SANS SECURITY AWARENESS

Návod k distribuci školení o zabezpečení – Bezpečná práce z domova

Stručný souhrn

Kvůli koronaviru jsou mnohé organizace nuceny přejít na podporu práce z domova. Může to být náročné, jelikož řada organizací nemá pravidla, technologie a školení, které by jim zabezpečily vzdálené pracoviště. Spousta zaměstnanců navíc nemusí mít s prací z domova zkušenosti nebo se jim ta myšlenka nemusí zamlouvat. Účelem tohoto návodu je umožnit vám tyto lidi rychle vyškolit a zajistit jim tak co možná největší bezpečí. Pokud máte ohledně tohoto návodu nějaké dotazy, dejte nám vědět na support@sans.org.

Jelikož vaši pracovníci jsou nejspíš pod velkým stresem a musí řešit řadu změn a vaše organizace nejspíš nemá potřebný čas a zdroje, soustředí se tento strategický návod na to, aby bylo školení co možná nejjednodušší. Doporučujeme vám zaměřit se pouze na ta nejdůležitější rizika, která budou mít největší dopad, jak popisujeme níže. Berte to jako výchozí bod. Pokud jsou zde nějaká další rizika či témata, která chcete přidat, rozhodně to udělejte. Akorát je třeba si uvědomit, že čím víc pravidel, procesů a technologií po svých pracovnících budete vyžadovat, tím je nižší šance, že je budete moct uplatnit všechny.

Jak používat tento návod

Doporučujeme vám začít tím, že si přečtete materiály v tomto návodu a podíváte se na odkazy na různé materiály, abyste měli představu o tom, jaké možnosti jsou dostupné. Uvidíte, že pro každé riziko poskytujeme různé materiály, které můžete použít ke školení ve své organizaci. Díky tomu si budete moct vybrat způsoby, které budou podle vás nejefektivnější vzhledem k vašim potřebám a kultuře. Až si přečtete tento dokument, přečtěte si doprovodnou Komunikační šablonu a Základní přehled, které jsou součástí této sady, abyste lépe pochopili, o co máte usilovat. Až si tuto dokumentaci přečtete, budete se muset zkoordinovat se dvěma klíčovými skupinami.

1. **Bezpečnostní tým**: Zkoordinujte se se svým bezpečnostním týmem, abyste měli lepší představu o tom, jaké klíčové nástrahy se pokoušíte zvládnout. V tomto návodu jsme uvedli rizika, která jsou podle nás pro lidi pracující z domova nejdůležitější a nejčastější, ale situace u vás se může lišit. Pozor: Jednou z běžných chyb, kterých se bezpečnostní týmy dopouštějí, je to, že se snaží zvládnout všechna rizika a zahltí lidi řadou pravidel a požadavků. Pokuste se omezit množství rizik, která budete řešit, na nutné minimum. Jakmile tato rizika určíte a upřednostníte, stanovte pravidla, která budou tato rizika řešit. Jak už jsme psali, pokud na to vaše organizace nemá dost času ani zdrojů, pak využijte to, co píšeme níže.

2. **Komunikační tým**: Jakmile určíte nejvyšší lidská rizika a klíčová pravidla k jejich zvládnutí, spojte se s komunikačním týmem a dejte svým pracovníkům o těchto pravidlech školení. Ty nejefektivnější programy bezpečnostního školení využívají silné vztahy s komunikačním týmem. Pokud je to možné, zjistěte, jestli můžete někoho z komunikačního týmu přeřadit do bezpečnostního týmu. V rámci komunikace těchto pravidel vašim pracovníkům se vyplatí zmínit, že toto školení jim pomůže nejen posílit zabezpečení v práci, ale umožní jim vytvořit kyber-zabezpečený domov, díky čemuž ochrání sami sebe i svou rodinu.

Spolupráce s těmito dvěma skupinami vám nakonec pomůže zajistit, že zabezpečení bude pro vaše pracovníky co možná nejjednodušší, a zároveň budete svoje pracovníky motivovat. To jsou dva klíčové prvky pro změnu chování. Doporučujeme vytvořit poradní fórum s klíčovými lidmi, jejichž zpětná vazba a komentáře vám pomůžou toto školení zavést. Kromě vašeho bezpečnostního a komunikačního týmu se můžete spojit například s oddělením lidských zdrojů a s právním oddělením.

Digitální stažitelný balíček MGT433

SANS Institute poskytuje dvoudenní školení MGT433: Jak vybudovat, udržovat a vyhodnocovat důležité školení o zabezpečení. Tento intenzivní kurz poskytuje veškerou teorii, schopnosti, rámec a zdroje k tomu, abyste mohli sestavit důležité školení, které vám umožní efektivně zvládnout a vyhodnotit lidské riziko. V rámci tohoto návodu poskytujeme bezplatný přístup k digitálnímu stažitelnému balíčku pro tento kurz, který obsahuje šablony a plánovací materiály. Ačkoliv jsou tyto materiály obsáhlejší než potřeby této iniciativy, mohou být cenné pro větší organizace či komplexnější situace.

Reagování na dotazy od pracovníků

Kromě komunikace s vašimi pracovníky a jejich školení důrazně doporučujeme nějaký typ technologie či fórum, kde můžete odpovídat lidem na otázky, pokud možno v reálném čase. Sem může patřit vyhrazený e-mail, Skype či chatovací kanál na Slacku nebo nějaký jiný druh online fóra, např. Yammer. Další možností je uspořádat bezpečnostní webcast, který můžete opakovat několikrát do týdne, aby si lidi mohli vybrat čas, který jim nejvíc vyhovuje, a sledovat ho živě a třeba i pokládat dotazy. Cílem je zpřístupnit zabezpečení co možná nejvíc a pomáhat lidem, kteří mají otázky. Je to úžasná příležitost zapojit své pracovníky a představit zabezpečení s lidskou tváří. Pokuste se této příležitosti využít. Pamatujte, že aby to všechno bylo efektivní, měli byste vyhradit někoho, kdo bude bezpečnostní kanály moderovat a bude aktivně odpovídat na dotazy.

Rizika a školicí materiály

Určili jsme tři základní rizika, která musíte zvládnout při práci z domova. Ta představují počáteční bod a nejspíše pro vás budou i nejcennější. Každé níže uvedené riziko obsahuje odkazy na řadu zdrojů, které vám pomohou toto téma probrat a školit. Poskytujeme řadu komunikačních materiálů, abyste si mohli vybrat ty, které budou mít největší dopad na vaši kulturu. Téměř všechny materiály jsou navíc přeložené do více jazyků. Pokud je toho všeho moc a vy máte extrémně málo času, pak vám doporučujeme projít si ty dva materiály uvedené níže.

1. Bezpečná práce z domova (je součástí zaváděcí sady).
2. Video Vytvoření kyber bezpečného domova (v angličtině), rovněž dostupné v dalších jazycích zde

Sociální inženýrství

Jedním z největších rizik, kterým budou lidé pracující na dálku čelit, zejména v této době dramatických změn a naléhavosti, jsou útoky využívající sociálního inženýrství. Sociální inženýrství je psychologický útok, kdy útočníci oklamou či napálí své oběti a přimějí je udělat chybu, což budou mít v této době změn a zmatků o to snazší. Klíčem je školení lidí o tom, co to je sociální inženýrství, jak odhalit nejčastější příznaky sociálního inženýrství a co dělat, pokud je lidé odhalí. Je důležité, abyste se nesoustředili jen na phishingové e-maily, ale i na další metody, mezi které patří telefonáty, textové zprávy, sociální sítě či fake news. Materiály potřebné ke školení ohledně tohoto tématu najdete v naší složce Podpůrné materiály k sociálnímu inženýrství. Zde jsou navíc dvě videa s bezpečnostním školením od SANS, na která můžete šířit odkaz – opět jsou dostupná ve více jazycích.

- Sociální inženýrství (v angličtině), rovněž dostupné v dalších jazycích zde
- Phishing (v angličtině), rovněž dostupné v dalších jazycích zde

Silná hesla

Jak jsme stanovili v rámci každoročního Verizon DBIR, slabá hesla představují hlavní slabinu v celosvětovém měřítku. Níže jsou čtyři klíčová pravidla, která vám pomohou toto riziko zvládnout. Materiály potřebné ke školení ohledně tohoto tématu a těchto čtyř pravidel najdete ve složce Hesla.

- Heslové fráze (poznámka: složitá hesla a obměna hesel už nestačí).
- Jedinečná hesla pro všechny účty
- Správci hesel
- Vícefaktorové ověření (MFA). Často uváděné jako dvoufaktorové ověření či ověření ve dvou krocích

Aktualizované systémy

Třetí riziko spočívá v zajištění toho, aby technologie, kterou vaši pracovníci používají, obsahovala nejnovější verzi operačního systému, aplikací a mobilních aplikací. Pokud lidi používají osobní zařízení, možná budou muset povolit automatické aktualizace. Materiály, které potřebujete ke školení ohledně tohoto tématu, najdete ve složkách Malware nebo Vytvoření kyber bezpečného domova.

Další témata ke zvážení

- **Wi-Fi**: Zabezpečení přístupového bodu Wi-Fi. Tohle probíráme v materiálech Vytvoření kyber bezpečného domova. Rovněž prosím uvažte toto video o Vytvoření kyber bezpečného domova (v angličtině), rovněž dostupné v dalších jazycích zde.

- **VPN**: Co je VPN a proč byste ji měli používat. Doporučujeme newsletter OUCH o VPN.

- **Práce na dálku**: Tohle je pro jedince, kteří pracují na dálku, ale NEPRACUJÍ z domova – například z kavárny, z terminálu na letišti nebo z hotelu. Zvažte použití našeho školicího videa Práce na dálku (v angličtině), rovněž dostupné v dalších jazycích zde.

- **Děti / Hosté**: Abyste rozšířili myšlenku, že rodina / hosté by neměli mít přístup k pracovním zařízením, zvažte použití školicího videa Práce na dálku (v angličtině), rovněž dostupné v dalších jazycích zde.

- **Odhalení / Reakce**: Chcete, aby vám lidi hlásili, pokud se domnívají, že došlo během práce z domova k nějakému incidentu? Pokud ano, co a kdy vám mají hlásit? Tohle probíráme v materiálech Napadení.

Newslettery OUCH

Navíc zvažte používání veřejně dostupných newsletterů OUCH, které mohou vaše školení podpořit. Každý newsletter byl přeložen do více než dvaceti jazyků. Níže najdete newslettery OUCH, které vám podle nás mohou nejlépe pomoct s iniciativou Bezpečná práce z domova. Všechny newslettery můžete najít v online archivech bezpečnostního školení OUCH.

PŘEHLED

Four Steps to Staying Secure (Čtyři kroky pro zabezpečení)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Vytvoření kyber bezpečného domova)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

SOCIÁLNÍ INŽENÝRSTVÍ

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

Messaging / Smishing (Zprávy / Textové zprávy)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Podvody šité na míru)
https://www.sans.org/security-awareness-training/resources/personalized-scams

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

Phone Call Attacks / Scams (Útoky přes telefon / Podvody)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

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

Scamming You Through Social Media (Podvody přes sociální sítě)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

HESLA

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

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

DALŠÍ

Yes, You Are a Target (Ano, i vy jste cíl)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

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

Rychlé tipy

Tipy a triky, které můžete sdílet, ve snadno přístupném formátu.

- Mezi nejefektivnější kroky, jak zabezpečit svou domácí bezdrátovou síť, je změna výchozího administrátorského hesla, povolení šifrování WPA2 a používání silného hesla k bezdrátové síti.
- Dávejte pozor na všechna zařízení, která se připojují k vaší domácí sítí, včetně chůviček, herních konzolí, televizí, přístrojů i vašeho auta. Postarejte se, aby všechna tato zařízení byla chráněná silným heslem a aby používala nejnovější verzi operačního systému.
- Jedním z nejefektivnějších způsobů, jak ochránit domácí počítač, je zkontrolovat si, jestli jsou operační systém a všechny vaše aplikace aktualizované a aktuální. Povolte automatické aktualizace, kdykoliv je to možné.
- Tou nejlepší ochranou je nakonec zdravý rozum. Pokud vám nějaký e-mail, telefonát či online zpráva přijdou divné, podezřelé nebo až příliš výhodné, může jít o útok.
- Pro každý svůj účet používejte silné a jedinečné heslo. Nepamatujete si všechna svoje hesla / heslové fráze? Zvažte použití správce hesel, který bude všechna hesla bezpečně ukládat za vás.
- Dvoufázové ověření je jedním z nejlepších kroků, kterými můžete zabezpečit jakýkoliv účet. Dvoufázové ověření znamená, že potřebujete nejen heslo, ale i zaslaný či vygenerovaný kód na vašem mobilním zařízení. Mezi služby, které podporují

dvoufázové ověření, patří Gmail, Dropbox a Twitter.

- Phishing znamená, když se vás útočník pokouší oklamat, abyste klikli na škodlivý odkaz nebo otevřeli přílohu v e-mailu. Dávejte pozor na jakýkoli e-mail či online zprávu, která vytváří pocit naléhavosti, jsou v ní pravopisné chyby nebo vás oslovuje "Vážený zákazníku".

Kontrola

Kontrola chování je v této situaci složitá, neboť je těžší sledovat, jak se lidi chovají doma. Některá z těchto pravidel navíc nejsou specifická pro práci (např. zajištění zabezpečení Wi-Fi). Můžete však sledovat zapojení lidí. Zjistili jsme, že osobní či emocionální témata, jako jsou tato, mohou být velmi zajímavá a mohou přitahovat větší zájem než jiná témata. Taková kontrola proto může být cenná.

- **Interakce**: Jak často lidé pokládají dotazy, zveřejňují nápady nebo žádají pomoc na některém z bezpečnostních kanálů či fór, která organizujete?
- **Simulace**: Provádějte nějaký druh simulací sociálního inženýrství, jako jsou třeba útoky přes phishing, textové zprávy či telefonáty.

Pokud chcete mnohem komplexnější seznam kontrol, stáhněte si interaktivní Matici kontroly bezpečnostního školení z Digitálního stažitelného balíčku MGT433.

Licence

Autor zaváděcí sady

Lance Spitzner máš přes 20 let zkušeností se zabezpečením na poli výzkumu kyber hrozeb, bezpečnostní architektury a školení. Pomáhal rozvíjet obor kyber rozvědky díky svému výtvoru honeynets a založení Honeynet Project. Jakožto instruktor SANS vyvinul kurzy MGT433: Bezpečnostní školení a MGT521: Bezpečnostní kultura. Lance navíc vydal tři knihy o zabezpečení, dělal konzultanta ve více než 25 zemích a pomohl více než 350 organizacím vybudovat bezpečnostní školení a kulturní programy pro zvládnutí lidského rizika. Lance je častý přednášející a tweeter (@lspitzner) a pracuje na celé řadě komunitních bezpečnostních projektů. Před informačním zabezpečením sloužil pan Spitzner jako důstojník v armádním Útvaru rychlého nasazení a získal MBA na univerzitě v Illinois.

O SANS Institute

SANS Institute byl založen v roce 1989 jako kooperativní výzkumná a vzdělávací organizace. SANS je nejdůvěryhodnější a zdaleka největší poskytovatel školení o kyber zabezpečení a certifikace pro profesionály ve vládních a komerčních institucích po celém světě. Renomovaní instruktoři SANS vyučují přes 60 různých kurzů v rámci více než 200 živých školení o kyber zabezpečení i online. GIAC, pobočka SANS Institute, ověřuje kvalifikaci praktikantů pomocí více než 35 praktických, technických certifikátů v oboru kyber zabezpečení. SANS Technology Institute, regionálně akreditovaná nezávislá pobočka, nabízí magisterské tituly v oboru kyber zabezpečení. SANS nabízí celou řadu bezplatných zdrojů komunitě InfoSec včetně konsensuálních projektů, výzkumných reportů a newsletterů. Rovněž provozuje internetový systém včasného varování – Internet Storm Center. V srdci SANS se nachází řada bezpečnostních praktikantů, kteří zastupují rozmanité globální organizace od korporací po univerzity, a spolupracují, aby pomohli celé komunitě kolem informačního zabezpečení. (https://www.sans.org)