AUDITOINTI JA ARVIOINTI

Tiedätkö, onko organisaationne tietoturvan hallinta alan tietoturvavaatimusten tasolla? Tiedätkö, miten voitte ottaa käyttöönne parhaat ja teille sopivimmat tietoturvakäytännöt? Entä oletko ajatellut, milloin viimeksi teille uudet silmäparit ovat antaneet näkökulmia asioihin, joihin tulisi kiinnittää huomiota tietoturvan kehittämiseksi?

Kokeneen ja riippumattoman tietoturvallisuusasiantuntijan suorittama tietoturvatarkastus, useimmiten nimellä auditointi, antaa päivitetyn tilannekatsauksen tarkastelun kohteena olevan ympäristön nykyisestä tietoturvan tasosta. Auditoinnin tarkoituksena on varmistaa tarkasteltavan IT-ympäristön turvallisuuden ajantasaisuus sekä se, että turvallisuutta myös kehitetään ajan vaatimuksia vastaavasti. Auditointi esimerkiksi varmistaa, että tietojärjestelmien ja organisaatioiden tietoturva toimii vaatimusten mukaisella tasolla ja että organisaatio ymmärtää, mitä sen täytyy tehdä saavuttaakseen liiketoiminnan tietoturvavaatimukset.

LOIHDE TRUST

LOIHDE TRUST

AUDITOINNIN 4K – KOHDE, KRITEERIT, KUKA, KOSKA?

Auditoinnin kohteena voi olla koko organisaatio, vain osa organisaatiosta, tietyt osastot tai jotkin projektit ja järjestelmät.

Auditoinnin alussa selvitetään yhdessä asiakkaan kanssa tavoiteltu tietoturvallisuuden taso, jonka mukaan valitaan auditoinnissa käytettävät tarkastuskohteet ja -menetelmät. Auditoinnissa on hyvä valita jokin kriteeristö, jonka mukaan auditointi suoritetaan. Yleisimpiä käytettäviä kriteeristöjä ovat VAHTI-ohjeisto, KATAKRI, ISO 27001/27002 sekä PCI-DSS. Hyvä auditointi ja auditoija sovittaa näistä valitut kriteeristöt todellista kohdeympäristöä ja toimintaa vastaavaksi.

Edellä mainittuun pohjautuen tarkastuksen suorittajalla on merkitystä. Kokenut ja esimerkiksi CISA- tai CISSP-sertifioitu asiantuntija on hyvä olla pääauditoijana aina, kun on kyseessä mikä tahansa merkittävä tai kriittinen tarkastelun kohde.

Aika ajoin on myös hyvä kysyä itseltään sellaisia kysymyksiä, kuten: Onko meillä järjestelmällinen ja säännöllinen prosessi tieto-turvallisuuden tason tarkastamiseksi? Tiedämmekö milloin ja miksi tieto-turvan taso on viimeksi tarkastettu sekä milloin ja miksi tämä olisi jälleen ajankohtaista seuraavan kerran?
Onko meillä siis vuosikello, jonka mukaan toimimme?

A NIIN KUIN AUDITOINTI, A NIIN KUIN ARVIOINTI – KUITENKIN KAKSI ERI ASIAA

Tietoturvallisuuden auditoinnista saa vielä enemmän irti, jos siihen yhdistää perinteisen auditoinnin lisäksi kokemusperäisen, riskianalyysiin ja toimintaympäristön erityispiirteisiin perustuvan arvioinnin.

Arviointi on vapaamuotoisempi organisaation turvallisuuden tasoa selvittävä kokonaisuus, joka selvittää organisaation kypsyystason suhteessa muihin vastaaviin toimijoihin. Auditoinnista poiketen arviointi ottaa kantaa myös muihin kuin kriteeristössä määriteltyihin ja havaittuihin asioihin. Arvioinnilla mitataan kohteen yleisempää turvallisuuden tasoa ja etsitään mahdollisia parannuskohteita.

Lopputuloksena on kuvaus tietoturvallisuuden nykytilasta sekä kehitysehdotukset käytännön toteutusmalleineen ja perustelut niille.

TURVAA KOKO TOIMINNALLE

On myös hyvä huomioida, että tietoturvallisuuden auditointi kattaa usein vain pienen osan organisaation turvallisuudesta sekä siitä turvallisuudesta, joka suojaa yritykselle tärkeitä tietoja. Osaava auditoinnin asiantuntijataho on kykenevä laajentamaan auditoinnin myös muille yritysturvallisuuden alueille, jolloin tarkastellaan lisäksi esimerkiksi hallinnollista turvallisuutta, henkilöstöturvallisuutta ja toimitilojen turvallisuuden tasoa. Tärkeää on, että auditoija osaa kiinnittää turvallisuusauditoinneissa ja -arvioinneissa huomiota eri osa-alueiden riippuvuuksiin ja tuomaan organisaatiolle selkeästi ilmi, miten eri osa-alueiden löydökset vaikuttavat toisiinsa.

AUDITOINTI

- Tutkii tietoturvan ajantasaisuutta ja vaatimustenmukaisuutta
- Kriteeristö määrittää tarkasteltavat kohteet
- Auditoijan pätevyys todennettavissa mm. sertifikaatein
- Säännöllisyys ja määräajat vuosikellon avulla

ARVIOINTI

- Vapaamuotoisempi nykytilanteen tason selvitys
- Laajempi katsantokanta - myös kriteeristön ulkopuoliset kohteet
- Vertailu muihin toimijoihin
- Kehityskohteet perusteluineen ja toteutusmalleineen

YHTEENVETO

Seuraavan kerran kun auditointi on teillä ajankohtaista, mieti siis seuraavia asioita:

1. Onko auditoija jo auditoinut ympäristömme useampana vuotena putkeen? Meneekö auditointi rutiinilla? Olisiko tuoreiden katsantokantojen aika?

2. Tarkistammeko tietoturvallisuuden tason riittävän usein ja säännöllisesti? Onko meillä vuosikello tätä varten?

3. Pohjautuvatko auditoinnin tarkastuskohteet ja -menetelmät aidosti toimintamme tarpeisiin ja sopivatko ne ympäristöömme?

4. Tiedämmekö, miten jokin puute esimerkiksi toimitilaturvallisuudessa saattaa vaikuttaa tietoturvallisuuteen? Tiedämmekö ylipäätään puutteitamme toimitilaturvallisuudessa?

5. Auditointi on vain osa kokonaisuutta. Ottamalla mukaan vapaamuotoisen arvion, saat paremmin selville myös muut kehityskohteet kuin mitä kriteeristö sanelee.

YHTEYSTIEDOT:

LOIHDE TRUST

myynti.trust@loihde.com

029 001 3000

www.loihdetrust.com


LOIHDE
TRUST