TIETOTURVAN ERIKOISLEHTI 2024

KYBER sanomat

Ole valmis!

Vinkkejä tietoturvallisempaan työ- ja vapaa-aikaan

Selätä kyber-hyökkäys

Digihuijarin 7 Suostuttelun periaatetta

5 viikossa digihuijariksi

Mikä ihme on CaaS

ja mitä se tarkoittaa yrityksille?

Esittelyssä

Social engineering

Kyberkriisiin varautuminen: miksi ja miten

Kyber- ja tietoturvan ajankohtaiset uhat

XAMK Kaakkois-Suomen ammattikorkeakoulu

30 vuotta KYMEN LAAKSON LIITTO

Euroopan unionin osarahoittama

Sisällysluettelo

Anna palautetta tai ota yhteyttä:
kyberkymi@xamk.fi

Lisää kyber- ja tietoturvasisältöjä, maksuttomia koulutuksia ja palveluja Kymenlaaksossa toimiville yrityksille:
www.kyberasema.fi

Tekijät: Markus Hölsä, Anni Lippo, Jouni Mäkelä, Hanna Nieminen, Janne Niinisaari ja Piia Selinkoski, Xamk.

Kuvat: Getty Images ja 123RF **Julkaistu:** Helmikuu 2024

Julkaisun ovat tuottaneet Kaakkois-Suomen ammattikorkeakoulun toteuttamat kehittämishankkeet Kyberturvan tulevaisuus Kymenlaaksossa, jota rahoittaa Kymenlaakson liitto oikeudenmukaisen siirtymän rahastosta (JTF) ja Kymvake – Kymenlaakson alueellisen varautumisyhteistyön kehittäminen, jota rahoittaa Kymenlaakson liitto Euroopan aluekehitysrahastosta (EAKR).

XAMK Kaakkois-Suomen ammattikorkeakoulu

30 vuotta KYMEN LAAKSON LIITTO

Euroopan unionin osarahoittama

Vahvista tietoturvaa ja lievitä kybertuskaa

Suomalaisia yrityksiä riivaavat useat eri kyberuhat ja -hyökkäykset, jotka koostuvat pääsääntöisesti haittaohjelmista yritysverkoissa ja laitteissa, sekä huijauksista kuten kalasteluviesteistä. Huijaukset ovat yhä kohdennetumpia ja taitavampia. Digihuijarit ja verkkorikolliset käyttävät vaikeaa maailmantilannetta luodakseen itselleen yhä uskottavampia tarinoita.

Kybertuskan hoito-opas: Tutki, Suojaa, Paranna

Tieto lisää tuskaa on vanha kansanviisaus, mutta kyberturvallisuudessa tietäminen on yksi parhaita keinoja parantaa omaa ja yrityksen tukalaa oloa. Kun tunnemme tekijät, jotka voivat altistaa meidät kyberhyökkäyksille niin voimme suojautua ja samalla parantaa digitaalista hyvinvointiamme.

Lue eteenpäin - luvassa hyödyllistä tietoa oman ja yrityksesi tietoturvan vahvistamiseen!

Lisää maksuttomia kyber- ja tietoturvasisältöjä, verkkokoulutuksia, podcasteja, videoita ja tapahtumia löydät sivustoltamme www.kyberasema.fi

Vinkkejä tietoturvallisempaan työ- ja vapaa-aikaan

- Käytä suojattuja verkkoja: Vältä julkisia verkkoja ja suosi mobiilitukiasemaa. Ota käyttöön VPN (Virtual Private Network).
- Rajoita ja hallitse jaettuja tietoja sosiaalisessa mediassa, jotta henkilökohtaiset tietosi pysyvät suojassa.
- Käytä pitkiä, monimutkaisia salasanoja tai vielä parempaa, salalauseita eri tileille. Hyödynnä salasanojen hallintaohjelmaa. Hyvä salasana on minimissään 15 merkkiä pitkä ja sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.
- Ota kaksivaiheinen tunnistautuminen käyttöön. Se on ainoa asia, joka pitää tilisi suojassa, jos salasanasi vuotaa.
- Tarkista puhelimesi sovellusten käyttöoikeudet ja anna niille vain tarvittavat oikeudet.
- Epäile kaikkea: Lähes 95 % kaikista haittaohjelmista leviää sähköpostin linkkien ja liitetiedostojen kautta, epäile siis etenkin näitä kahta, jos niitä tulee vastaan.
- Tarkista tilisi säännöllisesti: Seuraa pankkitiliäsi, luottokorttiasi ja muita tilejäsi säännöllisesti epäilyttävien toimien varalta.

5 viikossa digihuijariksi

Eli näin suojaudut manipuloinnilta

Ota haltuun suostuttelun 7 periaatetta – ja väistä ne

1. **Vastavuoroisuus:** Houkuttele kohteesi paljastamaan informaatiota tarjoamalla ensin itse vastaavaa tietoa itsestäsi.
2. **Johdonmukaisuus:** Uskottele kohteesi sitoutumaan pieniin toimiin, jotka sopivat hänen omiin tavoitteisiinsa.
3. **Sosiaalinen hyväksyntä:** Pyri saamaan kohde uskomaan, että ”kaikkihan näin tekevät”.
4. **Miellyttäminen:** Ihmiset ovat taipuvaisia sanomaan ”kyllä” ihmisille, joista he pitävät tai jotka he kokevat samanlaisiksi.
5. **Auktoriteetti:** Esiintyminen kohteen esihenkilönä tai kyseisen aiheen asiantuntijana on usein tehokas manipulaatiokeino.
6. **Niukkuus:** Esitä asiasi harvinaisena, haluttuna tai kiireellisenä.
7. **Yhtenäisyys:** Esiinny kuuluvasi johonkin samaan ryhmään tai jakavasi saman aatteen kohteen kanssa.

Tunnista riskisi joutua manipuloinnin kohteeksi

Välillä on tärkeää pysähtyä miettimään omaa ja yritykseen kohdistuvaa riskiä joutua hyökkäyksen kohteeksi. Riskin suuruutta voit arvioida pohtimalla omaa houkuttelevuuttasi hyökkääjän näkökulmasta. Tunnistamiseen auttaa kysymykset, kuten:

- **Kuinka esillä sinä tai yrityksesi on julkisuudessa?**
- **Onko sinulla tai yrityksellläsi paljon seuraajia tai aktiivisuutta sosiaalisessa mediassa?**
- **Täytyykö sinun luottaa monenlaisiin ihmisiin ja rooleihin työsi takia?**

Riskin kasvaessa kasvaa myös todennäköisyys joutua kohdennetumpien ja yksityiskohtaisempien hyökkäysten kohteeksi.

Avoimista lähteistä löytyy paljon tietoa

Jokainen kohdistettu kyberhyökkäys alkaa tiedon etsimisestä avoimista lähteistä (open source intelligence, OSINT) kuten hakukoneista, sosiaalisesta mediasta, julkisista foorumeista ja karttapalveluista. Kohteesta pyritään löytämään hyökkäystä edistäviä tietoja, kuten kontaktitietoja, käytössä olevia teknisiä työkaluja tai ohjelmia ja mieltymyksen kohteita.

”Social engineering eli käyttäjän manipulointi tarkoittaa ihmisluonteen hyväksikäyttöä, jolla saadaan kohde toimimaan vastoin hänen omia etujaan.

Ole ”kohteliaasti vainoharhainen”

Päivittäisten kiireiden keskellä voi olla vaikea havaita pahanaikeisia yhteydenottoja tai kanssakäymisiä, etenkin jos ne vaikuttavat oikeilta ja tulevat tutusta lähteestä. Alan asiantuntija Rachel Tobac käyttää tästä termiä ”ole kohteliaasti vainoharhainen”, eli käytä kahta kommunikointiväylää varmistaaksesi yhteydenottajan todenmukaisuus. Jos joku esimerkiksi pyytää arkaluontoista tietoa uudesta sähköpostiosoitteesta, varmista lähettäjä soittamalla hänen puhelinnumeroonsa, jonka ennalta tiedät.

Spoofing ja tekoälyn tuomat haasteet

Sähköposti, tekstiviesti tai jopa puhelu on yllättävän vaivatonta muokata näyttämään sen tulevan tutusta ja turvallisesta lähteestä. Tätä kutsutaan spoofingiksi eli lähettäjän tietojen muuttamista teknisesti näyttämään joltain muulta. Tähän kun lisätään tekoälyn avulla räätälöity viestin sisältö täydellisellä kohteen äidinkielellä ja ilman kirjoitusvirheitä, jolloin tietojen kalastelua on todella vaikea havaita. Tekoäly mahdollistaa myös soittajan äänen muuntamisen erittäin uskottavasti, joten hyökkääjä voi esiintyä jonain korkea-arvoisena henkilönä lisätäkseen auktoriteettiaan.

Lähde: Rachel Tobac - The hacker's guide to securing your organization. Bitwarden, julkaistu 2023.

Vinkkejä informaatiovaikuttamisen torjuntaan somessa ja verkossa

(lähde: Traficom)

- **Mieti miksi kyseinen viesti tai palvelun sisältö kiinnitti huomiosi.**
- **Varmista väitteet useammasta lähteestä.**
- **Lukuisat tykkäykset ja jaot eivät kerro postauksen sisällön todenmukaisuudesta.**
- **Luo koko teksti ennen kuin levität tai jaat sitä.**
- **Katso tarkkaan nettisivun verkko-osoite.**
- **Tarkista julkaisijan profiilin tuoreus, aktiivisuus, nimi ja kuva.**
- **Kiinnitä huomiota kielen johdonmukaisuuteen ja kielioppiin.**

Yrityksen kyber- ja tietoturvan ajankohtaiset uhat

Vanhat klassikot

1. Puhelinhuijaukset

Tämä tarkoittaa tilannetta, jossa joku soittaa sinulle ja yrittää huijata sinua antamaan heille arkaluontoisia tietoja, kuten henkilökohtaisia tietoja, salasanoja tai pankkitietoja. He voivat esimerkiksi esittää olevansa pankin työntekijä tai viranomainen ja pyytää tietoja, joita ei tulisi jakaa tuntemattomille.

2. Tekstiviesti-/sähköposti-huijaukset

Tämä tapahtuu, kun saat viestin puhelimeesi tai sähköpostiisi, joka näyttää tulevan luotettavalta taholta, mutta todellisuudessa se on huijaus. Näissä viesteissä pyritään usein saamaan sinut klikkaamaan linkkiä tai jakamaan henkilökohtaisia tietoja.

3. Päivittämättömät laitteet ja ohjelmistot

Kun laitteesi tai tietokoneesi ohjelmistoja ei ole päivitetty, ne voivat olla haavoittuvaisia hakkereiden hyökkäyksille. Päivitykset ovat kuin korjauksia, jotka auttavat pitämään laitteesi turvallisena.

4. Haittaohjelmat

Nämä ovat haittallisia ohjelmia, kuten viruksia tai haittaohjelmia, jotka voivat vahingoittaa tietokonettasi tai varastaa tietojasi ilman lupaa. Ne voivat aiheuttaa vahinkoa tai varastaa henkilökohtaisia tietoja.

5. Palvelunestohyökkäykset

Tämä on tilanne, jossa joku yrittää estää pääsyn tiettyyn verkkosivustoon tai palveluun kaatamalla sen valtavalla määrällä verkkoliikennettä.

Uudet haastajat

6. CaaS (Rikos palveluna)

Tämä tarkoittaa tilannetta, jossa rikolliset tarjoavat palvelujaan muille rikollisille, kuten haittaohjelmien luomista tai hyökkäysten toteuttamista maksua vastaan.

7. Toimitusketjuhyökkäykset

Kun hyökkääjät pyrkivät hakkeroimaan isomman yrityksen alihankkijan siinä toivossa, että pääsisivät sitä kautta käsiksi isomman yrityksen tietoverkkoon.

8. Hybridi- ja valtiollinen vaikuttaminen

Tämä viittaa tilanteisiin, joissa valtiot tai niiden toimijat käyttävät erilaisia keinoja, kuten disinformaatiota tai kyberhyökkäyksiä, vaikuttaakseen toisiin valtioihin tai organisaatioihin.

9. Identiteettivarkaus

Kun joku varastaa henkilökohtaisia tietojasi, kuten nimesi, osoitteesi tai sosiaaliturvatunnuksesi, voidakseen esiintyä sinuna tai tehdä rikoksia käyttämällä nimeäsi.

10. Opportunistiset huijausyritykset

Tämä tarkoittaa tilannetta, jossa huijarit hyödyntävät odottamattomia tai kaoottisia tilanteita, kuten luonnonkatastrofeja tai terveyskriisejä, huijatakseen ihmisiä hyödyntämään heidän epävarmuuttaan.

Mitä horisontissa

11. Tekoälyn hyödyntäminen rikollisuudessa

Kun rikolliset käyttävät tekoälyä esimerkiksi haitallisten ohjelmien kehittämisessä tai tiedonkalastelussa automatisoidakseen hyökkäyksiä ja petoksia.

12. Älylaitteiden elinkaari ja kierrätys

Koskee älylaitteiden, kuten älypuhelimien tai älykellojen, käyttöikää, kierrätystä ja turvallista hävittämistä niin, ettei henkilökohtaisia tietoja jää laitteisiin.

13. IoT kotona ja työpaikalla

IoT (Internet of Things) tarkoittaa älylaitteita, kuten älyvaloja tai älykkäitä termostaatteja, jotka ovat yhteydessä internetiin. Kotona ja työpaikoilla ne voivat tarjota kätevyyttä, mutta niiden turvallisuuteen on kiinnitettävä erityistä huomiota, jotta ne eivät altista verkkoa haavoittuvuuksille.

14. Rikollisten kybertoimien kaupallistaminen valtioille

Tämä viittaa tilanteeseen, jossa valtiot tai niiden toimijat ostavat rikollisilta ohjelmia ja palveluja käyttääkseen niitä omiin tarkoituksiin.

Selätä kyber-hyökkäys

kyberkriisin muistilista

1. Ennen

Minimoi riskit ja maksimoi kriisinkestävyys

- Tietoturva-, kriisiviestintä- ja jatkuvuussuunnitelma ovat ajan tasalla, ei pöytälaatikossa pölyttymässä.
- Yrityksen tietoturvariskit on tunnistettu ja niiden pohjalta on tehty riskienhallintasuunnitelma.
- Henkilöstön tietoturvavalmiuksia tuetaan säännöllisellä koulutuksella, ja tietoturva on yrityksessä yhteinen arvo.
- Tärkeät asiakirjat ja toiminnot varmuuskopioidaan säännöllisesti.
- Kyber- ja tietoturvaan kohdistuvia uhkia varten on harjoiteltu omin voimin, kyberharjoittelun ammattilaisten johdolla tai vaikka osallistumalla valtakunnalliseen Taisto-harjoitukseen.

2. Aikana

Johda, viesti ja huolehdi toimintakyvystä

- Selvitä tilannekuva ja päivitä sitä jatkuvasti. Kerää ylös mahdollisimman paljon tietoja hyökkäyksestä.
- Tunnista sisäiset ja ulkoiset tietotarpeet – hyödynnä riskienhallinnan ja kriisiviestinnän suunnitelmaa. Muista: älä valehtele!
- Ilmoita viranomaisille, kuten Tietosuojavaltuutetulle, Poliisille ja Traficomin Kyberturvallisuus- keskukselle ja seuraa heidän antamiaan ohjeita ja suosituksia.
- Säilytä toimintakyky - pidä huolta omasta ja koko henkilöstön jaksamisesta.

3. Jälkeen

Palaudu ja vahvista

- Ota palautussuunnitelman toimet käyttöön. Palautussuunnitelmasta tulisi esimerkiksi löytää ohjeet varmuuskopioiden palauttamiseen tai yleisesti ohjeet laitteiden palauttamiseen.
- Pidä yrityksessä yllä nostettua havainnointitasoa mahdollisten jatkohyökkäysten osalta.
- Jatka yhteistyötä viranomaisten kanssa ja varmista yrityksen tekninen infrastruktuuri.
- Jatka vastuullista viestintää ja huolehdi sidosryhmien tiedonsaannista tilanteen edellyttämällä tavalla.
- Muista jälkipuinti: mitä opittiin ja miten kehitetään varautumista jatkossa, mistä voidaan olla ylpeitä.
- Opi hyökkäyksestä ja tarjoa lisäkoulutusta työntekijöille hyökkäyksestä saatujen oppien avulla.

Ole valmis!

Yritysten digitaaliseen ja fyysiseen toimintaympäristöön kohdistuviin uhkiin ja häiriötilanteisiin voidaan varautua tunnistamalla tärkeät toiminnot ja niihin kohdistuvat riskit, toteuttamalla jatkuvuus- ja valmiussuunnitelmia, sekä koulutuksen ja harjoittelun avulla.

Esimerkiksi aluehallintovirastot järjestävät kuntien, viranomaisten, huoltovarmuuskriittisten yritysten ja muiden turvallisuustoimijoiden yhteisiä alueellisia valmiusharjoituksia.

Valmiusharjoitukset tuovat alueen toimijat simuloidun häiriötilanteen äärelle edistämään yhteiskunnan turvallisuutta. Harjoitukset kehittävät osallistuvien organisaatioiden valmiutta, tilannetietoisuutta ja yhteistoimintaa. Samalla tunnistetaan kehittämiskohteita ja voidaan luoda uusia toimintatapoja, jotka auttavat häiriötilanteen nopeassa hallinnassa ja siitä palautumisessa.

Miksi yritysten tulisi harjoitella ja kehittää toimintaympäristöön kohdistuviin uhkiin ja häiriötilanteisiin varautumista?

Kriisitilanteessa valmiussuunnitelmat ja niiden säännöllinen harjoittelu luovat pohjan yrityksen vakaalle toiminnalle. Valmistautuminen parantaa valmiuksia toiminnan kehittämiseen myös häiriötilanteissa. Samalla voidaan vahvistaa yrityksen ydintoimintoja ja saavuttaa kilpailuetua, muistuttaa juuri päättyneen aluehallintovirastojen yhteisen valmiusharjoitusten kehittämisprojektin vetäjä, eversti evp **Markku Hutka**.

Myös Xamk on mukana havainnoimassa ja arvioimassa harjoituksia. Kokemus valmiusharjoitusten suunnittelusta, valmistelusta ja toteutuksesta hyödynnetään myös Xamkin yrityksille tarjottavien palveluiden kehittämisessä ja yhteistyössä.

Kiinnostaako kyberkriisiharjoittelu?

Tarjoamme Kymenlaaksossa toimiville yrityksille mahdollisuuksia harjoitteluun, ota yhteyttä: kyberkymi@xamk.fi

Näin pääset kyberharjoittelussa alkuun:

Kyberkriisitilanteiden harjoittelu kannattaa aloittaa niistä kriisitilanteista, joista syntyy yritykselle eniten vahinkoa ja jotka ovat todennäköisimpiä.

Kriisitilanteita voi harjoitella ns. työpöytä- harjoituksina tai oikeilla tilanteilla. Työpöytäharjoituksissa yritys käy läpi sen mitä teoriassa tapahtuu, esimerkiksi kun johonkin yrityksen järjestelmään kohdistuu kyberhyökkäys. Oikean tilanteen harjoituksessa yritys toteuttaa kriisi- tilanteen hallitusti oikeilla laitteilla.

Kriisitilanteessa viestinnän, johtamisen ja yhteistoiminnan merkitys korostuu. Näitä on tärkeää harjoitella ennakkoon.

Harjoittelun jälkeen arvioidaan omaa toimintaa ja dokumentaatiota, jotta molempia voi kehittää.

Jatkuvuus- ja valmiussuunnitelma ja siihen liittyvät dokumentit kannattaa käydä läpi vähintään kerran vuodessa. Näin varmistetaan, että suunnitelma pysyy ajan tasalla eikä unohdu.

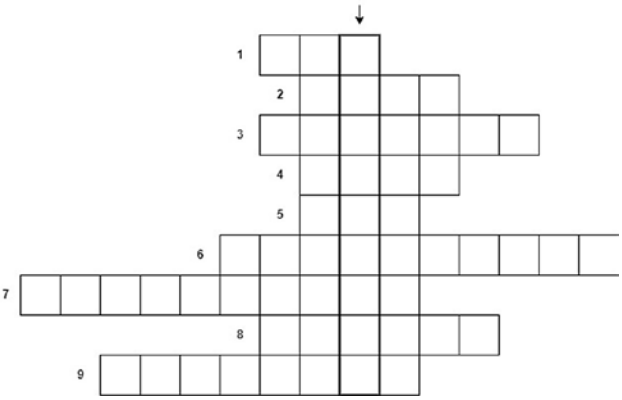
Pulmasivu

Mitä tässä lukee? **4pne45mZxZGW**
Alla olevista tehtävistä ja kuvasta löytyy vinkkejä koodin ratkaisuun. Ratkaisun apuna tarvitset myös hakupalveluita ja internetistä löytyviä työkaluja.

Tehtävä 1.

Täytä ristikko vihjeiden perusteella. Keskelle muodostunut sana auttaa koodin purkamisessa. Monet sanoista ovat lyhenteitä tai suoria käännöksiä. Kaikki sanat löytyvät tästä oppaasta.

1. Esineiden internet
2. Rikos palveluna
3. Artificial Intelligence
4. Kaakkois-Suomen ammattikorkeakoulu
5. Virtuaalinen erillisverkko
6. Kotkan Höyrypanimolla 21.3.2024
7. Kiristyshaittaohjelma
8. Suomen suurin digitaalisen turvallisuuden harjoitus
9. Viestin lähettäjän tietojen muuttaminen



Tehtävä 2.

Täytä alla oleva nonogrammi ohjeiden mukaisesti. Etsi ratkaisuna muodostuvan kuvan vihjettä hakupalveluista. Käytä apunasi hakutulosten antamia työkaluja.

	10	1 1 10	1 1 4 2	8 1 1 2	2 2 1 2	1 1 11	2 9	9 3	2 1 4 3	2 1 1 2 1	2 1 8	15	3 7	3 1 7	3 1 1 7
12															
1 2 9															
2 1 1 4															
1 1 1 3															
2 1 1 1 2															
4 1 3 1															
8 1 2															
12															
2 10															
2 4 1 5															
2 2 1 5															
2 1 2 5															
2 4 5															
9 5															
15															

Nonogrammin täyttöohje:
Ruuturivien ylä- ja sivumarginaaleissa kerrotaan vihjeenä kunkin rivin peräkkäisten väritettävien ruutujen määrä. Väritettyjen ruuturyhmien väliin on aina jätettävä vähintään yksi tyhjä ruutu.

Tehtävä 3.

Jo antiikin Roomassa käytettiin salausmenetelmiä viestien salaamiseen. Alla oleva kuva vihjaa koodin purkamisen viimeiseen vaiheeseen. Tässäkin hakukoneet ja niiden antamat työkalut auttavat ratkaisussa.

Kuva: Playground AI

Ratkaistuasi kaikki tehtävät, pystyt ratkaisemaan sivun alussa annetun koodin. Oikein vastanneiden kesken arvotaan palkintoja. Jos haluat osallistua arvontaan, mene osoitteeseen kyberasema.fi

HUOM. Jos vastaavat koodinratkaisutehtävät kiinnostavat enemmän, Xamk järjestää avoimia CTF- tapahtumia (Capture The Flag) kahdesti vuodessa. Seuraa tulevia tapahtumia kyberasema.fi /ctf.ictlab.fi.

Haetko potkua yrityksesi digikehitykseen? Siirry Digiasemalle!

Digiasema Kymenlaakso kokoaa yhteen osoitteeseen **www.digiasema.fi** kymenlaaksolaisille yrityksille suunnatut digipalvelut, koulutukset ja kehittämismahdollisuudet. Verkkopalvelusta löydät helposti tarpeisiisi sopivia digipalveluja ja koulutuksia. Saat maksutonta apua yrityksesi digiosaamisen ja kehitystarpeiden kartoittamiseen.

XAMK Kaakkois-Suomen ammattikorkeakoulu

cursor

Kouvola Innovation

Euroopan unionin osarahoittama

Tunne huominen.

Xamkin kyberturvallisuuden koulutuksissa saat käytännönläheistä opetusta, uusinta tietoa ja ammattitaitoa, mikä tarjoaa erinomaiset työllistymis- ja uramahdollisuudet kyber- ja tietoturvallisuuden alalla.

Kiinnostaako ura kyberturvallisuuden asiantuntijana?
Insinööri (AMK), kyberturvallisuus *Päiväopiskelu, Kotka*

AMK-koulutuksen ydin on toiminnallisen kyberturvallisuuden taidoissa eli käytännön tekemisessä.

Työskenteletkö jo kyber- ja tietoturvan parissa?
Insinööri (ylempi AMK), kyberturvallisuus *Monimuoto-opiskelu, Kotka*

Syvennä ja päivitä osaamistasi ja pätevöidy monipuolisiin johto-, kehittämis- ja asiantuntijatehtäviin.

Haluatko oppia lisää kyberturvallisuudesta? Hyödynnä Xamk Pulse avoimen amk:n kyberturvallisuuden opintotarjontaa.

Lisätietoa opintojen sisällöistä ja hakuajoista:
www.xamk.fi

XAMK Kaakkois-Suomen ammattikorkeakoulu

Kyberkestävyyttä Kymenlaaksoon!

Tuemme monipuolisella ja maksuttomalla palvelutarjonnalla kuten koulutuksilla ja kyberharjoituksilla kymenlaaksolaisten yritysten kyber- ja tietoturvavalmiuksia.

Teemoina ovat mm. yrityksen tietoturva, NIS2-yhteensopivuus, kyberhygienia ja tietosuoja sekä informaatiovaikuttaminen.

Varaa yritykseesi maksuton tietoturvainfo joko paikan päällä tai etänä!

Saat kattavan käsityksen siitä, miten suojaat yrityksesi ja asiakkaidesi tietoja sekä liiketoimintaasi digitaalisessa ympäristössä. Tarjoamme konkreettisia vinkkejä ja työkaluja, joilla henkilöstösi voi lisätä omaa ja yrityksenne tietoturvaa.

Muista myös kyberturvan huipputapahtuma Kybertuska-päivä maaliskuussa Kotkassa ja verkossa!

Ajankohtaisia sisältöjä, verkkokoulutuksia, podcasteja, videoita ja tapahtumia tieto- ja kyberturvallisuuden vahvistamiseen löydät osoitteesta **www.kyberasema.fi**

XAMK Kaakkois-Suomen ammattikorkeakoulu

30 vuotta KYMEN LAAKSON LIITTO

Euroopan unionin osarahoittama

Palveluja tuottaa Xamkin toteuttama Kyberturvan tulevaisuus Kymenlaaksossa -hanke, jota rahoitta Kymenlaakson liitto oikeudenmukaisen siirtymän rahastosta (JTF) yhteistyössä Kymvake – Kymenlaakson alueellisen varautumisyhteistyön kehittäminen -hankkeen kanssa, jota rahoittaa Kymenlaakson liitto Euroopan aluekehitysrahastosta (EAKR).

Osoitelähde: Vainu.io -yritystietokanta