

KYBERTURVALLISUUDEN PERUSTEET – tunnista uhat ja suojaa organisaatiosi

Kyberuhat eivät kosketa vain suuria yrityksiä tai IT-asiantuntijoita. Jokainen organisaatio, joka käyttää tietojärjestelmiä, sähköpostia, verkkopalveluita tai digitaalisia työvälineitä, voi joutua kyberhyökkäyksen kohteeksi. Yksittäinen huijausviesti, vaarantunut käyttäjätunnus tai haavoittunut tietojärjestelmä voi aiheuttaa merkittäviä häiriöitä organisaation toiminnalle.

Kyberturvallisuuden perusteet on kolmen tunnin käytännönläheinen koulutus, joka auttaa ymmärtämään, mitä kyberturvallisuus tarkoittaa ja miksi se on tärkeää kaikille toimialoille. Koulutuksessa perehdytään yleisimpiin kyberuhkiin, hyökkäystapoihin ja haavoittuvuuksiin sekä siihen, miten kyberriskejä voidaan tunnistaa ja pienentää osana jokapäiväistä toimintaa.

Koulutuksessa käsitellään muun muassa tietojenkalastelua, haittaohjelmia, kiristyshaittaohjelmia, käyttäjätunnusten vaarantumista, sosiaalista manipulointia ja tekoälyn hyödyntämistä huijauksissa. Lisäksi tutustutaan organisaation kyberturvallisuuden keskeisiin osa-alueisiin, varautumiseen, poikkeamatilanteissa toimimiseen ja toiminnan jatkuvuuden turvaamiseen.

Koulutus ei edellytä teknistä erityisosaamista. asiat käydään läpi selkeästi ja käytännön esimerkkien avulla, jotta jokainen osallistuja voi soveltaa oppimaansa omassa työssään ja organisaatiossaan.

Tavoitteena on, että koulutuksen jälkeen ymmärrät kyberturvallisuuden keskeiset periaatteet, tunnistat tavallisimmat kyberuhat ja tiedät, millä käytännön toimilla voit vaikuttaa oman organisaatiosi kyberturvallisuuteen.

Koulutuksen jälkeen osallistuja:

- ymmärtää kyberturvallisuuden merkityksen ja keskeiset käsitteet
- tunnistaa yleisimpiä kyberuhkia ja ymmärtää niiden mahdollisia vaikutuksia
- tuntee keskeiset tekniset ja organisatoriset suojautumiskeinot yleisellä tasolla
- ymmärtää kyberriskien hallinnan, varautumisen ja toiminnan jatkuvuuden merkityksen
- tietää, miten toimia kyberpoikkeaman epäilyssä ja kenelle siitä ilmoitetaan
- osaa tunnistaa oman roolinsa organisaation kyberturvallisuuden edistämisessä

Kouluttaja:

Yritysneuvoja ja kouluttaja, Heidi Ilmonen, Sotetraining

Päivämäärä ja aika:

22.01.2027, klo 09:00-12:00

19.03.2027, klo 09:00-12:00

Ohjelma klo 09:00-12:00 +/-15 min.

Mitä kyberturvallisuus tarkoittaa?

- Kyberturvallisuuden keskeiset käsitteet ja tavoitteet.

- Miten kyberturvallisuus liittyy tietosuojaan ja tietoturvaan?
- Miksi kyberturvallisuus koskettaa kaikkia organisaatioita?
- Kyberuhkien vaikutukset ihmisiin, palveluihin ja liiketoimintaan.
- Vastuut: johto, henkilöstö, IT ja yhteistyökumppanit.

Yleisimmät kyberuhat ja hyökkäystavat

- Tietojenkalastelu ja muut huijausviestit.
- Identiteetin väärentäminen.
- Haittaohjelmat ja kiristyshaittaohjelmat.
- Käyttäjätunnusten ja salasanojen varastaminen.
- Haavoittuvuuksien hyväksikäyttö ja päivittämättömät järjestelmät.
- Hyökkäykset toimitusketjun kautta.
- Tekoälyn mahdollistamat entistä uskottavimmat huijaukset.

Miten kyberhyökkäys etenee ja mihin se voi johtaa?

- Esimerkki kyberhyökkäyksen etenemisestä.
- Miten yksittäisestä virheestä voi syntyä laajempi häiriö?
- Tietojen vuotaminen, järjestelmien lukkiutuminen ja palvelukatkot.
- Taloudelliset, toiminnalliset ja maineeseen liittyvät vaikutukset.
- Miksi ennaltaehkäisy on usein helpompaa kuin vahinkojen korjaaminen?

Kyberturvallisuuden tärkeimmät suojautumiskeinot

- Monivaiheinen tunnistautuminen ja käyttöoikeuksien hallinta.
- Ohjelmistojen päivittäminen ja päätelaitteiden suojaaminen.
- Varmuuskopiot ja tietojen palauttamisen varmistaminen.
- Sähköpostin, verkkopalveluiden ja etätönn turvallinen käyttö.
- Tietojen turvallinen jakaminen ja hyväksytyjen työvälineiden käyttö.
- Henkilöstön osaaminen ja turvallisuuskulttuurin rakentaminen.

Kyberriskien hallinta ja toiminnan jatkuvuus

- Miten organisaatio tunnistaa tärkeimmät kyberriskinsä?
- Kriittiset järjestelmät, tiedot ja riippuvuudet.
- Palveluntarjoajat ja toimitusketjujen kyberturvallisuus.
- Varautuminen järjestelmähäiriöihin ja kyberhyökkäyksiin.
- Toiminta vaihtoehtoisilla menettelyillä häiriötilanteessa.
- Johdon rooli, ohjeet ja vastuut.

Kyberpoikkeamat ja niihin reagointi

- Mistä tunnistaa mahdollisen kyberhyökkäyksen?
- Miten toimia epäilyttävän viestin, haittaohjelman tai vaarantuneen tunnuksen yhteydessä?
- Kenelle poikkeamasta ilmoitetaan ja miksi nopeasti?
- Miksi epäiltyä haittaa ei pidä yrittää selvittää omin päin riskialttiilla toimilla?
- Poikkeaman rajaaminen, palautuminen ja opit tulevaa varten.

Yhteenveto ja seuraavat askeleet

- Kyberturvallisuuden tärkeimmät muistettavat asiat.
- Mitä jokainen voi tehdä?
- Kysymykset ja vastaukset.

ILMOITTAUTUMINEN

P. 09 696 2950, www.yritysakatemia.fi, ilmoittautuminen@yritysakatemia.fi

OSALLISTUMISMAKSU

450 euroa + alv laskutetaan koulutuspäivänä. Koulutus ja materiaalit sisältyvät hintaan.

Lisäosallistujat -50 %

PERUUTUSEHDOT, LIPPUTYYPIT JA HINNOITTELU:

Yli 60 päivää koulutukseen: Super Early Bird, -25%

Alle 60 päivää koulutukseen: normaalihinta

Estyneen tilalle voidaan vaihtaa toinen osallistuja kuluitta.

Peruutuksesta ja 14 päivää ennen koulutusta tehdyistä muutoksista veloitetaan toimistokuluina 15 % koulutuksen hinnasta. Myöhemmin kuin 14 päivää ennen koulutusta tehdyistä peruutuksista tai peruuttamatta jätetystä ja käyttämättömästä koulutuspaikasta veloitetaan osallistumismaksu kokonaisuudessaan. Peruutus on tehtävä kirjallisesti.

Alennushintaisilla lipuilla ei ole peruutus mahdollisuutta.

Varaamme oikeuden muutoksiin, ja siirtää jo sovittuja koulutuksia myöhempään ajankohtaan, tai muuttaa etäkoulutuksiksi. Koulutus saattaa siirtyä tai peruuntua mm. vähäisen osallistujamäärän vuoksi. Muutosten osalta tiedotamme osallistujia erikseen, YritysAkatemialla on oikeus peruuttaa koulutustilaisuus ilman korvausvelvollisuutta ilmoittamalla asiakkaalle siitä sähköpostilla viimeistään 4 arkipäivää ennen tilaisuuden ajankohtaa.