SANS SECURITY AWARENESS

Implementatiehandleiding Security Awareness - Veilig van thuis uit werken

Samenvatting

Door het coronavirus laten veel organisaties hun medewerkers momenteel van thuis uit werken. Dat kan een hele uitdaging zijn. Veel organisaties beschikken immers niet over het beleid, de technologie en de training om de veiligheid hierbij te garanderen. Daarnaast voelt van thuis uit werken voor veel medewerkers misschien niet vertrouwd of prettig aan. Deze handleiding helpt u dan ook om deze mensen snel zo veilig mogelijk te leren werken. Hebt u vragen over het gebruik van deze handleiding? Neem dan contact met ons op via support@sans.org.

Uw personeel krijgt momenteel wellicht heel wat stress en veranderingen te verwerken. Bovendien zijn uw tijd en middelen wellicht beperkt. Daarom is deze handleiding erop gericht de training zo eenvoudig mogelijk te houden. We raden aan om u te focussen op de belangrijkste risico's met de grootste gevolgen, die we hieronder beschrijven. Die kunt u als de basis beschouwen. U kunt zeker ook andere risico's of onderwerpen aankaarten. Houd er echter rekening mee dat de medewerkers minder verwerkt krijgen naarmate u meer gedragsinstructies, processen en technologieën toevoegt.

Zo gebruikt u deze handleiding

We raden aan om de informatie in deze handleiding eerst door te nemen en de verschillende links te bekijken, om een goed beeld te hebben van de mogelijkheden. U zult merken dat we voor ieder risico uiteenlopend materiaal verstrekken dat u kunt gebruiken om uw organisatie te motiveren en te trainen. Zo kunt u de keuzes maken waarvan u denkt dat ze het beste aansluiten bij uw behoeften en cultuur. Lees na dit document ook de Communicatietemplate en de Factsheet in deze kit. Die geven duidelijk aan wat u probeert te bereiken. Als u de documentatie hebt bekeken, zijn er twee belangrijke groepen waarmee u moet coördineren.

1. **Het beveiligingsteam**: coördineer met uw beveiligingsteam om een beter beeld te krijgen van de belangrijkste risico's die u probeert te beheersen. Wij hebben in deze handleiding aangegeven wat volgens ons de belangrijkste en courantste risico's zijn voor thuiswerkend personeel, maar uw risico's kunnen afwijken. Let wel op: een veel gemaakte fout is dat beveiligingsteams proberen om alle risico's te beheersen en de medewerkers daardoor overspoelen met regels en vereisten. Probeer het aantal risico's dat u wilt beheersen, zo klein mogelijk te houden. Wanneer u de risico’s en prioriteiten hebt bepaald, identificeert u welk gedrag die risico's beheersbaar houdt. Zoals eerder vermeld: als uw organisatie hiervoor de tijd of middelen niet heeft, kunt u focussen op wat we hieronder vermelden.

2. **Het communicatieteam**: zodra u de belangrijkste risico's hebt geïdentificeerd en het gedrag hebt bepaald om ze te beheersen, werkt u samen met uw communicatieafdeling om uw personeel te motiveren en te trainen. In de doeltreffendste beveiligingsbewustzijnsprogramma's is er een hechte samenwerking met het communicatieteam. Kijk eventueel of u iemand van het communicatieteam in uw beveiligingsteam kunt opnemen. Wanneer u communiceert met uw personeel, is het een doeltreffende motivatiemethode om te benadrukken dat de training hen niet alleen op het werk beveiligt. Ze kunnen zo immers ook de cyberbeveiliging van hun woning verzekeren en zichzelf en hun familie beschermen.

Door met deze twee groepen samen te werken probeert u beveiliging zo eenvoudig mogelijk te maken en uw personeel te motiveren: twee essentiële elementen voor gedragsverandering. We stellen zelfs voor om een adviesraad op te zetten met personen van wie u feedback en input nodig hebt om het programma uit te rollen. Naast uw beveiligings- en communicatieteam kunt u overwegen om samen te werken en te coördineren met andere afdelingen, zoals Personeelszaken en de juridische afdeling.

MGT433 Digitaal downloadpakket

SANS Institute biedt de 2-daagse cursus MGT433: Zo creëert, onderhoudt en meet u een doeltreffend beveiligingsbewustzijnsprogramma. Deze intensieve cursus bevat alle theorie, vaardigheden, kaders en middelen om een succesvol bewustzijnsprogramma te creëren waarmee u uw menselijke risico's doeltreffend kunt managen en meten. Als onderdeel van deze handleiding geven we u gratis toegang tot het Digitale downloadpakket van deze cursus, met templates en planningsmateriaal. Hoewel dit waarschijnlijk de behoefte van dit initiatief ver overschrijdt, kan dit materiaal toch waardevol zijn voor grotere organisaties of complexere projecten.

Vragen van medewerkers beantwoorden

Naast communicatie en training raden we technologie of een forum aan om vragen van uw medewerkers te beantwoorden, bij voorkeur in real time. Dat kan via een specifiek e-mailadres, een Skype- of Slack-chatkanaal of een onlineforum zoals Yammer. Een ander idee is een livestream over beveiliging die u gedurende de week enkele keren herhaalt, zodat mensen zelf kunnen bepalen wanneer ze hem live bijwonen en mogelijk zelfs vragen kunnen stellen. Het doel is dat u beveiliging zo laagdrempelig mogelijk maakt en mensen helpt met hun vragen. Dit is een uitgelezen kans om uw personeel te motiveren en beveiliging in een vriendelijker daglicht te zetten. Maak er dus gebruik van. Houd er rekening mee dat voor een doeltreffend verloop iemand de veiligheidskanalen moet modereren en actief vragen beantwoorden.

Risico's en trainingsmateriaal

We hebben drie kernrisico's geïdentificeerd die belangrijk zijn voor thuiswerkend personeel. Ze vormen de basis en zijn waarschijnlijk de risico's die voor u het waardevolst zijn. Bij ieder risico hieronder vindt u links naar materialen voor de communicatie en de training. We bieden meerdere communicatiematerialen aan, zodat u zelf kunt bepalen wat de grootste impact zal hebben in uw bedrijfscultuur. Daarnaast zijn bijna alle materialen beschikbaar in meerdere talen. Als dit allemaal wat overweldigend is en u weinig tijd hebt, dan raden we u aan om de twee materialen hieronder te gebruiken.

1. Factsheet Veilig werken van thuis uit (onderdeel van uw implementatiekit).
2. Video cyberbeveiliging thuis (Engels) ook beschikbaar in andere talen

Social engineering

Een van de grootste risico's voor thuiswerkers, vooral in deze tijd vol ingrijpende veranderingen en een sfeer van urgentie, zijn social-engineeringaanvallen. Social engineering is een psychologische aanval waarbij aanvallers hun slachtoffers misleiden om een fout te maken, wat een stuk eenvoudiger is in tijden vol verandering en verwarring. Het belangrijkste is om mensen te leren wat social engineering is, hoe ze de meest voorkomende aanwijzingen kunnen herkennen en wat ze dan moeten doen. Zorg ervoor dat u niet alleen phishingmails focust. Andere methodes zijn onder andere telefoontjes, sms'en, sociale media of nepnieuws. U vindt de trainingsmaterialen voor dit onderwerp in onze map Ondersteuningsmateriaal Social Engineering. Daarnaast zijn hier twee SANS Security Awareness-video's waarnaar u kunt linken. Ze zijn opnieuw beschikbaar in meerdere talen.

- Social Engineering (Engels) ook beschikbaar in andere talen
- Phishing (Engels) ook beschikbaar in andere talen

Sterke wachtwoorden

Zoals vermeld in de jaarlijkse Verizon DBIR, blijven zwakke wachtwoorden een van de voornaamste wereldwijde oorzaken van inbraken. Hieronder staan vier belangrijke tips om dit risico te helpen beheersen. U vindt de trainingsmaterialen voor dit onderwerp en deze vier gedragsaspecten in onze map Wachtwoorden.

- Wachtwoordzinnen (opmerking: zowel wachtwoordcomplexiteit als wachtwoordverloop zijn niet langer actief).
- Unieke wachtwoorden voor alle accounts
- Wachtwoordmanagers
- Multifactorverificatie. Vaak ook tweefactorauthenticatie of tweestapsverificatie genoemd

Bijgewerkte systemen

Een derde element is zorgen dat de technologie die uw personeel gebruikt, bijgewerkt is naar de nieuwste versies van het besturingssysteem, de programma's en de mobiele apps. Voor mensen die persoonlijke apparaten gebruiken, kan dit betekenen dat ze automatisch updaten moeten inschakelen. U vindt de trainingsmaterialen voor dit onderwerp in onze map Malware of Cyberbeveiliging thuis.

Andere mogelijke onderwerpen

- **Wifi**: Uw wifinetwerk beveiligen. Dit wordt behandeld in het materiaal van Cyberbeveiliging thuis. Bekijk ook deze video over Cyberbeveiliging thuis (Engels) ook beschikbaar in andere talen.
- **VPN's**: Wat is een VPN en waarom moet u dit gebruiken? Wij raden u de OUCH-nieuwsbrief over VPN's aan.
- **Telewerken**: Dit is bedoeld voor personen die telewerken, maar NIET thuiswerken (bijvoorbeeld mensen die werken vanuit een café, het vliegveld of een hotel). Overweeg hiervoor onze Trainingsvideo telewerken (Engels) ook beschikbaar in andere talen.
- **Kinderen/gasten**: Om te benadrukken hoe belangrijk het is dat familie/gasten geen toegang mogen hebben tot werkapparatuur, kunt u onze Trainingsvideo telewerken (Engels) ook beschikbaar in andere talen overwegen.
- **Detectie/reactie**: Wilt u dat medewerkers vermoedelijke incidenten melden terwijl ze thuiswerken? En zo ja, wat wilt u dat ze melden en wanneer? Dit wordt behandeld in ons Gehackt-materiaal.

OUCH-nieuwsbrieven

Overweeg daarnaast om gebruik te maken van onze vrij verkrijgbare OUCH-nieuwsbrieven om uw programma te ondersteunen. Ze zijn allemaal vertaald in meer dan twintig talen. Hieronder staan de OUCH-nieuwsbrieven die volgens ons het beste uw initiatief kunnen ondersteunen om veilig thuis te werken. U kunt alle nieuwsbrieven terugvinden in het onlinearchief van de OUCH-nieuwsbrieven rond beveiligingsbewustzijn.

OVERZICHT

Four Steps to Staying Secure (Vier stappen om veilig te blijven)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

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

SOCIAL ENGINEERING

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

Messaging/Smishing (Sms'en/smishing)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

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

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

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

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

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

WACHTWOORDEN

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

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

AANVULLEND

Yes, You Are a Target (Ja, u bent een doelwit)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

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

Snelle tips

Tips en trucs die u eenvoudig kunt delen in een makkelijk behapbaar format.

- De doeltreffendste stappen om uw draadloze netwerk thuis te beveiligen? Het standaardwachtwoord veranderen, WPA2-versleuteling inschakelen en een sterk wachtwoord gebruiken voor uw draadloze netwerk.
- Weet welke apparaten verbonden zijn met uw thuisnetwerk, zoals babyfoons, spelconsoles, tv's, huishoudelijke apparaten of zelfs uw auto. Zorg ervoor dat al die apparaten beveiligd zijn met een sterk wachtwoord en de nieuwste versie van hun besturingssysteem.
- Een van de doeltreffendste manieren om uw computer thuis te beveiligen is ervoor zorgen dat zowel het besturingssysteem als alle programma's zijn gepatcht en bijgewerkt. Schakel indien mogelijk altijd automatisch updaten in.
- Uiteindelijk is gezond verstand uw beste bescherming. Lijkt een e-mail, telefoongesprek of onlinebericht vreemd, verdacht of te mooi om waar te zijn, dan is het mogelijk een aanval.
- Zorg ervoor dat u sterke en unieke wachtwoorden gebruikt voor al uw accounts. Kunt u al uw wachtwoorden/wachtwoordzinnen niet onthouden? Overweeg dan een wachtwoordmanager om ze allemaal te beheren.
- Tweestapsverificatie betekent dat u zowel uw wachtwoord nodig hebt als een code die wordt verstuurd of gegenereerd door uw mobiele apparaat. Tweestapsverificatie

betekent dat u zowel uw wachtwoord nodig hebt als een code die wordt verstuurd of gegenereerd door uw mobiele apparaat. Voorbeelden van diensten die tweestapsverificatie aanbieden, zijn Gmail, Dropbox en Twitter.

- Phishing betekent dat een aanvaller u probeert te misleiden om op een schadelijke link te klikken of een bijlage in een e-mail te openen. Wees argwanend bij e-mails of onlineberichten die een gevoel van urgentie creëren, taalfouten bevatten of u aanspreken als 'Geachte klant'.

Meetgegevens

Gedrag meten is moeilijk in deze situatie, aangezien niet evident is om te monitoren hoe mensen zich thuis gedragen. Daarnaast is bepaald gedrag niet werkspecifiek (zoals het beveiligen van een wifinetwerk). U kunt echter wel de betrokkenheid meten. We hebben gemerkt dat persoonlijke of emotionele onderwerpen als deze voor een grote betrokkenheid zorgen en veel meer interesse opwekken dan andere onderwerpen. Daarom kunnen metingen als deze van waarde zijn.

- **Interactie**: Hoe vaak stellen mensen vragen, posten ze ideeën of vragen ze om hulp via een van de beveiligingskanalen of forums die u hebt opgezet?
- **Simulaties**: doe een social-engineeringsimulatie, zoals phishing, sms'en of een telefonische aanval.

Voor een veel uitgebreidere lijst met metingen kunt u de interactieve Security Awareness-metingenmatrix downloaden uit het MGT433 Digitaal downloadpakket.

Licentie

Implementatiekit auteur

Lance Spitzner heeft meer dan 20 jaar beveiligingservaring in cyberbedreigingsonderzoek, beveiligingsarchitectuur en bewustwording en training. Hij heeft pionierswerk verricht op het vlak van misleiding en cyberinformatie met de creatie van Honeynets en de oprichting van het Honeynet Project. Als SANS-instructeur heeft hij de trainingen MGT433: Beveiligingsbewustzijn en MGT521: Beveiligingscultuur ontwikkeld. Daarnaast heeft Lance drie boeken over beveiliging gepubliceerd, in meer dan 25 landen advies gegeven en meer dan 350 bedrijven geholpen om beveiligingsbewustzijns- en bedrijfscultuurprogramma's op te zetten om te helpen bij het beheersen van hun menselijke risico's. Lance is geregeld presentator, een fanatiek Twitteraar (@lspitzner) en werkt aan verschillende communitybeveiligingsprojecten. Voordat hij zich bezig ging houden met informatiebeveiliging, diende Lance Spitzner als officier in de Rapid Deployment Force van het Amerikaanse leger en behaalde hij zijn MBA aan de universiteit van Illinois.

Over SANS Institute

Het SANS Institute is in 1989 opgericht als coöperatieve onderzoeks- en onderwijsorganisatie. SANS is de meest betrouwbare en veruit de grootste aanbieder van cyberbeveiligingstrainingen en certificering voor professionals bij overheden en commerciële instituten wereldwijd. Erkende SANS-instructeurs geven meer dan 60 verschillende livetrainingen op meer dan 200 evenementen rond cyberbeveiliging en ook online. GIAC, een onderdeel van SANS Institute, valideert de kwalificaties van een beoefenaar via meer dan 35 praktische, technische certificeringen in cyberbeveiliging. Het SANS Technology Institute, een regionaal geaccrediteerde onafhankelijke dochteronderneming, biedt masteropleidingen in cyberbeveiliging. SANS biedt de InfoSec-gemeenschap een groot

aantal gratis middelen, waaronder consensusprojecten, onderzoeksrapporten en nieuwsbrieven. Het beheert ook het systeem voor vroegtijdige waarschuwing van internet – het Internet Storm Center. De kern van SANS zijn de vele beveiligingsmedewerkers, die uiteenlopende wereldwijde organisaties vertegenwoordigen, van bedrijven tot universiteiten, die samenwerken om de hele informatiebeveiligingsgemeenschap te helpen. (https://www.sans.org)