SANS SECURITY AWARENESS

Útmutató a biztonságtudatossági intézkedések bevezetéséhez – A biztonságos otthoni munkavégzés

Vezetői összefoglaló

A koronavírus következtében számos szervezet állítja át munkavállalóit otthoni munkavégzésre. Ez esetenként kihívásokat jelenthet, mivel számos szervezet nem rendelkezik a távoli munkavégzéshez biztosításához szükséges szabályozással, technológiákkal és képzéssel. Emellett az alkalmazottak számára is ismeretlen vagy kényelmetlen lehet az otthoni munkavégzés fogalma. A jelen útmutató célja, hogy Ön képessé váljon az ilyen munkavállalók részére gyorsan megtanítani, hogyan dolgozhatnak a lehető legbiztonságosabban. Amennyiben kérdése merülne fel az útmutató használatával kapcsolatban, írjon nekünk a support@sans.org e-mail-címen.

Lévén a munkavállalók életében feltehetőleg rengeteg feszültség és változás lép fel jelenleg, és feltehetőleg a szervezet ideje és forrásai is korlátozottak, a jelen stratégiai útmutató arra fókuszál, hogy a képzést a lehető legegyszerűbbé tegye. Javasoljuk, hogy a legfontosabb kockázatokra összpontosítson, amelyeknek a legnagyobb hatása lehet. Ezeket alább ismertetjük. Tekintse ezeket kiindulópontként. Amennyiben ezeket további kockázatokkal vagy témakörökkel bővíteni szeretné, ne érezze akadályát. Azt azonban érdemes észben tartani, hogy minél több eljárásrendi, folyamatbeli vagy technológiai követelményt támaszt munkavállalóival szemben, annál kevésbé valószínű, hogy mindegyiket képesek lesznek megvalósítani.

Az útmutató használata

Első lépésként javasoljuk, hogy olvassa át az útmutatóban foglaltakat, valamint az egyéb anyagokra mutató megadott hivatkozásokat, hogy képbe kerüljön az elérhető információk és lehetőségek tekintetében. Mint azt látja majd, mindegyik kockázat esetében számos különböző anyagot biztosítunk, amelyek segítségével a szervezet munkavállalóit bevonhatja és képezheti. Így szabadon megválaszthatja azokat a módszereket, amelyek érzése szerint a leghatékonyabban használhatók a szervezet igényei és kultúrája ismeretében. Miután a jelen dokumentumot átolvasta, tanulmányozza át a csomagban foglalt kapcsolódó Kommunikációs sablont és Tájékoztatót, amelyek segítenek könnyebben megérteni az elérendő célokat. Miután a dokumentumokat áttekintette, két kulcsfontosságú csapattal érdemes egyeztetnie.

1. **Biztonsági csapat**: Biztonsági csapatával egyeztetve tárja fel, hogy milyen nagyobb kockázatokat érdemes kezelnie. Ebben az útmutatóban azonosítottuk, hogy szerintünk melyek az otthoni munkát érintő fontosabb, leggyakoribb kockázatok, az Ön kockázatai azonban eltérhetnek ezektől. Azonban hadd intsük óvatosságra! Gyakori probléma, hogy a biztonsági csapatok az összes kockázatot megpróbálják egyszerre kezelni, és így számos különböző szabályzattal és követelménnyel árasztják el az alkalmazottakat. Próbálja a célzott kockázatokat lehetőleg minimálisra szorítani. Miután azonosította és priorizálta a kockázatokat, fektesse le az azokat kezelő eljárásokat. Mint már említettük, ha a szervezet nem rendelkezik az ehhez szükséges idővel vagy forrásokkal, használhatja az alább dokumentáltakat.

2. **Kommunikációs csapat**: Miután azonosította a legfontosabb kockázatokat és az azok kezelését célzó fő eljárásokat, a kommunikációs csapat segítségével vonja be és képezze ki a munkavállalókat ezekre a eljárásokra. A leghatékonyabb biztonságtudatossági programok erősen támaszkodnak a biztonsági csapatra. Amennyiben lehetséges, a kommunikációs csapat valamelyik tagját involválja közvetlenül a biztonsági csapat munkájában. A munkavállalókkal való kommunikáció során hatékony módszer lehet a munkavállalók bevonására, ha hangsúlyozza, hogy a képzés nem csupán a munkavégzés biztonságának biztosítására alkalmas, hanem annak mentén képesek lehetnek kiberbiztonságos otthoni környezetet is kialakítani, ezáltal saját maguk és családjuk biztonságáról gondoskodva.

Végső soron ezzel a két csapattal együttműködve egyfelől a lehető legegyszerűbbé teheti a biztonságot a munkavállalók számára, másfelől motiválhatja is őket, ez pedig az eljárásokkal kapcsolatos szokások megváltoztatásának két alappillére. Javasoljuk, hogy adott esetben állítson fel Tanácsadó testületet a kulcsfontosságú érintettek részvételével, akiknek a véleménye és közreműködése szükséges a program bevezetéséhez. A biztonsági és a kommunikációs csapaton túl még a HR és a jogi osztállyal is szükséges egyeztetni és együttműködni.

MGT433 Digitális letöltéscsomag

A SANS Institute a kétnapos MGT433: Nagy hatékonyságú biztonságtudatossági program kialakítása, fenntartása és értékelése tanfolyamot kínálja. Ez az intenzív képzés teljes körűen biztosítja a nagy hatékonyságú biztonságtudatossági programok kialakításához szükséges elméleteket, képességeket, keretrendszert és forrásanyagokat, amelyek segítségével Ön hatékonyan kezelheti és értékelheti az emberi kockázatokat. Az útmutató részeként ingyenesen elérhetővé tesszük a tanfolyam sablonokat és tervezési forrásanyagokat tartalmazó Digitális letöltéscsomagját. Bár a jelen kezdeményezés igényeit valószínűleg messze meghaladják, az anyagok hasznosak lehetnek a nagyobb szervezetek és az összetettebb környezetek számára.

A munkavállalók kérdéseinek megválaszolása

A munkavállalókat érintő kommunikáció és képzés mellett kiemelten javasoljuk olyan technológia vagy fórum bevezetését, amelyen keresztül az érdeklődők kérdéseit lehetőleg valós időben meg lehet válaszolni. Ez lehet egy kifejezetten erre a célra szánt e-mail-cím, Skype vagy Slack csevegőcsatorna, esetleg valamilyen online fórum, például a Yammer. Másik lehetőség a biztonsági webközvetítés, amely a hét folyamán többször is megtekinthető, így mindenki kiválaszthatja a neki leginkább megfelelő időpontot, és élőben részt vehet az eseményen, sőt akár kérdéseket is feltehet. A cél, hogy a biztonságot a lehető legkézzelfoghatóbbá tegye, és segítsen a munkavállalóknak a felmerülő kérdéseik kapcsán. Ez egy fantasztikus lehetőség, hogy kapcsolatot teremtsen munkavállalóival, és a

biztonság kérdését barátságos formában közelítse meg. Próbáljon előnyt kovácsolni ebből. Azt azonban mindenképp tartsa szem előtt, hogy ez csak akkor működik hatékonyan, ha megfelelő erőforrásokat rendel a biztonsági csatornák moderálására, és aktívan válaszol a kérdésekre.

Kockázatok és tananyagok

Három alapvető kockázatot azonosítottunk, amelyeket a távolról dolgozó munkavállalók esetében kezelni érdemes. Ezek csak kiindulópontként szolgálnak, és ezek azok, amelyek valószínűleg a legnagyobb értéket képviselik az Ön számára. Az alábbi kockázatok mindegyikéhez több forrásra is hivatkoztunk, amelyek segíthetnek az adott témakörrel kapcsolatos kommunikációban és képzésben. Több kommunikációs anyagot is biztosítunk, így Ön kiválaszthatja azokat, amelyek a leghatékonyabban alkalmazhatók az Ön szervezeti kultúrájában. Az anyagok majd mindegyike több nyelven is elérhető. Amennyiben ez túl soknak tűnne, és az ideje rendkívül korlátozott, azt javasoljuk, hogy használja a két alábbi anyagot.

1. Tájékoztató: A biztonságos otthoni munkavégzés (a Bevezetési csomag tartalmazza).
2. A kiberbiztonságos otthon megteremtése (angol nyelven), amely itt más nyelveken is elérhető

Pszichológiai manipuláció

Az egyik legnagyobb kockázat, amely a távolról dolgozókat fenyegeti, különösen ebben a drámai változásoktól és sürgető légkörtől terhes időkben, a pszichológiai manipulációnak való kitettség. A pszichológiai manipuláció olyan pszichológiai támadás, amelynek során a támadó csalással ráveszi az áldozatot, hogy az hibázzon, ami az ilyen változó és zavart keltő helyzetekben még sokkal könnyebben megeshet. Kulcsfontosságú, hogy megtanítsa a munkavállalóknak, miben is áll a pszichológiai manipuláció, hogyan vehetők észre az ezen alapuló támadások gyakoribb ismertető jelei, és mi a teendő ezek észlelésekor. Fontos, hogy ne csak az e-mailes adathalász támadásokra fókuszáljon, hanem a többi módszerre is, úgymint a telefonhívások, a szöveges üzenetek, a közösségi oldalak és a hamis hírek használatára. A kapcsolódó képzéshez és a téma bevéséséhez szükséges forrásokat a Pszichológiai manipulációval kapcsolatos támogató anyagok mappában találja. Emellett használhatja az alábbi két SANS biztonságtudatossági videó hivatkozásait is, amelyek közül mindkettő több nyelven is elérhető.

- Pszichológiai manipuláció (angol nyelven), amely itt más nyelveken is elérhető
- Adathalászat (angol nyelven), amely itt más nyelveken is elérhető

Erős jelszavak

A Verizon éves adatbiztonsági jelentése (Verizon DBIR) szerint globálisan továbbra is a gyenge jelszavak jelentik az elsődleges veszélyt az adatbiztonság terén. Ez a kockázat az

alább felsorolt négy kulcsfontosságú eljárással kezelhető. A kapcsolódó képzéshez és a téma, valamint a négy kulcsfontosságú eljárás bevéséséhez szükséges forrásokat a Jelszavak mappában találja.

- Jelmondatok (vegye figyelembe, hogy a jelszavak összetettségén és a jelszavak gyakori cseréjén alapuló megközelítések egyaránt zsákutcának bizonyulnak).
- Egyedi jelszó használata minden fiókhoz
- Jelszókezelők
- Többtényezős hitelesítés (MFA). Egyéb néven Kéttényezős hitelesítés vagy Kétlépcsős azonosítás

Frissített rendszerek

A harmadik kockázat pedig arra vonatkozik, hogy gondoskodni kell róla, hogy a munkavállalók által használt technológiák az operációs rendszerek, alkalmazások és mobilalkalmazások legújabb verzióit futtassák. A magántulajdonú eszközök esetében ez azt jelentheti, hogy a felhasználónak engedélyeznie kell az automatikus frissítéseket. A kapcsolódó képzéshez és a téma bevéséséhez szükséges forrásokat a Kártékony szoftverek és A kiberbiztonságos otthon megteremtése mappákban találja.

További megfontolandó témakörök

- **Wi-Fi**: A Wi-Fi hozzáférési pont biztonságossá tétele. Ezt A kiberbiztonságos otthon megteremtése anyagok tárgyalják. Emellett érdemes megtekinteni A kiberbiztonságos otthon megteremtése (angol nyelven) videót, amely itt más nyelveken is elérhető.

- **VPN-ek**: Mi az a VPN, és miért érdemes használni? Figyelmébe ajánljuk a VPN-ekkel kapcsolatos OUCH-hírlevelet.

- **Távoli munkavégzés**: Ez azokra a munkavállalókra vonatkozik, akik távolról, de nem otthonról dolgoznak, például egy kávézóból, repülőtéri váróból vagy szállodából. Érdemes megfontolni a Távoli munkavégzés oktatóvideó (angol nyelven) használatát, amely itt más nyelveken is elérhető.

- **Gyerekek/vendégek**: Annak bevésése érdekében, hogy a munkavállalók ne engedjék családjuk/vendégeik számára a munkaeszközeik használatát, érdemes megfontolni a Távoli munkavégzés oktatóvideó (angol nyelven) használatát, amely itt más nyelveken is elérhető.

- **Észlelés/válasz**: Szeretné, ha a munkavállalók jeleznék, ha valamilyen incidens történt az otthoni munka során? Ha igen, mit és mikor szeretné, ha jelentenének? Ezt a Feltörés esetén anyagok tárgyalják.

OUCH-hírlevelek

Ezeken felül érdemes a program támogatására a nyilvánosan elérhető OUCH-hírleveleket is igénybe venni, amelyek több mint húsz nyelven elérhetők. Az alábbiakban felsoroljuk azokat az OUCH-hírleveleket, amelyek véleményünk szerint leginkább támogathatják Biztonságos otthoni munka iniciatívájá̀t. A hírleveleket online az OUCH biztonságtudatossági hírlevelek archívumában találja.

ÁTTEKINTÉS

Four Steps to Staying Secure (A biztonság megőrzésének négy lépése)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (A kiberbiztonságos otthon megteremtése)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

PSZICHOLÓGIAI MANIPULÁCIÓ

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

Messaging / Smishing (Üzenetküldés/SMS-en keresztüli adathalászat)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Személyre szabott csaló támadások)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Vállalatvezető nevében elkövetett csalás)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

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

Stop That Phish (Állj az adathalászatnak!)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (A közösségi oldalakon keresztül elkövetett csalás)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

JELSZAVAK

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

Lock Down Your Login (2FA) [A bejelentkezés biztonságosabbá tétele (kéttényezős hitelesítés)]
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

EGYÉB ANYAGOK

Yes, You Are a Target (Igen, Ön is célpont!)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

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

Gyorstippek

Tippek és trükkök, amelyeket könnyen fogyasztható formában megoszthat.

- A leghatékonyabb lépések, amelyekkel biztosíthatja az otthoni vezeték nélküli hálózat biztonságát: az alapértelmezett adminisztrátori jelszó megváltoztatása, a WPA2-titkosítás engedélyezése, valamint az erős jelszó használata a vezeték nélküli hálózaton.
- Legyen tisztában vele, hogy milyen eszközök használják az otthoni hálózatot, beleértve a babamonitorokat, a játékkonzolokat, a televíziókat, az egyéb készülékeket, sőt akár az autóját is. Gondoskodjon róla, hogy ezek az eszközök erős jelszóval védettek, és/vagy operációs rendszereik legfrissebb verzióit futtatják.
- Az egyik leghatékonyabb módszer, amellyel otthoni számítógépét védheti, ha gondoskodik róla, hogy az operációs rendszer és az alkalmazások frissítései és javítócsomagjai telepítve legyenek. Ha módja van rá, kapcsolja be az automatikus frissítéseket.
- Végső soron a legjobb védelem, ha követi, amit a józan ész diktál. Ha egy email, üzenet vagy telefonhívás gyanús, vagy túl szép, hogy igaz legyen, támadásról lehet szó.
- Minden fiókján használjon külön, egyedi jelszót. Nem tud minden jelszót/jelmondatot fejben tartani? Fontolja meg egy jelszókezelő használatát, amelyben mindegyiket

biztonságosan eltárolhatja.

- A kétlépcsős azonosítás az egyik legjobb módszer, amellyel védheti fiókját. A kétlépcsős azonosítás egy jelszót, valamint egy, a mobileszközére küldött vagy az eszköz által generált kódot használ. A kéttényezős azonosítást használó szolgáltatások például a Gmail, a Dropbox és a Twitter.
- Az adathalászat olyan támadás, amelynek során a támadó megpróbálja rávenni, hogy egy kártékony hivatkozásra kattintson vagy megnyisson egy mellékletet egy e-mailben. Minden olyan e-mail vagy online üzenet esetében érdemes gyanút fogni, amely sürgető, rossz a helyesírása, vagy a „Kedves ügyfelünk” általános megszólítást tartalmazza.

Mutatók

Az eljárásokra vonatkozó mutatók ebben a helyzetben nehezebben állíthatók elő, mivel nehezebben mérhető, hogy az emberek otthon milyen eljárásokat alkalmaznak. Emellett ezeknek az eljárásoknak némelyike nem csak a munkavégzést érinti (például a Wi-Fi-eszköz védelme). A bevonódás azonban mérhető. Tapasztalataink szerint az ilyen személyes vagy érzelmi témák képesek jól bevonni az embereket, és más témáknál sokkal nagyobb érdeklődésre tartanak számot. Íly módon az ilyen mutatók értékesek lehetnek.

- **Interakció**: Milyen gyakran tesznek fel az emberek kérdéseket, tesznek közzé ötleteket vagy kérnek segítséget az üzemeltetett biztonsági csatornákon vagy fórumokon?
- **Szimulációk**: Hajtson végre valamilyen jellegű pszichológiai manipulációra, például adathalászatra, szöveges üzeneten vagy telefonhíváson alapuló támadásokra vonatkozó szimulációkat.

A mutatók átfogóbb listájáért töltse le az interaktív Biztonságtudatossági mutatók mátrixa anyagot az MGT433 Digitális letöltéscsomagból.

Licenc

A bevezetési csomag szerzője

Lance Spitzner több mint 20 év biztonsági gyakorlattal rendelkezik a kiberfenyegetések elleni kutatások, a biztonsági architektúrák, a biztonságtudatosság és a biztonsági képzések terén. A Honeynet Project megalapításával és kapcsolódó hálózatok létrehozásával úttörő szerepet játszott a megtévesztés elleni és kibernetikus elhárítás területén. A SANS instruktoraként ő dolgozta ki az MGT433: Biztonságtudatosság és az MGT521: Biztonsági kultúra tanfolyamokat. Emellett Lance a biztonság témakörében három könyvet is kiadott, több mint 25 országban folytatott tanácsadói tevékenységet, és több mint 350 szervezetben segített kiépíteni a biztonságtudatossággal és a biztonsági kultúrával kapcsolatos programokat az emberi kockázat kezelésére. Lance gyakorlott előadó, aktív Twitter-felhasználó (@lspitzner) és számos közösségi biztonsági projekten dolgozik. Mielőtt az információbiztonság területére tévedt volna, Lance páncélos tisztként szolgált a hadsereg gyors bevetésű alakulatánál, és mesterdiplomát szerzett az Illinois Egyetemen.

A SANS Institute

A SANS Institute 1989-ben alakult kooperatív kutató és oktató szervezetként. A SANS a legmegbízhatóbb és legnagyobb szolgáltató a kiberbiztonsági képzések és tanúsítás terén a kormányzati és piaci szervezetek részére világszerte. A SANS elismert instruktorai több mint 60 különböző tanfolyamot tartanak több mint 200 élő kiberbiztonsági képzési esemény keretében, valamint online. A GIAC, a SANS Institute partnere a szakemberek minősítését több mint 35 gyakorlati és technikai kiberbiztonsági tanúsítvány alkalmazásával hitelesíti. A SANS regionálisan akkreditált független leányvállalata, a SANS Technology Institute mesterkurzusokat kínál a kiberbiztonság területén. A SANS ingyenes forrásanyagok széles tárházát kínálja az információs biztonsági közösség számára, többek közt konszenzusos projekteket, kutatási jelentéseket és hírleveleket, valamint az internet korai jelző rendszerével, az Internet Storm Centerrel is együttműködik. A SANS gárdájának szívét az a rengeteg biztonsági szakember adja, akik a különféle globális szervezetek, vállalatok és egyetemek képviseletében együttműködnek a teljes információbiztonsági közösség támogatása érdekében. (https://www.sans.org)