopimusta muuttuvissa olosuhteissa ja tunnistaa päivitystarpeet yhteistyössä eri asiantuntijoiden kanssa, jotta sopimus tukee organisaation tietoturvaa koko ohjelmiston elinkaaren ajan.

Ymmärtää sopimuksen roolin tietoturvan jatkuvassa toteutumisessa

Sopimus ei ole pelkkä staattinen asiakirja, vaan keskeinen työkalu organisaation tietoturvan ylläpitämisessä koko ohjelmiston elinkaaren ajan. Sopimusjuristin tulee yhteistyössä muiden asianosaisten kanssa varmistaa, että sopimuksen rakenteet ja ehdot mahdollistavat organisaation turvallisuusvaatimusten toteutumisen myös allekirjoituksen jälkeen ja muuttuvissa olosuhteissa. Tietoturvan jatkuvaa toteutumista on tuettava esimerkiksi tulkitsemalla ehtoja ja osallistumalla sopimuksen seurantaan.

Osaa hallita sopimuksen muutoksia ja päivittää ehtoja

Tietoturvavaatimukset eivät ole pysyviä, vaan ne voivat muuttua sääntelyn, uhkakuvan, teknologian tai liiketoiminnan tarpeiden muuttuessa. Sopimusjuristin on osattava tunnistaa tilanteet, joissa sopimusta on päivitettävä, ja huolehdittava siitä, että muutokset tehdään hallitusti, dokumentoidusti ja sopimuksen mukaisesti. Tämä edellyttää, että sopimukseen on sisällytetty toimivat muutosmekanismit, kuten tarkistusväleihin perustuvat katselmukset, muutosesitysten käsittelyprosessit ja mahdollisuus ehtojen uudelleenneuvotteluun. Sopimusjuristi tukee myös muutosten vaikutusten arviointia ja varmistaa, että uudet ehdot ovat yhteensopivia alkuperäisen sopimuksen rakenteen ja tavoitteiden kanssa.

Osaa käsitellä poikkeamia ja sopimusrikkomuksia tietoturvan näkökulmasta

Sopimusjuristin on osattava määritellä ja soveltaa menettelytapoja, joilla poikkeamat ja sopimusrikkomukset käsitellään tietoturvan kannalta. Tämä voi tarkoittaa esimerkiksi tietoturvaloukkausta, auditointioikeuden rajoittamista, raportointivelvoitteiden laiminlyöntiä tai palvelutason alittamista. On osattava arvioida, miten sopimusehdot mahdollistavat tilanteeseen puuttumisen, millaisia seuraamuksia voidaan soveltaa ja mitä korjaavia toimenpiteitä voidaan vaatia. Sopimusjuristi tukee myös dokumentoinnissa ja viranomaisyhteistyössä, mikäli poikkeama liittyy sääntelyyn.

Sopimuksen loppu on uuden turvallisemman sopimuksen alku.

Ymmärtää yhteistyön merkityksen sopimuksen hallinnassa

Sopimuksen hallinnointi edellyttää jatkuvaa yhteistyötä eri asiantuntijoiden kanssa. Juristin on ymmärrettävä, miten sopimuksen tietoturvaehdot kytkeytyvät käytännön toimintaan, ja varmistettava, että sopimus tukee organisaation kykyä ylläpitää ja kehittää tietoturvaa palvelun aikana. Tämä tarkoittaa esimerkiksi yhteistyötä tietoturva-asiantuntijoiden kanssa auditointien ja poikkeamien käsittelyssä, palvelupäälliköiden kanssa sopimuksen seurannassa sekä hankintatoimen kanssa mahdollisissa jatkosopimus- tai muutosneuvotteluissa. Sopimusjuristi toimii linkkinä juridisten ehtojen ja operatiivisen toteutuksen välillä.

Keskeiset toimet:

- Tarkasta säännöllisesti, että sopimus vastaa ajankohtaisia sääntelyvaatimuksia ja uhkakuvia.
- Käynnistä sopimuksen päivitysprosessi, kun tietoturvavaatimukset muuttuvat.
- Määrittele menettelytavat poikkeamien ja sopimusrikkomusten käsittelyyn tietoturvan näkökulmasta.
- Hyödynnä asiantuntijoita sopimuksen valvonnassa, auditoinneissa, poikkeamien käsittelyssä ja muutosneuvotteluissa.

SOPIMUKSEN UUSIMINEN TAI PÄÄTTÄMINEN

Sopimuksen uusimisen tai päättämisen yhteydessä sopimusjuristin tehtävänä on varmistaa, että tietoturvan ja tietosuojan velvoitteet toteutuvat myös sopimussuhteen päättyessä. Sopimusjuristin tulee osata arvioida sopimuksen toteutumista, hallita tietojen ja pääsyoikeuksien sopimukselliset velvoitteet, tunnistaa päättymiseen liittyvät riskit ja valmistella sopimuksen uusiminen siten, että tietoturva säilyy ja kehittyy myös muutosten myötä.

Osaa arvioida nykyisen sopimuksen toteutumista

Sopimusjuristin tulee osata arvioida, miten voimassa oleva sopimus on toteuttanut sovitut tietoturvavaatimukset. Puutteet, poikkeamat ja riskit tulee osata tunnistaa sekä analysoida, miten nämä havainnot vaikuttavat sopimuksen jatkamiseen, uusimiseen tai päättämiseen. Sopimusjuristi tuo esiin opitut asiat ja tukee organisaatiota varmistamalla, että ne huomioidaan seuraavassa sopimuksessa tai sopimuksen päättämisen yhteydessä.

Ymmärtää tietojenhallinnan ja pääsyoikeuksien sopimukselliset velvoitteet

Sopimusjuristin tulee osata tulkita ja soveltaa sopimuksen ehtoja niin, että tietoturva säilyy myös sopimuksen päättyessä tai uusittaessa. On ymmärrettävä, miten sopimus ohjaa tietojen säilyttämistä, poistamista, palauttamista ja siirtoa sekä pääsyoikeuksien hallintaa. Lisäksi sopimusjuristin on osattava hyödyntää sopimusta välineenä riskien hallinnassa ja varmistaa, että velvoitteet tukevat tietosuojaa ja tietoturvaa myös sopimussuhteen jälkeen.

Osaa tunnistaa vastuut, riskit ja toimenpiteet sopimuksen päättyessä

Velvoitteet eivät välttämättä pääty sopimuksen päättyessä. Sopimusjuristin tulee osata tunnistaa sopimuksen päättymiseen liittyvät velvoitteet, kuten tietojen säilyttäminen ja raportointi. On tärkeää osata arvioida, miten vastuut ja riskit, esimerkiksi tietoturvaloukkauksien osalta, jakautuvat sopimuksen päättymisen jälkeen.

Osaa valmistella sopimuksen uusimisen ja hallita muutoksia

Sopimusjuristin on osattava valmistella sopimuksen uusiminen siten, että aiemmista riskeistä ja puutteista opitut asiat otetaan huomioon. On varmistettava, että tietoturvaehdot ovat ajan tasalla suhteessa lainsäädäntöön, hyviin käytäntöihin ja organisaation tarpeisiin. Sopimusjuristi huolehtii, että kaikki muutokset dokumentoidaan selkeästi. Hän tukee organisaatiota muutosten vaikutusten arvioinnissa ja varmistaa, että sopimuksen rakenteet mahdollistavat tietoturvan jatkuvan kehittämisen.

Keskeiset toimet:

- Arvioi, miten nykyinen sopimus on toteuttanut tietoturvavaatimukset ja tuo esiin opitut asiat jatkopäätösten tueksi.
- Varmista, että sopimus ohjaa turvalliseen tietojen säilyttämiseen, poistamiseen ja siirtämiseen.
- Tunnista sopimuksen päättymiseen liittyvät tietoturvavelvoitteet, vastuut ja riskit, erityisesti tietoturvaloukkausten osalta.
  - Valmistele sopimuksen uusiminen siten, että aiemmista kokemuksista opitut asiat korjataan ja tietoturvaehdot päivitetään vastaamaan lainsäädäntöä ja käytäntöjä.

Tietosuojavastaava

Tässä osiossa kuvataan, millaista ohjelmistoturvallisuuteen liittyvää tietosuojaosaamista tietosuojavastaavalla tulisi olla. Osio on suunnattu tietosuojavastaavan roolissa toimiville ja auttaa hahmottamaan, mitä osaamista tarvitaan ohjelmiston eri elinkaaren vaiheissa aina määrittelystä käytöstä poistoon.

Tietosuojavastaaja tekee tietosuojasta käytäntöä ja käytännöstä luottamusta.

MIKSI OHJELMISTOTURVALLISUUS KUULUU TIETOSUOJAVASTAAVALLE?

Tietosuojavastaaja varmistaa, että organisaation ohjelmistot ja niiden käsittelemät tiedot täyttävät tietosuojalainsäädännön, kuten GDPR:n, vaatimukset. Hän toimii linkkinä lainsäädännön ja organisaation käytännön toimintatapojen välillä, tulkiten sääntelyn vaatimukset selkeiksi ohjeiksi ja prosesseiksi.

Rooliin kuuluu riskien arviointi, vaikutustenarviointien ohjaaminen ja seuranta, jotta henkilötietojen käsittely pysyy lainmukaisena ja turvallisena. Tietosuojavastaava osallistuu ohjelmistohankintoihin ja -kehitykseen tuomalla esiin tietosuojavaatimukset ja arvioimalla niiden vaikutukset päätöksiin.

Hän valvoo, että tietosuoja sisältyy sopimuksiin ja että käytännöt tukevat tietoturvaa ja tietosuojaa koko ohjelmiston elinkaaren ajan. Tietosuojavastaava auttaa myös organisaatiota varautumaan mahdollisiin tietoturvaloukkauksiin ja hoitamaan niihin liittyvät raportointivelvoitteet.

Tietosuojavastaajan rooli on keskeinen organisaation luottamuksen rakentamisessa, lainsäädännön noudattamisessa ja henkilötietojen turvallisuuden varmistamisessa.

Tiivistelmä

TIETOSUOJAVASTAAVAN OSAAMISTARPEET

- Osaa tunnistaa ja arvioida henkilötietojen käsittelyn tarpeet, riskit ja vaikutukset rekisteröidyille.
- Osaa varmistaa tietosuojaperiaatteiden, kuten minimoinnin, läpinäkyvyyden ja käyttötarkoitussidonnaisuuden, toteutumisen ohjelmiston suunnittelussa, käytössä ja poistossa.
- Tuntee vaikutustenarvioinnin (DPIA) vaatimukset ja osaa arvioida, milloin se on tarpeen.
- Osaa arvioida palveluntarjoajien roolit, vastuut ja tietojen siirtoihin liittyvät velvoitteet.
- Osaa arvioida muutosten ja päivitysten vaikutukset tietosuojaan ja tunnistaa tilanteet, joissa tarvitaan uusia arviointeja.
- Ymmärtää sopimusehtojen, poikkeamien hallinnan ja rekisteröityjen oikeuksien käytännön toteutumisen merkityksen.
- Hallitsee käytöstä poiston tietosuojaosaamisen: tietojen poistamisen, anonymisoinnin, säilyttämisen ja dokumentoinnin.

Tietosuoja alkaa jo suunnittelupöydältä.

MÄÄRITTELY, SUUNNITTELU JA HANKINTA

Tietosuojavastaavan tehtävänä on varmistaa, että henkilötietojen käsittely on suunniteltu alusta alkaen lainmukaisesti, turvallisesti ja rekisteröityjen oikeuksia kunnioittaen. Tämä edellyttää aktiivista osallistumista ohjelmiston määrittelyyn ja hankintaan, riskien arviointiin, sopimusehtojen valmisteluun sekä yhteistyötä eri asiantuntijoiden kanssa.

Osaa tunnistaa henkilötietojen käsittelyn tarpeet ja vaikutukset

Tietosuojavastaavan tulee osata tunnistaa, mitä henkilötietoja ohjelmistossa käsitellään, mihin tarkoitukseen ja millä oikeusperusteella. On ymmärrettävä, miten käsittely vaikuttaa rekisteröityjen oikeuksiin ja miten GDPR sekä kansallinen lainsäädäntö ohjaavat ohjelmiston suunnittelua ja määrittelyä. Tietosuojavaatimusten arvioinnissa on huomioitava myös tekoälyn käyttö ohjelmistossa, erityisesti silloin kun se käsittelee henkilötietoja tai tekee automaattisia päätöksiä, joilla voi olla vaikutusta rekisteröityihin. Tietosuojavastaava varmistaa, että käsittelytoimet dokumentoidaan asianmukaisesti esimerkiksi rekisteriselosteiden ja käsittelytoimien kuvausten avulla. Tulee tehdä yhteistyötä juristien, tietoturva-asiantuntijoiden ja liiketoiminnan kanssa, jotta tietosuojavaatimukset huomioidaan kokonaisvaltaisesti jo ohjelmiston alkuvaiheessa.

Osaa ohjata tietosuojan sisällyttämistä suunnitteluun (privacy by design)

Tietosuojaperiaatteiden sisällyttäminen ohjelmiston arkkitehtuuriin ja toiminnallisuuksiin on välttämätöntä, jotta henkilötietojen käsittely on alusta asti lainmukaista ja turvallista. Tietosuojavastaavan tulee ymmärtää, miten periaatteet kuten minimointi, läpinäkyvyys, käyttötarkoitussidonnaisuus ja turvallisuus näkyvät käytännön ratkaisuissa. Tämä tarkoittaa esimerkiksi tietojen säilytysaikojen määrittelyä, poistamisen ja oikaisun mahdollistamista, anonymisointia sekä tietojen siirrettävyyden tukemista. Tietosuojavastaavan on osattava arvioida, miten ohjelmisto tukee rekisteröityjen oikeuksien toteutumista, ja varmistaa, että nämä vaatimukset kytkeytyvät osaksi ohjelmiston määrittelyä.

Osaa tunnistaa tietosuojariskit ja ohjata vaikutustenarviointia

Tietosuojavastaavan tulee osata arvioida henkilötietojen käsittelyyn liittyviä riskejä ja tunnistaa tilanteet, joissa ohjelmisto voi aiheuttaa korkean riskin rekisteröidyille. On tunnistettava, milloin vaikutustenarviointi (DPIA) on lain mukaan tarpeen, ja osattava ohjata sen käynnistämistä. Vaikka tietosuojavastaava ei vastaa arvioinnin teknisestä tai liiketoiminnallisesta sisällöstä, hänen tehtävänään on varmistaa, että arviointi toteutetaan asianmukaisesti ja että sen tulokset tukevat ohjelmiston suunnittelua ja riskienhallintaa tietosuojan näkökulmasta.

Osaa arvioida palvelutarjoajien roolit ja vastuut henkilötietojen käsittelyssä

Palveluntarjoajien roolien tunnistaminen on keskeinen osa henkilötietojen käsittelyn hallintaa. Tietosuojavastaavan on osattava arvioida, toimiiko palveluntarjoaja rekisterinpitäjänä, käsittelijänä vai yhteisrekisterinpitäjänä, ja ymmärrettävä, mitä velvoitteita ja vastuita kukin rooli tuo mukanaan. Tietosuojavastaavan tukea vastuiden ja roolien dokumentointia sopimuksiin ja hankintaprosessiin. Lisäksi tietosuojavastaavan on osattava tunnistaa henkilötietojen siirrot, esimerkiksi pilvipalveluihin tai EU/ETA-alueen ulkopuolelle, ja varmistaa, että siirtoihin liittyvät vaatimukset, kuten mallisopimuslausekkeet (SCC) ja siirtojen vaikutustenarvioinnit (TIA), tulevat huomioiduiksi.

Osaa ohjata sopimusehtojen valmistelua tietosuojan näkökulmasta

Sopimuksilla on olennainen merkitys tietosuojan varmistamisessa. Tietosuojavastaavan tulee osata varmistaa, että sopimuksiin sisällytetään henkilötietojen käsittelyä koskevat ehdot, kuten käsittelyohjeet, oikeus tarkastaa ja auditoida käsittelyä, alihankkijoiden käyttöön liittyvät rajaukset sekä tietoturvavelvoitteet. On varmistettava, että sopimuksissa määritellään velvollisuus ilmoittaa tietoturvaloukkauksista ja muut vähimmäisvaatimukset, joita hankintatiimin on käytettävä tarjouspyyntöjä ja sopimuksia valmisteltaessa. Näin sopimukset tukevat tietosuojaa koko yhteistyön ajan.

Keskeiset toimet:

- Tunnista, mitä henkilötietoja ohjelmistossa käsitellään ja arvioi käsittelyn vaikutukset rekisteröidyille.
- Varmista, että tietosuojaperiaatteet sisällytetään ohjelmiston suunnitteluun ja määrittelyyn alusta alkaen.
- Käynnistä ja ohjaa vaikutustenarviointia, jos henkilötietojen käsittely aiheuttaa korkean riskin.
- Arvioi palveluntarjoajien roolit ja vastuut henkilötietojen käsittelyssä ja dokumentoi ne hankintaprosessiin.
- Selvitä, minne henkilötietoja siirretään ja varmista, että siirrot tehdään lainmukaisesti ja dokumentoidusti.
- Varmista, että sopimuksiin sisällytetään tietosuojaa koskevat velvoitteet ja oikeudet, kuten auditointimahdollisuudet ja tietoturvaloukkausten ilmoittaminen.

KÄYTTÖÖNOTTO JA KÄYTTÖ

Tietosuojavastaavan rooli korostuu ohjelmiston käyttöönotossa ja käytössä, kun varmistetaan rekisteröityjen oikeuksien toteutuminen, tietosuojakäytäntöjen toimivuus ja sääntelyn noudattaminen. Työ painottuu seurantaan, ohjeistamiseen ja jatkuvaan yhteistyöhön eri sidosryhmien kanssa, jotta tietosuojavaatimukset pysyvät ajan tasalla ohjelmiston kehittyessä ja organisaation toiminnan muuttuessa.

Osaa varmistaa tietosuojakäytännöt ja rekisteröityjen oikeudet

Tietosuojavastaavan tulee osata varmistaa, että ohjelmisto tukee rekisteröityjen oikeuksien toteutumista käytön aikana. Tämä tarkoittaa esimerkiksi mahdollisuutta oikaista, poistaa ja siirtää tietoja sekä toteuttaa muita GDPR:n mukaisia oikeuksia. Tietosuojavastaavan on ymmärrettävä, miten henkilötietojen käsittely tapahtuu ohjelmistossa eri käyttäjäryhmien ja toimintojen kautta, ja miten nämä ratkaisut vaikuttavat rekisteröityjen asemaan. Lisäksi on huolehdittava, että pyyntöjen käsittely on dokumentoitua, auditoitavaa ja että prosessit ovat henkilöstölle selkeitä. Tietosuojavastaavan tulee osata tukea myös ohjeiden ja koulutusmateriaalien laatimista ja jalkauttamista, jotta käytännöt tulevat arjessa käyttöön.

Ymmärtää seurannan ja jatkuvuuden merkityksen

Tietosuojavastaavan on osattava valvoa, että tietosuojavaatimuksia noudatetaan ohjelmiston käytössä. Tietosuojavastaavan tulee osallistua seurantaan ja raportointiin, erityisesti rekisteröityjen oikeuksien toteutumisen osalta, ja tukea organisaatiota kyvyssä reagoida muuttuviin riskeihin ja sääntelyvaatimuksiin. Tietosuojavastaavan tulee tehdä tiivistä yhteistyötä tietoturva-asiantuntijoiden, IT:n ja liiketoiminnan kanssa varmistaakseen, että tietosuoja toteutuu käytännössä. Lisäksi on ylläpidettävä jatkuvaa vuoropuhelua toimittajan kanssa, jotta ohjelmiston ratkaisut ja päivitykset pysyvät ajantasaisina myös käytön aikana.

Osaa arvioida muutosten ja päivitysten vaikutukset

Ohjelmistot elävät ja kehittyvät, ja tietosuojavastaavan on ymmärrettävä muutosten ja päivitysten vaikutukset henkilötietojen käsittelyyn. On varmistettava, että merkittävien muutosten yhteydessä arvioidaan tietosuojavaikutukset ja että tarvittaessa käynnistetään vaikutustenarviointi (DPIA). Tietosuojavastaavan tehtävänä on tuoda esiin tietosuojavaatimukset muutosten suunnittelussa ja toteutuksessa, jotta ohjelmiston tietosuoja pysyy ajan tasalla koko sen käytön ajan.

Tietosuoja elää ohjelmiston mukana.

Ymmärtää poikkeamien ja loukkausten hallinnan
Tietosuojavastaavan on osattava ohjata organisaatiota tietosuojarikkomusten ja tietoturvaloukkausten hallinnassa. Tämä sisältää rikkomusten havaitsemisen periaatteiden tuntemisen, ilmoittamisen prosessien varmistamisen ja sääntelyn mukaisten menettelytapojen ylläpitämisen. Tietosuojavastaavan tulee osata tukea organisaatiota myös poikkeamien hallintaprosessien ja mittareiden kehittämisessä, jotta toiminta on järjestelmällistä ja läpinäkyvää. Lisäksi on huolehdittava, että kaikki poikkeamat dokumentoidaan asianmukaisesti ja että ilmoitusvelvollisuudet toteutuvat lain edellyttämällä tavalla.

Keskeiset toimet:

- Varmista säännöllisesti, että ohjelmisto tukee rekisteröityjen oikeuksia ja että prosessit ovat dokumentoituja ja selkeitä.
- Seuraa tietosuojavaatimusten toteutumista käytön aikana ja raportoi havaituista puutteista.
- Ylläpidä yhteistyötä IT:n, tietoturvan, liiketoiminnan ja toimittajan kanssa tietosuojan varmistamiseksi.
- Arvioi muutosten ja päivitysten vaikutukset tietosuojaan ja käynnistä tarvittaessa vaikutustenarviointi.
- Varmista, että poikkeamat ja loukkaukset käsitellään ja dokumentoidaan asianmukaisesti sekä että ilmoitusvelvollisuudet täyttyvät.

KÄYTÖSTÄ POISTO

Ohjelmiston käytöstä poisto edellyttää huolellista suunnittelua myös tietosuojan näkökulmasta. Tietosuojavastaavan tehtävänä on varmistaa, että henkilötietojen käsittely päättyy sääntelyn mukaisesti, riskit tunnistetaan ja dokumentointi tukee osoitusvelvollisuutta koko poistoprosessin ajan – myös toimittajien ja kolmansien osapuolten osalta.

Osaa tunnistaa ja arvioida poistamiseen liittyvät riskit
Tietosuojavastaavan tulee osata tunnistaa ohjelmiston käytöstä poistoon liittyvät keskeiset riskit, kuten varmuuskopioiden, lokitietojen ja pääsyoikeuksien hallinnan sekä tietojen siirtämisen ja säilyttämisen haasteet. On ymmärrettävä, miten nämä riskit vaikuttavat sääntelyn noudattamiseen ja rekisteröityjen oikeuksiin. Lisäksi tietosuojavastaavan on osattava arvioida, miten puutteet poistoprosessissa voivat johtaa poikkeamiin tai tietoturvaloukkauksiin, ja tukea organisaatiota varautumisessa ja reagointiprosessien suunnittelussa.

Osaa ohjata tietojen käsittelyä käytöstä poiston jälkeen
Tietosuojavastaavan on ymmärrettävä, milloin henkilötiedot on poistettava, anonymisoitava, siirrettävä tai arkistoitava sääntelyn mukaisesti. On osattava arvioida poistomenetelmien luotettavuutta ja auditoinnin merkitystä sekä kysyä, miten tiedot poistetaan tai suojataan myös käytöstä poiston jälkeen esimerkiksi varmuuskopioista. Tietosuojavastaavan tulee hallita periaatteet, joiden avulla voidaan arvioida, ovatko käytetyt menetelmät riittäviä tietosuojan ja tietoturvan näkökulmasta.

Ymmärtää toimittajan ja kolmansien osapuolten vastuut poistossa
Toimittajien ja alihankkijoiden vastuilla on suuri merkitys ohjelmiston käytön päättyessä. Tietosuojavastaavan tulee osata arvioida toimittajan ja sen alihankkijoiden vastuut henkilötietojen poistamisesta ohjelmiston käytön päättyessä. On varmistettava, että poistamista koskevat velvoitteet on kirjattu sopimuksiin ja että niiden toteutuminen voidaan myös osoittaa. Tietosuojavastaavan on tunnettava käytännöt, joilla dokumentoidaan todisteet tietojen poistosta myös toimittajan ja alihankkijoiden ympäristöissä, jotta osoitusvelvollisuus täyttyy.

Ohjelmisto poistuu, tietosuoja jää.

Osaa varmistaa dokumentoinnin ja jäljitettävyyden
Tietosuojavastaavan tulee hallita poistoprosessiin liittyvä dokumentointi ja sen merkitys osoitusvelvollisuuden ja auditoitavuuden kannalta. On ymmärrettävä, mitä poistamiseen liittyviä tietoja on säilytettävä, kuten poistotodistukset ja lokit, ja mitä tietoja ei saa jäädä talteen. Lisäksi tietosuojavastaavan on osattava varmistaa, että kaikki toimenpiteet ovat jälkikäteen todennettavia ja läpinäkyviä, jolloin organisaatio pystyy osoittamaan toimineensa sääntelyn mukaisesti.

Keskeiset toimet:

- Tunnista poistamiseen liittyvät riskit ja arvioi riskien vaikutukset sääntelyn noudattamiseen ja rekisteröityjen oikeuksiin.
- Varmista, että henkilötiedot poistetaan, anonymisoidaan, siirretään tai arkistoidaan sääntelyn mukaisesti.
- Tarkasta, että poistomenetelmät ja todentamismenetelmät ovat riittäviä tietosuojan ja tietoturvan näkökulmasta.
- Arvioi toimittajan ja alihankkijoiden vastuut poistossa ja varmista sopimukselliset velvoitteet.
- Varmista, että poistoprosessi on dokumentoitu ja että toimenpiteet ovat jälkikäteen todennettavissa ja läpinäkyviä.

Ohjelmistotuvallisuuden osaamistarpeet rooleittain

Osaamisalue	Johto	Ohjelmistohankinnoista vastaava	Ohjelmistokehityksen tilaaja	Projektipäällikkö	Tuoteomistaja / palvelupäällikkö	Sopimusjuristi	Tietosuojavastaava
Liiketoimintastrategia ja johtaminen	Osaa linjata ja johtaa turvallisuusasioita	Ymmärtää vaikutukset hankintaan	Ymmärtää liiketoimintayhteyden	Ymmärtää tavoitteiden vaikutukset	Osaa sovittaa tietoturvan liiketoimintaan	Ymmärtää sopimusten strategisen merkityksen	Tuntee tietosuojan strategisen merkityksen
Ohjelmiston elinkaari	Ymmärtää elinkaariajattelun	Ymmärtää vaikutukset hankintaan	Osaa suunnitella elinkaaren vaatimukset	Ymmärtää elinkaariajattelun	Osaa seurata tietoturvaa koko elinkaaren ajan	Tuntee sopimusten elinkaaren	Tuntee tietojen elinkaaren hallinnan
Turvallisen ohjelmistokehityksen periaatteet	Ymmärtää keskeiset periaatteet	Tuntee periaatteet ja osaa vaatia toimittajalta	Osaa vaatia ja arvioida toteutumista	Tuntee keskeiset periaatteet	Osaa soveltaa käytännössä	Tuntee sopimukselliset vaatimukset	Ymmärtää vaikutukset henkilötietojen käsittelyyn
Sääntely ja vaatimustenmukaisuus (NIS2, CRA, GDPR)	Tuntee ja varmistaa noudattamisen	Tunnistaa ja huomioi hankinnassa	Tunnistaa ja huomioi tilauksessa	Tuntee sovellettavat vaatimukset	Ymmärtää ja osaa soveltaa käytännössä	Osaa muotoilla sopimuksiin vaatimuksiksi	Vastaa tulkinnasta ja seurannasta
Tietoturvan viitekehykset ja standardit	Tuntee ja linjaa hyödyntämisen	Tunnistaa ja huomioi sovellettavat viitekehykset	Tunnistaa ja huomioi sovellettavat viitekehykset	Tuntee sovellettavat viitekehykset	Ymmärtää kehitystyön tukena	Osaa muotoilla sopimuksiin vaatimuksiksi	Tuntee tietosuojan viitekehykset
Riskien tunnistaminen ja arviointi	Osaa arvioida riskejä strategisesti	Osaa tunnistaa ja arvioida hankintariskit	Osaa tunnistaa ja arvioida riskit tilauksessa	Osaa tunnistaa ja arvioida projektiriskit	Osaa tunnistaa ja arvioida ohjelmiston riskit	Osaa arvioida sopimusriskit	Osaa arvioida henkilötietojen käsittelyyn liittyvät riskit
Riskienhallinta	Osaa hyödyntää päätöksenteossa	Osaa hyödyntää päätöksenteossa	Osaa hyödyntää päätöksenteossa	Osaa hallita projektin riskejä	Osaa hallita ohjelmiston riskejä	Osaa hallita riskejä sopimusehdoilla	Osaa ohjata tietosuojariskien hallintaa
Toimitusketjuturvallisuus	Ymmärtää riskit turvallisuudessa ja jatkuvuudessa	Ymmärtää ja osaa arvioida toimitusketjuriskejä	Ymmärtää ja osaa arvioida toimitusketjuriskejä	Ymmärtää toimitusketjuriskien vaikutukset	Osaa arvioida toimitusketjuriskejä ja tuntee vastuut	Tunnistaa sopimukselliset vastuut	Ymmärtää toimitusketjun tietosuojariskit

Osaamisalue	Johto	Ohjelmistohankinnoista vastaava	Ohjelmistokehityksen tilaaja	Projektipäällikkö	Tuoteomistaja / palvelupäällikkö	Sopimusjuristi	Tietosuojavastaava
Toimittajaturvallisuus	Ymmärtää toimittajavalinnan merkityksen	Osaa arvioida toimittajien turvallisuuskyvykkyyttä	Osaa arvioida toimittajien turvallisuuskyvykkyyttä	Ymmärtää toimittajien merkityksen turvallisuudelle	Osaa arvioida ja seurata toimittajien turvallisuutta	Ymmärtää toimittajaturvallisuuden sopimuksellisen merkityksen	Osaa tunnistaa roolit ja vastuut
Vaatimusten määrittely ja suunnittelu	Ymmärtää turvallisuusvaatimusten merkityksen	Osaa määritellä tietoturvavaatimukset	Osaa määritellä tietoturvavaatimukset	Osaa määritellä projektin tietoturvavaatimukset	Osaa muuntaa vaatimukset hyväksymiskriteereiksi	Osaa muuntaa turvallisuusvaatimukset sopimusehdoiksi	Osaa arvioida ja määritellä tietosuojavaatimukset
Sopimusten hallinta	Ymmärtää sopimuksen merkityksen turvallisuudessa	Osaa laatia tietoturvaehdot	Osaa laatia tietoturvaehdot	Osaa tuoda sopimusvelvoitteet käytäntöön	Ymmärtää sopimuksen merkityksen tietoturvaan	Osaa hallita muutoksia ja päivittää ehtoja	Tuntee tietosuojaa koskevat sopimusehdot ja valvontavelvoitteet
Haavoittuvuuksien hallinta	Ymmärtää merkityksen liiketoiminnan jatkuvuudelle	Osaa sisällyttää velvoitteet sopimuksiin	Osaa sisällyttää velvoitteet sopimuksiin	Ymmärtää projektitason toimet haavoittuvuuksien hallinnassa	Osaa priorisoida korjaukset ja seurata toteutumista	Ymmärtää sopimukselliset korjaus- ja ilmoitusvelvoitteet	Ymmärtää haavoittuvuuksien merkityksen tietosuojaan
Pääsynhallinta	Ymmärtää merkityksen turvallisuudelle	Ymmärtää merkityksen toimittajasuhteissa	Ymmärtää merkityksen toimittajasuhteissa	Osaa valvoa projektin käytäntöjä	Osaa hallita pääsyoikeuksia turvallisesti	Tuntee pääsyhallinnan juridiset vaatimukset ja vastuut	Tuntee pääsynhallinnan ja käyttöoikeuksien tietosuojavaatimukset
Tiedonhallinta ja tietojen luokittelu	Osaa ja hyväksyy tiedonhallinnan periaatteet	Ymmärtää ja huomioi hankinnoissa	Ymmärtää ja huomioi tilauksessa	Osaa ohjata ja valvoa projektin tietojenkäsittelyä	Ymmärtää vaatimukset ja osaa johtaa käytännössä	Tuntee tietojen käsittelyn juridiset vaatimukset	Ymmärtää tiedon elinkaaren ja säilytysvaatimukset
Testaus (tekninen)	Ymmärtää merkityksen turvallisuudelle	Osaa määrittää testausvaatimukset	Osaa määrittää testausvaatimukset	Osaa koordinoida ja hyödyntää tuloksia	Osaa koordinoida ja hyödyntää tuloksia	Ymmärtää sopimuksissa asetetut velvoitteet	Ymmärtää testausvaiheen tietosuojariskit

Osaamisalue	Johto	Ohjelmistohankinnoista vastaava	Ohjelmistokehityksen tilaaja	Projektipäällikkö	Tuoteomistaja / palvelupäällikkö	Sopimusjuristi	Tietosuojavastaava
Tarkastus ja auditointi (hallinnollinen ja tekninen)	Ymmärtää merkityksen turvallisuudelle	Osaa määrittää tarkastus tai auditointioikeudet	Osaa määrittää tarkastus tai auditointioikeudet	Osaa koordinoida ja hyödyntää tuloksia	Osaa koordinoida ja hyödyntää tuloksia	Ymmärtää sopimuksissa asetetut velvoitteet	Osaa hyödyntää tuloksia tietosuojan kehittämisessä
Tietosuoja	Tuntee strategisen merkityksen	Ymmärtää sovellettavat vaatimukset	Ymmärtää sovellettavat vaatimukset	Tuntee periaatteet ja osaa huomioida projektissa	Tuntee periaatteet ja osaa toteuttaa käytännössä	Hallitsee tietosuojaa koskevat sopimusvelvoitteet	Hallitsee GDPR:n ja kansallisen lainsäädännön soveltamisen käytäntöön
Turvallinen käyttöönotto	Ymmärtää merkityksen turvallisuudelle	Osaa määritellä käyttöönoton tietoturvavaatimukset	Osaa määritellä käyttöönoton tietoturvavaatimukset	Osaa varmistaa turvallisen siirtymän tuotantoon	Osaa varmistaa turvallisen käyttöönoton	Osaa huomioida sopimusta laadittaessa	Osaa arvioida käyttöönoton vaikutukset tietosuojaan
Turvallinen käytöstä poisto	Ymmärtää merkityksen turvallisuudelle	Osaa huomioida jo hankintavaiheessa	Osaa huomioida jo tilausvaiheessa	Osaa huomioida tietoturvan projektin lopetuksessa	Osaa varmistaa turvallisen käytöstäpoiston	Osaa huomioida sopimusta laadittaessa	Osaa varmistaa henkilötietojen poistamisen vaatimukset
Tietoturvapoikkeamien käsittely	Tuntee poikkeamienhallinnan prosessin	Ymmärtää toimittajavelvoitteet	Ymmärtää toimittajavelvoitteet	Osaa johtaa projektipoikkeamien hallintaa	Osaa johtaa operatiivista reagointia	Osaa määritellä raportointi- ja vastuuvaatimukset	Osaa hallita ja raportoida tietoturvaloukkaukset
Monitorointi ja jatkuva seuranta	Ymmärtää monitoroinnin merkityksen turvallisuudelle	Osaa huomioida monitoroinnin vaatimukset hankinnassa	Osaa huomioida monitoroinnin vaatimukset tilauksessa	Osaa seurata projektin tietoturvan tilaa	Ymmärtää monitoroinnin merkityksen turvallisuudelle	Osaa huomioida monitoroinnin vaatimukset sopimuksissa	Ymmärtää tietosuojan seurannan ja osoitusvelvollisuuden merkityksen

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus
Puhelin: 029 534 5000 (vaihde)
PL 313 (Erik Palménin aukio 1)
00561 Helsinki

Finnish Transport and Communications Agency
National Cyber Security Centre Finland (NCSC-FI)
Phone: +358 29 534 5000 (switchboard)
P.O. Box 313 (Erik Palménin aukio 1)
FI-00561 Helsinki

Huoltovarmuuskeskus

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus