Kohti
kyberturvallisuuskulttuuria

Kuinka innostat
ihmiset nostamaan
kyberturvatietoisuuden
tasoa organisaatiossasi

CGI

SISÄLLYSLUETTELO

Kyberturvallisuuskulttuuria rakentamassa

Lukuisat esimerkit ovat osoittaneet, että aikamme kyberuhat koskettavat paitsi liiketoimintoja, myös yksityisyyden suojaa. Kyberturvallisuuden tärkeys on tunnistettu ja siihen investoidaan. Mutta miksi, kaikista teknologioista huolimatta, riskit ovat ainoastaan lisääntyneet? Koska kyberturvan kannalta tärkein tekijä on inhimillinen tekijä – tottumuksemme, joilla vaarannamme sen. Juuri tätä heikkoutta hyödyntääkseen rikolliset kehittävät entistä kekseliäämpiä huijauskeinoja.

Kyberturvallisuuden tulisikin olla ennen kaikkea rutiinia, aivan kuten huolellisen käsienpesun flunssakaudella. Mutta paraskin ohjeistus on vain ohjeistus, ja parhaatkin ohjeistukset unohtuvat. Niin myös kerran vuodessa järjestettävät koulutukset. Jokaisen on tiedostettava paitsi oma vastuunsa, myös oma etunsa, sillä kyberturvan kannalta riskialttiit tavat eivät rajoitu työpaikoille.

Mutta miten kyberturvallisuudesta luodaan osa arkea? Innostamalla, kannustamalla, auttamalla, ohjeistamalla, tukemalla ja avoimella keskustelulla – säännöllisesti. Näin syntyy vahva kyberturvakulttuuri, joka auttaa varmistamaan päivittäisen toiminnan.

Missiomme CGI:llä on auttaa tekemään kyberturvallisuudesta innostavaa ja arkipäiväistä. Tämä opas on kirjoitettu organisaatiosi kaikille toiminnoille ja tasoille. Havainnollistamme käytännön esimerkein, kuinka pienistä teoista riippuvat suuret asiat, sekä kerromme, miten kyberturvatietoisuus aikaansaadaan ja -kulttuuri rakennetaan.

Oivaltavia lukuhetkiä toivottaen,

Pauliina Nikko-Takala
Director, Security Programs and Awareness

83 %
haittatapahtumista johtuu huonosta kyberhygieniasta

90 %
kyberongelmista aiheutuu inhimillisestä virheestä

91 %
kyberhyökkäyksistä alkaa tietojen kalastelulla

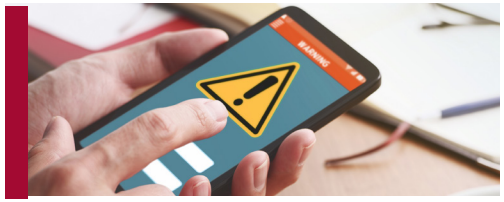
KYBERTURVALLISUUS NYT – NYKYTILAN HAASTEET

Kyberturvallisuus koskee kaikkia

Tiesitkö, että yli 90 prosenttia kyberuhista aiheutuu ihmisen myötävaikutuksesta? Tai että yli 91 prosenttia kyberhyökkäyksistä alkaa tietojen kalastelulla? Vaarassa eivät ole ainoastaan liiketoiminnot, vaan myös ihmisten henkilökohtaiset ja arkaluontoiset tiedot. Seuraavat arkiset esimerkit osoittavat, kuinka oveliksi kyberhyökkäykset ovat muuttuneet. Jos kokeneen kyberturvallisuusasiantuntijan on usein mahdotonta tunnistaa väärennystä aidosta, kuinka siihen pystyisivät tavalliset ihmiset?

KIIREELLINEN KYSYMYS

Oli kuuma kesäpäivä, ja lomakausi oli juuri alkanut. Maija oli hilpeällä mielellä, sillä tämä oli palkanlaskennasta vastaavalle harvinaista herkkua. Vastuullisena työntekijänä Maija piti työpuhelinta mukanaan, kaiken varalta. Pian hän saikin kiireelliseksi merkityn sähköpostiviestin, jossa luki: ”Hei Maija, voisitko auttaa minua pikaisesti. Vaihdoin pankkia juuri ennen kesälomaani, ja seuraava palkka pitäisi ohjata uudelle tililleni. Uusi tilinumeroni on FI12 1234 1234 1234 12. Kiitos, että vastaat nopeasti ja pahoittelut, että jouduin häiritsemään lomaasi. Terveisin, Matti Meikäläinen”. Seurauksena Matin palkka ohjautui huijarin tilille.



LAINAKSI JA AINIAAKSI POISSA

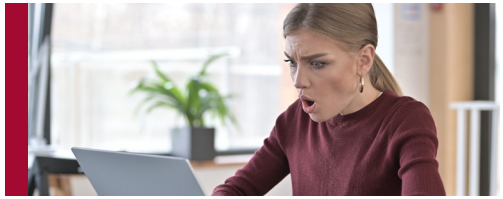
Työpuhelin kulki kotiin myös viestintäjohtaja Pasin taskussa – olihan yhdestä laitteesta tarpeeksi vaivaa. Sitä paitsi häntä saatettiin tarvita. Mutta iltaisin perheen varhaisnuoriso pyysi kerta toisensa jälkeen Pasin puhelinta lainaksi, jotta he voisivat pelata siihen lataamiaan pelejä. Puhelimeen asennetun peliohjelman kautta laitteeseen pääsi haittaohjelma ja Pasin arkaluonteiset tiedot päätyivät vääriin käsiin.

SAISINKO SALASANAN

Talouspäällikkö Riitta oli kiireinen nainen, jolla riitti tekemistä. Hän oli oppinut yksinkertaistamaan kaiken minkä voi, myös salasanansa. Riitalla oli sama, lyhyt ja helposti arvattava salasana kaikkiin sovelluksiin ja palveluihin sekä kotona että työssä. Kukapa niitä jaksaisi muistella? Laitteiden käytössä Riittaa häiritsivät eniten jatkuvat päivitykset ja ilmoitukset. Erään kerran häneltä pyydettiin salasanan vahvistusta. Ärsyyntynyt Riitta syötti salasanan tutulta näyttävään ikkunaan, mutta kuinka kävikään? Kysyjä ei ollut sitä, miltä näytti. Asiaa ei auttanut se, että talouspäällikkönä Riitan tunnuksilla oli pääsy kaikkiin yrityksensä talousdokumentteihin ja -järjestelmiin. Vahinko laskettiin miljoonissa.

PÄÄ PILVISSÄ

Liiketoimintajohtaja Seppo oli varma, että hänen organisaatiossaan olivat kyberturvallisuusasiat kunnossa. Olihan heillä paitsi kattava näkyvyys liiketoiminnan uhkiin, kyberuhkat mukaan lukien myös ajan tasalla oleva teknologia ja asiantunteva kumppani varmistamassa kyberuhkien havainnointia. Lisäksi henkilöstölle oli tehty ohjeistus, jopa järjestetty vuosittaiset tietoturvakoulutukset. Mutta Seppo ei ottanut huomioon, että hänen liiketoiminta-alueella oli juuri otettu käyttöön uusi IoT-järjestelmä, jonka kyberturvallisuuden varmistaminen ei ollut kenenkään vastuulla. Verkkotason eristäminen oli jäänyt tekemättä ja laitteisiin oli jäänyt haavoittuvuuksia, jonka johdosta ne altistuivat kyberhyökkäyksille.



KIRISTYSTÄ

Toimistosihteeri Niina oli menevä nuori aikuinen, jolle älypuhelin oli kuin toinen elämä. Työpuhelin kulki hänen mukanaan kaikkialle, ja laitteeseen tallentui sellaisiakin asioita, joiden ei olisi pitänyt. Eräänä päivänä Niinaa odotti järkytys – sähköposti, jossa ilmoitettiin, että kirjoittaja oli kaapannut hänen arkaluontoiset valokuvansa. Niina oli kyllä lukenut näistä rikollisista, mutta kohtasi nyt ensimmäistä kertaa sellaisen. Kiristäjä asetti ehdot – ”Anna bitcoineja, tai julkaisemme arkaluonteisen aineiston kaikille kontakteillesi”. Niina totteli ja maksoi pyydetyt lunnaat.

VÄÄRÄ OSOITE

Vastuuntuntoinen lääkäri Pertti oli tehnyt jälleen kerran liikaa töitä. Hänen hermojaan oli koeteltu jo viikkoja, väsymys painoi ja väsymystä seurasivat virheet. Tällä kertaa virhe päätyi vastaanottajan osoitekenttään. Arkaluontoinen potilastieto sosiaaliturvatunnuksineen lähti väärille henkilöille, eikä sitä huomannut edes Pertti itse. Mutta seuraukset eivät jääneet keneltäkään huomaamatta.

Haasteista heräämiseen

Teknologia yksin ei riitä takaamaan kyberturvallisuutta. Nykyisiin ja tuleviin uhkiin vastaaminen edellyttää saumatonta yhdistelmää älykästä teknologiaa, uhkatietoa, kyberturva-ammattilaisten osaamista ja mikä tärkeintä, tavallisten ihmisten tietoja ja taitoja.

Miksi tietoturvaohjeita ja -käytäntöjä on niin helppo laiminlyödä? Tahattomasti tai tahallaan. Yrityksissä, joilla ei ole syntynyt kyberturvakulttuuria, toistuvat aina samat haasteet. Niistä merkittävin on se, etteivät ihmiset tiedosta omaa rooliaan, vastuutaan eivätkä tekojensa seurauksia. Suuri osa ihmisistä ajattelee edelleen, että kyberturvallisuusasiat ratkaistaan organisaation it- tai tietotuvaturvaosastolla. Sitä, että turvallisuus on lopulta jokaisen ihmisen omissa käsissä, ei ymmärretä.

Tyypillisiä kyberturvaan liittyviä kommentteja:

- ”En mitenkään muista kaikkien palveluiden salasanoja. On paljon helpompaa käyttää samoja salasanoja useammassa palvelussa.”
- ”Miksi minun pitäisi huolehtia laitteiden ja ohjelmistojen päivityksestä tai yrityksen kyberturva-asioista? Meillähän on IT-osasto sitä varten, että he miettivät nämä asiat puolestani.”
- ”Mitä sitten, jos klikkaan jotain väärää linkkiä? Koneellani on virustorjuntaohjelmisto, joka nappaa kiinni kaikki virukset.”
- ”Minulla on niin kova kiire ja paine töissä, että en mitenkään ehdi suorittaa kyberturvakoulutuksia tai lukea ohjeita.”
- ”Haluamme julkaista uusia digipalveluja nopeasti ja ketterästi. Kyberturvan varmistaminen on liian hidasta ja kallista. Kilpailijat ehtivät edellemme, jos joudumme noudattamaan kaikkia prosesseja.”
- ”Kuka muka olisi kiinnostunut meidän tiedoistamme? Mehän olemme niin pieni toimija turvallisessa Suomessa, etteivät huijarit meihin kohdista hyökkäyksiä.”

Ongelman ydin on se, etteivät kyberturvallisuuden tarpeellisuuden, vaatimustenmukaisuuden tai riskikäyttäytymisen todistamiseen perustuvat puisevat koulutukset motivoi ihmisiä oppimaan. Tilannetta eivät paranna monimutkaiset, pitkät ja monesti tekniset ohjeistukset, joiden sisältöä on vaikea omaksua. Siksi kyberturvallisuutta on lähdettävä kehittämään uusin ja innostavin keinoin. Avainsanoja ovat avoimuus, vaikuttavuus, kokemuksellisuus, yhteinen kieli, yhteiset tavoitteet, mitattavat tulokset ja toisto – kestävän kyberturvakulttuurin kulmakivet.

Tunnista tilanteesi, löydä ratkaisusi

Jotta kyberturvallisuudesta saadaan osa ihmisten arkea ja kulttuuria, tulee toimintaa kehittää, seurata ja mitata järjestelmällisesti. Tähän auttaa kyberturvatietoisuuden kypsyysmalli:

0. Organisaatiossani ei ole panostettu henkilöstön kyberturvatietoisuuden kehittämiseen

Kun kyberturvallisuus on henkilöstölle uusi ja tuntematon käsite, hyviä tapoja aloittaa ovat esimerkiksi kyberturvatietoisuusohjelman luominen ja vuosikello sekä koko henkilöstön säännöllinen kouluttaminen ja ohjeistusten päivittäminen kaikille ymmärrettäviksi.

I. Organisaationi kyberturvatietoisuus perustuu vaatimuksenmukaisuuteen

Pienissä ja julkisen sektorin organisaatioissa sekä vahvasti säädellyillä toimialoilla tyypillinen tilanne on se, että organisaation kyberturvatietoisuus perustuu pakkoon. Ulkopuolisten vaatimusten johdosta henkilöstöä on koulutettava ja ohjeistettava kyberturvallisuusasioissa. Tällöin ohjeistuksia noudatetaan vain pakosta, eivätkä ihmiset ymmärrä sen hyötyä tai merkitystä itselleen. Valitettavasti hyvät tavat unohtuvat nopeasti. Tällöin sopivia keinoja tietoisuuden kehittämiseksi ovat kyberturvatietoisuusohjelman luominen, testaukset ja harjoitukset sekä riskiryhmille räätälöidyt koulutukset.

II. Organisaatiossani on aloitettu kyberturvatietoisuuden kehittäminen

Kyberturvatietoisuuden merkitys on ymmärretty ja toimenpiteisiin on ryhdytty. Toimenpiteitä toteutetaan tärkeimpien teemojen ympärillä ja ne tähtäävät muuhunkin kuin pakolliseen vuosittaiseen koulutukseen. Seuraava askel on lähteä kehittämään kyberturvakulttuuria säännöllisillä toimenpiteillä.

III. Organisaatiossani on kyberturvatietoisuuden ohjelma, tavoitteenaan kyberturvakulttuurin luominen

Kun ihmiset ovat ymmärtäneet kyberturvan merkityksen sekä työssään että henkilökohtaisessa elämässään, haasteena on ylläpitää ja kehittää innostusta. Tämä onnistuu kyberturvatietoisuusohjelman mukaisilla säännöllisillä toimenpiteillä. Näitä voivat olla esimerkiksi tietoisuustason testaaminen palkitsevin haastein, innostava viestintä, sisäiset kampanjat, tempaukset ja teemapäivät, pelillistämistä hyödyntävät koulutukset, ohjeistusten visualisointi yhä ymmärrettävämpään muotoon sekä toistuvat harjoitukset kriisitilanteiden varalta.

IV. Organisaationi kyberturvatietoisuus perustuu pitkän tähtäimen suunnitteluun ja kulttuuriin

Kyberturvatietoisuusohjelmaa johdetaan ja hallitaan järjestelmällisesti. Ohjelmalla on hiotut prosessit, riittävät resurssit ja johdon tuki. Kyberturvatietoisuus on osa henkilöstön arkea ja kulttuuria. Kyberturvallisuuden ja kyberturvatietoisuusohjelman merkitys ja tarpeellisuus ymmärretään laajasti koko organisaatiossa.

V. Organisaationi kyberturvatietoisuus perustuu mitattaviin tuloksiin ja jatkuvaan kehittämiseen

Organisaatiosi on saavuttanut kyberturvatietoisuudessa sellaisen tason, jossa se voi paitsi vahvistaa omaa asemaansa mitatuin tuloksin, myös toimia edelläkävijänä markkinassa. Tietoisuuden ja kulttuurin kehittymistä seurataan ja mitataan järjestelmällisesti. Kyberturvatietoisuusohjelma ja organisaation kyberturvallisuuden hallinta kehittyvät mittaamisen tuloksena. Kyberturvallisuudestaan tunnettu organisaatio on sekä haluttu ja arvostettu kumppani että työnantaja, joka voi vaikuttaa myönteisesti koko toimialaansa.

I. Kyberturvatietoisuus perustuu vaatimuksenmukaisuuteen

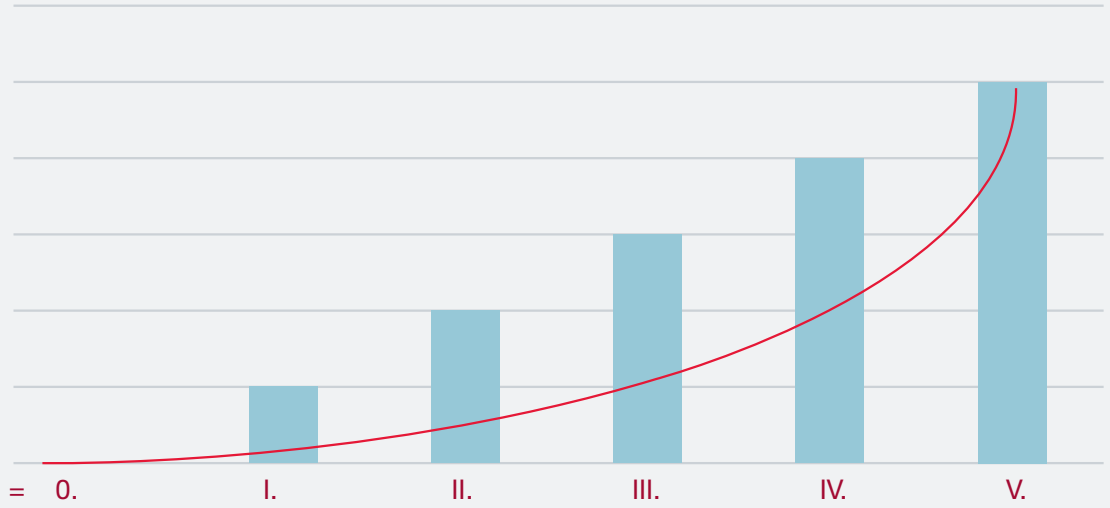
II. Kyberturvatietoisuuden ohjelma käynnistetty

III. Kyberturvatietoisuuden ohjelma tähtää kulttuurin muutokseen

IV. Kyberturvatietoisuuden ohjelma on hallittua ja osa kulttuuria

V. Toimintaa seurataan, mitataan ja kehitetään järjestelmällisesti

Kyberturvatietoisuuden tasot



KUINKA INHIMILLISET KYBERTURVALLISUUSHAASTEET RATKAISTAAN

Kyberturvaa ilon kautta – kuinka kyberturvakulttuuri rakennetaan

Oppiminen on tehokkainta, kun se tapahtuu ilon ja oivalluksen kautta, ja tämä pätee myös kyberturvallisuuteen. Siksi ei ole samantekevää, kuinka asiat esitetään. Ihmiset on saatava ennen kaikkea samaistumaan ja innostumaan. Entä miksi osallistaminen on niin tärkeää? Koska unohdamme pääosan yksisuuntaisen viestinnän sisällöstä. Pelkästä lukemisesta ja kuulemisesta mieleemme jää vain murto-osa, mutta keskustelu, jaetut kokemukset ja toisille opettaminen muuttavat asetelman täysin, toistosta puhumattakaan.

Viime vuosina yleistä tieto- ja kyberturvallisuuskeskustelua on leimannut pelko. Uhilla pelottelemalla ja syyttelemällä on yritetty saada ihmiset ymmärtämään, että he ovat tietoturvan heikoin lenkki. Asenteita, käyttäytymistä tai kyberturvakulttuuria ei kuitenkaan voida muuttaa pakon ja pelottelun keinoin – ilman korjaavien toimenpiteiden ja työkalujen antamista tämä voi jopa heikentää ihmisten motivaatiota noudattaa tietoturvaohjeistuksia.

Asenteisiin ja käyttäytymiseen vaikutetaan parhaiten auttamalla ihmisiä ymmärtämään riskien vakavuus ja todennäköisyys heidän omasta näkökulmastaan sekä tarjoamalla tietoa siitä, kuinka näihin riskeihin tulisi suhtautua ja miten toimia niitä kohdatessaan. Ihmisille on tehtävä selväksi heidän tärkeä roolinsa kyberturvallisuuden ylläpitäjinä, myönteisen kautta. Kulttuurin luomisen lähtökohtia ovat koulutukset, säännöllinen viestintä ja ohjeistukset.

Toistolla tuloksiin

Perinteisiä ja tehokkaita koulutuskeinoja ovat koko henkilöstön perustason tietoturvakoulutukset ja valmennussarjat. Niiden tehtävänä on tietoisuuden herättäminen ja ylläpito. Käytännössä tämä tarkoittaa esimerkiksi tunnin koulutusta tai toistuvia 15 minuutin tietoiskuja, joiden sisältö on omaksuttavissa joko sellaisenaan tai osana laajempaa kokonaisuutta. Koulutukset voit järjestää yhtä hyvin luokkahuoneessa tai liittämällä ne sähköiseen koulutusalustaan ja intranetiin. Tehokkaimpia ovat toistuvat lyhyet koulutukset tai tietoiskut. Koulutusten teemoja voivat olla esimerkiksi kyberturvallisuuden tilanne ja trendit, riskit oman organisaation näkökulmasta, perustelut siitä miksi jokaisen rooli on tärkeä, oman työympäristön, tietojen ja laitteiden suojaaminen sekä oikeat toimintatavat eri tilanteissa.

Organisaation eri toiminnoille, kuten johdolle, taloushallinnolle, asiakastyötä tekeville, ohjelmistokehittäjille, tuotannolle ja myymälähenkilöstölle suunnatut roolipohjaiset valmennukset tukevat perustason tietoiskuja ja koulutuksia. Valmennusten sisältö tulee räätälöidä kullekin kohderyhmälle sopivaksi. Niiden teemoja voivat olla esimerkiksi ohjelmistokehityksen tietoturva, ISO27001, kyberturva taloushallinnossa, DevSecOps, etätyön kyberturva, sosiaalinen manipulointi ja niin edelleen – pääasia on, että sisällöt vastaavat kuulijoiden osaamistasoa ja arkista tarvetta.

Vain selkeä viesti menee perille

Viestinnän rooli ja tärkeys unohtuvat helposti, kun kyberturvallisuutta jalkautetaan. Tavallisesti it- tai tietoturvaosaston teknisesti suuntautuneet henkilöt vastaavat myös henkilöstöohjeistusten laatimisesta. Ohjeista tulee helposti pitkiä ja teknisiä. Pahimmillaan ohjeita ei lue kuin murto-osa henkilöstöstä. Toimiva ratkaisu tietoturvaohjeistuksiin on tuottaa pakollisen tietoturvapolitiikan ja toimeenpanevien ohjesäännösten ohella helposti ja nopeasti omaksuttavia lyhyitä pikaohjeita. Parhaimmillaan ne ovat visuaalisia, viestivät positiiviseen sävyyn ja auttavat ihmisiä ymmärtämään asiat yhdellä silmäyksellä.

Säännöllinen viestintä ja aiheen tärkeydestä muistuttaminen ovat avaimet onnistumiseen. Mitä henkilökohtaisemmaksi ja ajankohtaisemmaksi viestin tai ohjeen saat, sitä varmemmin se toimii vastaanottajassa. Jos esimerkiksi kyberturvakumppanisi kautta käytössänne oleva tietoturvan valvontapalvelu varoittaa Suomeen mahdollisesti rantautuvasta uudesta kalastelukampanjasta, kannattaa henkilöstölle viestiä asiasta ennen kuin tuhoa ehtii syntyä.

Pisimmällä kyberturvallisuuskulttuurin luomisessa ovat ne organisaatiot, joissa ymmärretään viestinnän ja markkinoinnin merkitys – toisinaan kyberturvatietoisuudesta vastaa viestintätaustainen henkilö ja toisinaan taas toimintaa johdetaan vahvasti tietoturvaorganisaatiosta, mutta talon sisäiset ja kumppaneiden resurssit on valjastettu kyberturvatietoisuustyöhön. `

INNOSTAVAT KEINOT

Innostavia keinoja kyberturvakulttuurin luomiseen ovat esimerkiksi pelillistäminen, visuaalinen viestintä, kilpailut, kampanjat, tempaukset ja teemapäivät. Nämä soveltuvat parhaiten organisaatioille, joissa on jo panostettu kyberturvallisuustietoisuuden lisäämiseen ja käyttäytymisen muutokseen. Silloin perinteisistä keinoista, kuten koulutuksista ja valmennussarjoista, on tullut rutiinia.

Hyviä keinoja ovat esimerkiksi:

- Sisäisen tietoturvan brändäys: oma tunnistettava logo, tunnus tai hahmo, joka toistuu kaikessa tietoturvaan liittyvässä viestinnässä sekä koulutuksissa ja ohjeistuksissa.
- Positiivinen äänensävy: parhaan vaikutuksen henkilöstöösi tekevät kannustaminen ja myönteinen asenne.
- Vuosittainen kyberturvallisuusviikko: järjestetään toimenpiteitä niin sisäisissä digikanavissa kuin fyysisesti paikan päällä. Lokakuussa järjestettävän kansainvälisen kyberturvallisuuskuukauden aikana julkaistaan kerran viikossa uusi innostava video, joka pureutuu tärkeimpiin kyberturvallisuusteemoihin henkilöstön näkökulmasta.
- Tietoturvaohjeet sarjakuvana: toteutetaan tärkeimmistä henkilöstön ohjeistuksista sarjakuva, jossa seikkailee koko organisaatiolle tuttu rooli tai hahmo.
- Säännölliset kalasteluharjoitukset: autetaan henkilöstöä tunnistamaan kalasteluviestejä sekä toimimaan oikein lähettämällä heille säännöllisesti tekaistuja kalasteluviestejä.
- Kyberturvallisuusaiheinen pakohuonepeli: ihmiset saadaan kiinnostumaan kyberturvallisuudesta oman kokemuksen ja pelillistämisen avulla.
- Palkitseminen hyvästä kyberturvatoiminnasta: kun huomaat, että ohjeita noudatetaan ja tietoisuus lisääntyy, anna palkintoja ja positiivista huomiota, kuten kunniakirja kaikille tietoturvakoulutuksen täysin pistein läpäisseille, mitali vuoden parhaimmille kalasteluviestibongareille tai pieni lahja kyberturvallisuuden teemaviikon kilpailuun osallistuneille.

Tietoturvaorganisaation kulttuurinmuutos kumppaniksi ja mahdollistajaksi

Liiketoiminnan ja sisäisen tietoturvaorganisaation välissä on usein kuilu. Osapuolet ymmärtävät toisiaan tai toimintaansa vaikuttavia tekijöitä riittävästi vain harvoin. Tieto- ja kyberturvallisuudesta vastaaville henkilöille tietoturva on luonnollisesti aina ykkönen, jolloin helppoudesta ja käytettävyydestä joudutaan toisinaan tinkimään, jotta organisaatio, tiedot ja ihmiset pysyvät turvassa. Liiketoiminnan ajureina toimivat tyypillisesti asiakaskokemus ja kasvu – työtä halutaan tehdä ketterästi ja uusia palveluita julkaista nopeasti. Entä jos tietoturvaorganisaatio olisikin kasvun mahdollistaja? Liiketoiminnan kumppani, joka tukee uusia työtapoja, liiketoiminnan kehitystä ja digitalisaatiota. Ja vieläpä siten, että kaikki osapuolet sitoutuvat yhteisiin toimintamalleihin ja työkaluihin.

Esimerkkejä keinoista onnistuneeseen kulttuurinmuutokseen:

Yhteinen kieli:

varmista, että osapuolet puhuvat toisilleen ymmärrettävällä tavalla.

Avoin keskustelu:

erilaisten näkökulmien ja tarpeiden ymmärtäminen on lähtökohta muutokselle. Keskustelua liiketoimintojen ja tietoturvan avainhenkilöiden välillä tarvitaan paljon ja säännöllisesti.

Nykytilan ymmärtäminen:

selvitä ja tutki, missä prosesseissa luistetaan ja mitä it:n hyväksymättömiä palveluja ja työkaluja on käytössä. Tärkeintä on selvittää syy, miksi näin toimitaan.

Oikea asenne:

suhtautumalla ymmärtäväisesti, tarjoamalla kieltojen sijasta ratkaisuja sekä tukemalla liiketoimintoja muutoksessa, onnistut luomaan luottamuksellisen kumppanuuden, joka auttaa huomioimaan tietoturvan kehityshankkeiden alusta alkaen.

Yhteisön voima:

koko organisaation kyberturvallisen toiminnan varmistaminen ei voi olla yhden tai muutaman henkilön varassa. Valjasta lisää oikealla tietoturva-asenteella varustettuja henkilöitä tärkeään työhön. Heitä voidaan kutsua esimerkiksi Security Business Partnereiksi, Security Ambassadoreiksi tai Security Championeiksi.

Yhteinen päämäärä:

asetetaan tavoitteet siten, että niiden yhteinen hyöty on kaikille osapuolille selvä.

KYBERTURVATIETOISUUDEN KEHITTÄMINEN JA JOHTAMINEN

Kaiken perusta: kyberturvatietoisuuden ohjelma ja vuosikello

Ensimmäinen ja tärkein askel henkilöstön kyberturvatietojen ja -taitojen kehittämisessä on luoda kyberturvatietoisuusohjelma, johon organisaation johto sitoutuu. Kyberturvatietoisuuden tasoa on mahdollista nostaa järjestelmällisesti ja kustannustehokkaasti ainoastaan organisaation tarpeisiin, tavoitteisiin ja resursseihin perustuvalla ohjelmalla.

Askeleet kyberturvatietoisuusohjelman luomiseksi

1. **Analysoi nykytilanne:** selvitä organisaatiosi kybeturvatietoisuuden kypsyystaso. Millaisia haasteita ja tarpeita toimintaan kohdistuu? Mitkä ovat toiminnan kipupisteet ja pullonkaulat? Mitä toimenpiteitä on tähän mennessä tehty ja millaista palautetta niistä on saatu? Tutki, testaa ja haastattele eri henkilöitä organisaatiossasi.
2. **Suunnittele ohjelma:** määrittele lyhyen ja pitkän tähtäimen tavoitteet, kohderyhmät, resurssit ja mittarit, joilla ohjelmaa hallitaan. Rakenna tiekartta, valitse tärkeimmät viestittävät teemat ja luo vuosikello, jossa kyberturva-asioista viestitään henkilöstölle säännöllisesti ja innostavasti.
3. **Toteuta eri kohdeyleisöille suunnattuja toimenpiteitä:** tärkeintä on positiivisuus, ajankohtaisuus ja toisto. Vaihtelua tuo erilaisten toimenpiteiden yhdistely – alkuvuodesta panostetaan koulutukseen ja ohjeistuksiin, syksyllä järjestetään sisäinen teemaviikko tai kampanja ja loppuvuodesta toteutetaan fyysisen turvallisuuden testaus tai kyberturvallisuusharjoitus. Jatkuvana toimenpiteenä toteutetaan esimerkiksi kuukausittaisia kalastelutestauksia ja viestiintää.
4. **Mittaa vaikutusta:** kerää dataa ja palautetta säännöllisesti. Yksittäisten toimenpiteiden mittaamisen lisäksi seuraa myös kyberturvatietoisuusohjelman edistymistä ja vaikuttavuutta sekä käyttäytymisen muutosta ja -kulttuurin kehittymistä.
5. **Optimoi ja kehitä toimintaa:** vertaa tuloksia tavoitteisiin ja analysoi. Tunnista kehityskohteita, uusia tarpeita, teemoja ja kohdeyleisöjä. Pyri jatkuvaan kehittymiseen. Toteuta toimenpiteitä, jotka näkyvät myös organisaatiosi ulkopuolelle. Valjasta valkohattuhakkerit käyttöösi Bug Bounty -ohjelmalla, organisoi Hack Day -tapahtuma tai järjestä henkilöstön ja asiakkaiden perheille tietoturvapäivä.

Esimerkki kyberturvatietoisuuden vuosikellosta

1 Vuosisuunnittelu
- Vuosikellon päivitys ja kehitystoimien määrittely
- Viestintä: tulokset, tavoitteet ja tulevat toimenpiteet

2 Koulutus
- Tietoisku tai koulutus valitusta aiheesta

3 Viestintä
- Nosto tai vinkki valitusta aiheesta

4 Testaus tai harjoitus
- Esim. kalasteluharjoitus (koko henkilöstö ja kohdennettu)

5 Tapahtuma
- Vuoden päätapahtuma, esim. tietoturvaviikko, valituilla toimipisteillä

6 Viestintä
- Loma-aikana huomioitavat tietoturva-asiat

7 Puolivuotiskatsaus
- Suunnitelmien ja raporttien kevyt päivitys ja läpikäynti

8 Koulutus
- Tietoisku tai koulutus valitusta aiheesta

9 Viestintä
- Syksyn toimenpiteet ja nosto tai vinkki valitusta aiheesta

10 Kyberturvallisuuskuukausi
- Awareness-kampanja kaikilla toimipisteillä
- Kohdennettuja koulutuksia ja tapahtumia

11 Testaus
- Kyberturvatietoisuuden tason testaus esim. henkilöstökyselyn avulla

12 Yhteenveto
- Vuoden raportti ja analyysi
- Koulutus: lisäkoulutus sitä tarvitseville

* Esimerkki kyberturvatietoisuuden vuosikellosta koko henkilöstölle.
Vuosikello suunnitellaan aina asiakaskohtaisesti.

Hyvän kyberturvatietoisuusohjelman sisältö

1. Tavoitteet ja mittarit

Millaisia lyhyen ja pitkän tähtäimen tavoitteita toiminnalle asetetaan? Mille kyberturvatietoisuuden kypsyystasolle organisaatio tähtää? Millainen on henkilöstölle viestittävä innostava visio tai tavoite, joka mahdollistaa kulttuurinmuutoksen? Pue tavoitteesi sanoiksi, joihin jokainen ihminen organisaatiosi jokaisella tasolla voi samaistua. Määrittele myös mittarit, joilla seuraat tavoitteiden saavuttamista.

2. Kohderyhmät

Millaisia ihmisiä organisaatiossasi työskentelee? Mitkä roolit ovat kyberturvan kannalta kriittisimmät? Mitä tarpeita heillä mahdollisesti on, ja millaisia uhkia heihin kohdistuu? Koko henkilöstön ohella kyberturvatietoisuusohjelmassa erikseen huomioitavia kohderyhmiä ovat esimerkiksi johto ja esimiehet, IT, ohjelmistokehittäjät sekä kolmannen osapuolen toimittajat ja tuotantohenkilöstö.

3. Tärkeimmät teemat

Mitkä ovat tärkeimpiä teemoja, joista kohdeyleisöille tulisi viestiä? Onko näköpiirissä uudenlaisia toimintatapoja tai kehityshankkeita, jotka edellyttävät henkilöstön lisäkouluttamista tai ohjeistusta? Tyypillisiä teemoja ovat esimerkiksi kyberturvallisuushygienia (mm. salasanat, päivitykset ja muut kyberturvan perusasiat), etätyön tietoturva, ohjelmistokehityksen tietoturva sekä huijausten välttäminen.

4. Viestinnän ilme ja sävy

Myös sisäinen viestintä tarvitsee visuaalisen ilmeen, jonka tulee näkyä henkilöstön päivittäisessä työssä ja kaikissa ympäristöissä aina, kun viestitään tai ohjeistetaan tietoturvaan liittyviä asioita. Entä millainen on tapa, jolla sisäinen tietoturvaorganisaatio viestii? Sisäisen viestinnän äänensävy kannattaa määritellä etukäteen – varmimmin toimivat myönteinen asenne, kannustaminen ja avoimuus.

5. Viestinnän kanavat

Mitä sisäisiä viestintäkanavia organisaatiossasi on käytössä? Kuinka eri kohdeyleisöt tavoitetaan? Millä tavoin viestintä on tehokasta ja tarkoituksenmukaista? Sisäiset viestintäkanavat kannattaa määritellä kohdeyleisön mukaisesti – esimerkiksi ohjelmistokehittäjiä kannattaa lähestyä eri tavalla kuin koko henkilöstöä.

6. Tarkoituksenmukaiset toimenpiteet

Millaiset toimenpiteet ovat toimineet tähän asti? Minkälaisista ohjeista, koulutuksista tai tempauksista olet saanut hyvää palautetta? Millaisia toimenpiteitä käytettävissä olevalla budjetilla on mahdollista toteuttaa?

Palveluksessasi CGI – kyberturvallisuuskulttuurisi rakentaja

CGI muuttaa uhat mahdollisuuksiksi innostaen henkilöstösi kyberturvallisuudesta. Tehtävämme on varmistaa organisaatiosi toimintakyky, sujuvat työnkulut ja mielenrauhasi – ympäri vuorokauden ja vuoden jokaisena päivänä.

Miksi CGI on oikea kumppanisi:

- Kaikki tarvitsemasi kyberturvallisuuden palvelut saman katon alta, alkaen riskien hallinnasta kyberturvatietoisuuden kehittämiseen ja jatkuvaan kyberturvauhkien valvontaan.
- Asiakastyytyväisyys 9+/10: motivoitunut ja koulutettu henkilöstö palveluksessasi.
- Kansainvälistä puolustuskykyä: maailmanlaajuinen, 1700 kyberturva-ammattilaisen, Suomessa 100+ ammattilaisen ja kahdeksan kyberturvallisuuskeskuksen verkosto käytössäsi.
- Yhdistelmä kyberturvan teknistä ja hallinnollista asiantuntijuutta yhdistettynä markkinoinnin ja viestinnän osaamiseen.
- Apua tarpeesi mukaan: hoidamme niin jatkuvat palvelut kuin yksittäiset kyberturvaratkaisut.
- Kyberturvaa rutiinilla: yli 40 vuoden kokemus valtioiden, yritysten ja yhteisöjen kyberturvasta Pohjoismaissa, Euroopassa, Yhdysvalloissa ja Aasiassa.
- Toimintaperiaatteena jatkuva kehittäminen. Tavoitteemme on aikaansaada mitattavia tuloksia kohti aitoa organisaation kyberturvakulttuuria. Hyödynnämme parhaita käytäntöjä ja monistettavia ratkaisuja sekä innovoimme uusia palveluja – Suomessa ja globaalisti.

Kohti kyberturvallisuuskulttuuria

Autamme sinua kehittämään henkilöstösi kyberturvatietoisuutta ja organisaatiosi kyberturvakulttuuria. Alkuun pääset yhdessä suunnittelemamme kyberturvatietoisuusohjelman ja vuosikellon avulla. Selvitämme henkilöstösi osaamistason kyselyillä, testauksilla ja harjoituksilla, sekä valmennamme heidät säännöllisesti ja innostavasti. Parhaat tulokset saavutat yhdistämällä CGI:n vankan teknisen ja hallinnollisen kyberturvallisuusosaamisen innostavaan viestintään. Tuemme sinua kyberturvatietoisuuden ja -kulttuurin kehittämisessä myös jatkuvana palveluna. Astu kanssamme kyberturvallisempaan huomiseen!

Lisätietoa: cgi.fi/kyber

Pauliina Nikko-Takala
Director, Security Awareness and Programs
050 410 8369
pauliina.nikko-takala@cgi.com

Stefan Anderson
Director, Cybersecurity Consulting
040 160 8686
stefan.anderson@cgi.com

CGI LYHYESTI

CGI on globaali, Suomessa yli 3 700 asiantuntijaa työllistävä ICT-palveluyritys, joka konsultoi asiakkaitaan liiketoiminnan sekä ICT-ratkaisujen kehittämisessä ja on luotettu ulkoistuskumppani. CGI:n tavoitteena on toimialan laatujohtajuus toimittamalla palvelut ja projektit sovitun aikataulun ja budjetin mukaisesti.

cgi.fi