SANS SECURITY AWARENESS

Tietoturvaopas – Turvallinen työskentely kotona

Tiivistelmä

Koronavirus on saanut useat organisaatiot siirtämään henkilöstönsä työskentelemään kotoa käsin. Tämä voi olla haastavaa, sillä monilla organisaatioilla ei ole sovittuja käytäntöjä tai tarvittavaa teknologiaa ja koulutusta turvallisen etätyöskentelyn takaamiseen. Lisäksi monet työntekijät voivat kokea kotoa käsin työskentelyn vieraana tai epämukavana. Tämän oppaan tarkoitus on mahdollistaa kyseisten ihmisten nopea tietoturvakouluttaminen. Jos oppaan käytöstä herää kysyttävää, ottakaa meihin yhteyttä sähköpostitse osoitteeseen support@sans.org.

Koska henkilökuntanne elää tällä hetkellä todennäköisesti merkittävän stressin ja muutosten keskellä ja koska aika ja resurssit todennäköisesti rajoittavat organisaationne mahdollisuuksia, tämän strategisen oppaan on tarkoitus tehdä kouluttamisesta mahdollisimman yksinkertaista. Suosittelemme, että keskitytte vain alla kuvaamiimme suurimpiin riskeihin, joilla saattaa olla merkittävin vaikutus. Näitä voi pitää aloituspisteenä. Halutessanne voitte myös käsitellä muita riskejä tai aiheita. On hyvä pitää mielessä, että mitä enemmän toimintamalleja, käytäntöjä tai teknologioita henkilöstön on omaksuttava, sitä todennäköisemmin niitä kaikkia ei osata käyttää kunnolla.

Oppaan käyttöohje

Suosittelemme, että aloitatte lukemalla tämän oppaan ja käymällä läpi linkit eri materiaaleihin, jotta saatte käsityksen siitä, mitä kaikkea on tarjolla. Tulette huomaamaan, että tarjoamme jokaiselle riskille erilaisia materiaaleja, joita voitte hyödyntää henkilökunnan aktivoinnissa ja kouluttamisessa. Näin voitte valita ne moduulit, joiden uskotte olevan tehokkaimpia omat tarpeenne ja työkulttuurinne huomioiden. Kun olette lukeneet tämän asiakirjan, lukekaa mukana tullut viestintäpohja ja tietolehtinen, jotta saatte muodostettua tarkemman kuvan siitä, mihin olette pyrkimässä. Kun olette käyneet dokumentit läpi, teidän on koordinoitava kahden avainryhmän välillä.

1. **Tietoturvatiimi**: Tehkää yhteistyötä tietoturvatiimin kanssa, jotta saatte paremman käsityksen niistä riskeistä, joita yritätte hallita. Tässä oppaassa käymme läpi mielestämme suurimmat ja yleisimmät riskit, jotka kotoa käsin työskentelevä henkilökunta kohtaa, mutta teidän riskinne voivat erota niistä. Varoituksen sana: yleinen tietoturvatiimien tekemä virhe on pyrkiä hallitsemaan kaikkia riskejä ja sitä kautta hukuttaa ihmiset lukuisten käytäntöjen ja vaatimusten tulvaan. Yrittäkää rajoittaa käsittelemänne riskit mahdollisimman pieneen määrään. Kun olette tunnistaneet ja priorisoineet riskit, vahvistakaa käyttäytymismallit, jotka auttavat hallitsemaan niitä. Jos organisaatiollanne ei kuitenkaan ole aikaa tai resursseja tähän, hyödyntäkää alla olevaa tietoa.

2. **Viestintä**: Kun olette tunnistaneet suurimmat ihmislähtöiset riskit sekä tärkeimmät käyttäytymismallit niiden hallintaan, kouluttakaa henkilökuntanne noudattamaan näitä malleja yhteistyössä viestintäosastonne kanssa. Tehokkaimmissa tietoturvakoulutusohjelmissa tehdään tiivistä yhteistyötä viestintätiimien kanssa. Kannattaa selvittää, onko viestintäosastolta mahdollista kiinnittää joku osaksi tietoturvatiimiä. Kun kommunikoitte henkilökuntanne kanssa, tehokas aktivointikeino on painottaa, että koulutus auttaa työn suojelemisen lisäksi luomaan kyberturvallisen kodin, joka suojaa sekä työntekijöitä itseään että heidän perheitään.

Tavoite näiden kahden ryhmän kanssa työskentelyssä on tehdä tietoturvasta mahdollisimman yksinkertainen asia oppia ja motivoida henkilökuntaa. Nämä kaksi ovat avainroolissa, kun tarkoituksena on muuttaa toimintamalleja. Suosittelemme jopa luomaan neuvottelukunnan, joka koostuu sellaisista avainhenkilöistä, joiden palautetta tarvitsette ohjelman toteuttamiseen. Tietoturva- ja viestintäosastojenne lisäksi kannattaa harkita yhteistyötä henkilöstö- ja lakiosastojen kanssa.

Digitaalinen MGT433-latauspaketti

SANS Institutella on tarjolla kaksipäiväinen kurssi MGT433: Kuinka rakentaa, ylläpitää ja arvioida laajamittaista tietoturvatietoisuusohjelmaa. Tämä intensiivikurssi tarjoaa teorian, taidot, kehyksen ja resurssit, joita tarvitaan laajamittaisen tietoturvakoulutuksen järjestämiseen, minkä jälkeen pystytte tehokkaasti hallitsemaan ja arvioimaan ihmislähtöiset riskinne. Osana tätä opasta tarjoamme ilmaisen käyttöoikeuden kurssin digitaaliseen latauspakettiin, joka sisältää kurssin mallipohjat ja suunnitteluresurssit. Vaikka nämä materiaalit voivat olla ylimitoitettuja juuri tähän tilanteeseen, niistä voi olla hyötyä isoille organisaatioille tai mutkikkaammille käyttöönotto-ohjelmille.

Henkilökunnan kysymyksiin vastaaminen

Henkilökunnan tiedottamisen ja kouluttamisen lisäksi suosittelemme lämpimästi jonkinlaista teknologista ratkaisua tai foorumia, jossa voitte vastata ihmisten kysymyksiin mieluiten reaaliajassa. Tällaisia voivat olla asialle omistettu sähköpostiosoite, Skype- tai Slack-chat-kanava tai jokin verkkofoorumi, kuten Yammer. Yksi mahdollisuus on tietoturvaa käsittelevä verkkolähetys, joka toistetaan useita kertoja viikossa, jotta ihmiset voivat katsoa sen itselleen sopivana ajankohtana suorana ja jopa esittää kysymyksiä lähetyksessä. Tavoitteena on tehdä tietoturvasta mahdollisimman lähestyttävä ja auttaa ihmisiä, joilla on kysyttävää. Tämä on erinomainen tilaisuus aktivoida henkilökuntaa ja saada tietoturva näyttämään lähestyttävämmältä, joten tilaisuus kannattaa hyödyntää. Pitäkää mielessä, että jotta toiminta olisi mahdollisimman tehokasta, tietoturvakanavien valvomiseen ja kysymyksiin vastaamiseen on suositeltavaa kohdentaa resursseja.

Riskit ja koulutusmateriaalit

Olemme tunnistaneet kolme suurinta riskiä, joita tulee hallita etätyövoiman suojaamiseksi. Nämä ovat hyvä lähtöpiste, sillä näistä on todennäköisesti eniten hyötyä teille. Jokainen alla olevasta riskistä sisältää linkkejä useisiin resursseihin, jotka tekevät aiheen tiedottamisesta ja opettamisesta helpompaa. Tarjolla on useita viestintämateriaaleja, jotta voitte valita ne, jotka ovat käyttökelpoisimpia omassa työympäristössänne. Lisäksi lähes kaikki materiaalit ovat tarjolla useilla kielillä. Jos kaikki tämä tuntuu ylivoimaiselta ja aikanne on kortilla, suosittelemme hyödyntämään seuraavaa kahta materiaalia.

1. Turvallinen työskentely kotona -tietolehtinen (mukana paketissa).
2. Kodin kyberturvallisuus -video (englanti), saatavilla myös muilla kielillä täältä.

Manipulointihyökkäykset

Yksi suurimmista riskeistä etätyöntekijöille varsinkin tällaisina dramaattisten muutosten ja kiireellisten tilanteiden aikoina ovat manipulointihyökkäykset. Manipulointihyökkäykset ovat psykologisia hyökkäyksiä, joissa hyökkääjät huijaavat uhrinsa tekemään virheen, ja niiden toteuttaminen on entistä helpompaa muutoksen ja sekasorron aikana. Tärkeintä on kertoa ihmisille, mitä manipulointihyökkäykset ovat, kuinka tunnistaa manipulointihyökkäysten yleisimmät tunnusmerkit ja kuinka reagoida, kun hyökkäyksen merkkejä ilmenee. Muistakaa olla keskittymättä ainoastaan sähköpostin välityksellä tehtävään tietojen kalasteluun, sillä muita hyökkäyskeinoja ovat puhelut, tekstiviestit, sosiaalinen media ja valeuutiset. Manipulointihyökkäyksiä koskevaan koulutukseen tarvittavat materiaalit löytyvät kansiostamme Manipulointihyökkäysten tukimateriaalit. Lisäksi alla on kaksi SANS-tietoturvavideota, jotka voitte linkata ja jotka ovat myös saatavilla usealla kielellä.

- Manipulointihyökkäykset (englanti), saatavilla myös muilla kielillä täältä.
- Tietojen kalastelu (englanti), saatavilla myös muilla kielillä täältä.

Vahvat salasanat

Kuten Verizonin vuotuisessa DBIR-tietomurtotutkimusraportissa ilmenee, heikot salasanat ovat yhä yksi tietomurtojen pääasiallisista syistä globaalissa mittakaavassa. Alla on lueteltuna neljä tärkeintä toimintatapaa, joilla tätä riskiä voidaan hallita. Salasanoja koskevaa koulutusta ja näitä neljää toimintatapaa käsittelevät materiaalit löytyvät Salasanat-kansiostamme.

- Salasanalauseet (huomaa, että sekä salasanan monimutkaisuus että salasanan vanheneminen ovat vanhentuneita tietoturvakäsitteitä).
- Yksilölliset salasanat kaikilla tileillä.
- Salasananhallintaohjelmat.

- Monivaiheinen tunnistautuminen (tunnetaan myös kaksivaiheisena tunnistautumisena tai kaksivaiheisena todennuksena).

Päivitetyt järjestelmät

Kolmas riski ovat vanhentuneet ohjelmistot. Varmistakaa, että henkilökuntanne käyttävät aina käyttöjärjestelmien, ohjelmistojen ja mobiilisovellusten viimeisimpiä versioita. Henkilökohtaisia laitteita käyttäville henkilöille tämä voi tarkoittaa automaattisten päivitysten käyttöönottamista. Päivityksiä koskevaa koulutusta käsittelevät materiaalit löytyvät Haittaohjelmat tai Kodin kyberturvallisuus -kansioistamme.

Muita asiaan liittyviä aiheita

- **Wi-Fi**: Wi-Fi-tukiaseman suojaaminen. Tämä käsitellään Kodin kyberturvallisuus -materiaaleissa. Kannattaa myös harkita Kodin kyberturvallisuus (englanti) -videota, joka on saatavilla myös muilla kielillä täältä.

- **VPN:t**: Mikä on VPN ja miksi sellaista tulisi käyttää. Suosittelemme VPN:ää käsittelevää OUCH-uutiskirjettä.

- **Etätyöskentely**: Tämä on henkilöille, jotka tekevät työtä etänä mutta EIVÄT työskentele kotoa käsin, vaan esimerkiksi kahvilassa, lentokentän terminaalissa tai hotellissa. Kannattaa harkita Etätyöskentely (englanti) -koulutusvideotamme, joka on saatavilla myös muilla kielillä täältä.

- **Lapset/vieraat**: Vahvistaaksenne ajatusta, että perheenjäsenet/vieraat eivät saisi käyttää työhön liittyviä laitteita, kannattaa harkita Etätyöskentely (englanti) -koulutusvideotamme, joka on saatavilla myös muilla kielillä täältä.

- **Havaitseminen/reagointi**: Haluatteko, että ihmiset ilmoittavat, jos he uskovat tietoturvan vaarantuneen kotona työskentelyn aikana? Jos haluatte, niin mitä haluatte heidän ilmoittavan ja milloin? Tämä aihe käsitellään Hakkeroitu-materiaaleissamme.

OUCH-uutiskirjeet

Lisäksi kannattaa harkita julkisesti saatavilla olevia OUCH-uutiskirjeitä ohjelmanne tueksi. Uutiskirjeet on käännetty yli 20 kielelle. Alla on lueteltuna OUCH-uutiskirjeitä, joiden uskomme tukevan parhaiten Turvallinen työskentely kotona -aloitetta. Löydätte kaikki uutiskirjeet verkosta OUCH Security Awareness Newsletter Archives -arkistosta.

YLEISKATSAUS

Four Steps to Staying Secure (Neljä askelta suojautumiseen)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Kodin kyberturvallisuus)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

MANIPULOINTIHYÖKKÄYKSET

Social Engineering (Manipulointihyökkäykset)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Pikaviestit/tekstiviestihuijaukset)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Räätälöidyt huijaukset)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Pomohuijaus)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Puheluhyökkäykset/-huijaukset)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Estä tietojen kalastelu)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Huijaaminen sosiaalisessa mediassa)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

SALASANAT

Making Passwords Simple (Salasanoista yksinkertaisempia)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Suojaa kirjautumisesi)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

LISÄKSI

Yes, You Are a Target (Kyllä, sinä olet kohde)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Kodin älylaitteet)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Pikavinkit

Vihjeitä ja vinkkejä, joita voitte jakaa helposti sisäistettävässä muodossa.

- Tehokkain tapa suojata langaton verkko on muuttaa ylläpitäjän oletussalasana, ottaa käyttöön WPA2-salaus ja käyttää vahvaa salasanaa langattomassa verkossa.
- On syytä ottaa huomioon, mitkä kaikki laitteet muodostavat yhteyden kotiverkkoon, mukaan lukien itkuhälyttimet, pelikonsolit, televisiot, kodinkoneet ja jopa autot. Varmistakaa, että kaikki nuo laitteet ovat vahvojen salasanojen suojaamia ja/tai että käytätte laitteiden käyttöjärjestelmien uusimpia versioita.
- Yksi tehokkaimmista keinoista suojata tietokone kotona on pitää huolta, että sekä käyttöjärjestelmään että sovelluksiin on ladattu ja asennettu uusimmat korjaukset ja päivitykset. Kytkekää automaattiset päivitykset käyttöön mahdollisuuksien mukaan.
- Loppujen lopuksi terve järki on paras puolustuskeino. Jos sähköposti, puhelu tai verkkoviesti vaikuttaa oudolta, epäilyttävältä tai liian hyvältä ollakseen totta, se voi olla hyökkäys.
- Muistakaa käyttää vahvaa ja yksilöllistä salasanaa kullakin tilillä. Tuottaako kaikkien salasanojen muistaminen vaikeuksia? Kannattaa harkita salasananhallintaohjelman käyttöä salasanoista huolehtimiseen.
- Kaksivaiheinen tunnistautuminen on yksi parhaista keinoista suojata mikä tahansa tili. Kaksivaiheinen tunnistautuminen tarkoittaa sekä salasanan että mobiililaitteeseen lähetettävän tai mobiililaitteen luoman koodin käyttämistä. Esimerkkejä palveluista,

jotka tukevat kaksivaiheista tunnistautumista, ovat Gmail, Dropbox ja Twitter.

- Tietojen kalastelu tarkoittaa sitä, että hyökkääjä yrittää huijata uhrinsa napsauttamaan haittalinkkiä tai avaamaan sähköpostin liitetiedoston. Kannattaa epäillä kaikkia sähköposteja tai pikaviestejä, joissa luodaan kiireen tunnetta, joissa on kirjoitusvirheitä tai joissa vastaanottajaan viitataan muodossa "Hyvä asiakas".

Mittarit

Käyttäytymismallien mittaus on hankalaa tällaisessa tilanteessa, sillä ihmisten käyttäytymistä kotona on vaikea mitata. Lisäksi jotkin näistä käyttäytymismalleista eivät liity vain töihin (esimerkiksi Wi-Fi-laitteen suojaaminen). Voitte kuitenkin yhä mitata aktiivisuutta. Olemme huomanneet, että henkilökohtaiset tai tunteisiin vetoavat aiheet voivat aktivoida tehokkaasti ja saada paljon tavallista enemmän huomiota. Sen vuoksi seuraavat mittarit voivat olla hyödyllisiä.

- **Kanssakäyminen**: Kuinka usein ihmiset kysyvät kysymyksiä, julkaisevat ideoita tai pyytävät apua tarjoamienne tietoturvakanavien tai -foorumien kautta?
- **Simulaatiot**: Suorittakaa jonkinlaisia simuloituja manipulointihyökkäyksiä, esimerkiksi tietojen kalastelua, tekstiviestihyökkäyksiä tai puheluhyökkäyksiä.

Laajempi valikoima mittareita on tarjolla Security Awareness Metrics Matrixissa, joka löytyy digitaalisesta MGT433-latauspaketista.

Lisenssi

Toimeenpanopaketin kirjoittaja

Lance Spitznerillä on yli 20 vuoden tietoturvakokemus kyberuhkien tutkimisesta sekä tietoturvaa koskevasta arkkitehtuurista, tietoisuudesta ja koulutuksesta. Hän toimi kyberpetoksen ja kybertiedustelualan uranuurtajana luodessaan honeynet-verkostot ja perustaessaan Honeynet Projectin. SANS-kouluttajana hän on kehittänyt MGT433: Tietoturvatietoisuus ja MGT521: Tietoturvakulttuuri -kurssit. Lisäksi Lance on julkaissut kolme tietoturvakirjaa, konsultoinut yli 25 maassa ja auttanut yli 350 organisaatiota kehittämään tietoturvatietoisuuttaan ja -kulttuuriaan ihmislähtöisten riskien hallitsemiseksi. Lance järjestää tiuhaan luentoja, twiittaa taukomatta (@lspitzner) ja työskentelee lukuisten yhteisötietoturvaprojektien parissa. Ennen tietoturva-alaa Spitzner palveli panssarivaunu-upseerina Yhdysvaltain maavoimien valmiusjoukoissa ja ansaitsi MBA-tutkinnon Illnois'n yliopistosta.

Tietoa SANS Institutesta

SANS Institute perustettiin vuonna 1989 yhteistyötä tarjoavaksi tutkimus- ja koulutusorganisaatioksi. SANS on luotetuin ja ylivoimaisesti suurin maailmanlaajuisesti tietoturvakoulutusta ja -sertifiointia valtiojohdossa ja kaupallisissa organisaatioissa työskenteleville asiantuntijoille tarjoavista tahoista. Maineikkaat SANS-kouluttajat opettavat yli 60:tä kurssia yli 200:ssa paikan päällä tapahtuvassa kyberturvallisuustapahtumassa sekä myös verkossa. GIAC, SANS Instituten yhteistyökumppani, validoi ammatinharjoittajan pätevyyden hyödyntämällä yli 35:ttä teknistä käytännön sertifikaattia kyberturvallisuudesta. SANS Technology Institute, alueellisesti akkreditoitu itsenäinen tytäryhtiö, tarjoaa maisterin tutkintoon johtavaa kyberturvallisuuskoulutusta. SANS tarjoaa lukemattomia ilmaisia resursseja tietoturvayhteisölle, mukaan lukien konsensusprojekteja, tutkimusraportteja ja uutiskirjeitä. Se myös operoi internetin varhaisvaroitusjärjestelmää – Internet Storm Centeriä. SANSin ytimen muodostavat monet tietoturva-ammattilaiset, jotka edustavat lukuisia globaaleja organisaatioita yhtiöistä yliopistoihin ja työskentelevät yhdessä auttaakseen koko tietoturvayhteisöä. (https://www.sans.org)