SANS SECURITY AWARENESS

Security Awareness implementatiehandleiding - Thuis veilig werken

Samenvatting

Als gevolg van het Coronavirus zijn veel organisaties op dit moment bezig om hun werknemers vanuit huis te laten werken. Dit kan een hele uitdaging zijn, omdat het veel bedrijven ontbreekt aan beleid, technologie en training om het personeel op afstand te beveiligen. Daarnaast zijn veel werknemers misschien niet bekend met het idee van thuiswerken of voelen ze zich hier niet prettig bij. Het doel van deze handleiding is om u de mogelijkheid te bieden deze mensen snel te trainen in veilig werken. Mocht u vragen hebben over het gebruik van deze handleiding, neem dan contact met ons op via support@sans.org.

Aangezien uw personeel op dit moment waarschijnlijk met veel stress en veranderingen te maken heeft en uw organisatie waarschijnlijk maar een beperkte hoeveelheid tijd en middelen heeft, is deze handleiding erop gericht de training zo eenvoudig mogelijk te houden. We raden aan om u alleen te richten op de belangrijkste risico's met de grootst mogelijke gevolgen, die we hieronder beschrijven. Zie deze als een beginpunt. Indien er aanvullende risico's of onderwerpen zijn die u wilt toevoegen, doe dit dan vooral. Besef echter wel dat hoe meer gedragingen, processen en technologieën u van uw personeel vereist, hoe kleiner de kans wordt dat ze alles kunnen opvolgen.

Zo gebruikt u deze handleiding

We raden u aan om te beginnen met het doorlezen van de informatie in deze handleiding en het bekijken van de links naar diverse informatie, zodat u een idee krijgt wat er beschikbaar is. U zult merken dat wij voor ieder risico een verscheidenheid aan materiaal hebben dat u kunt gebruiken om uw organisatie te betrekken en te trainen. Zo kunt u de modaliteiten selecteren waarvan u denkt dat ze het beste aansluiten bij uw behoeften en cultuur. Nadat u dit document hebt doorgelezen, lees dan ook de bijgesloten Communicatietemplate en Factsheet door die onderdeel uitmaken van deze kit, zodat u beter kunt begrijpen wat u probeert te bereiken. Nadat u deze documentatie hebt doorgelezen, zijn er twee belangrijke groepen waarmee u moet coördineren.

1. **Beveiligingsteam**: coördineer met uw beveiligingsteam om beter zicht te krijgen op de belangrijkste risico's die u probeert te beheersen. Wij hebben in deze handleiding geïdentificeerd wat volgens ons de belangrijkste, meest voorkomende risico's zijn voor thuiswerkend personeel, maar uw risico's kunnen afwijken. Let wel op: een veel gemaakte fout door beveiligingsteams is dat ze proberen om alle risico's te beheersen en daardoor werknemers overspoelen met regels en vereisten. Probeer het aantal risico's dat u wilt beheersen zo klein mogelijk te houden. Wanneer u deze risico's geïdentificeerd en prioriteit hebt gegeven, bevestig dan welk gedrag die risico's beheersbaar houdt. Zoals

eerder al vermeld: als het uw organisatie ontbreekt aan de tijd of middelen om dit te doen, neem dan over wat we hieronder vermelden.

2. **Communicatieteam**: zodra u uw belangrijkste menselijke risico's hebt geïdentificeerd en het gedrag hebt bepaald om die risico's te beheersen, werk dan samen met uw communicatie-afdeling om uw personeel te betrekken bij en trainen in dit gedrag. De meest effectieve beveiligingsbewustzijnsprogramma's hebben een nauwe samenwerking met hun communicatieteam. Indien mogelijk kunt u kijken of u iemand van het communicatieteam in uw beveiligingsteam kunt opnemen. Wanneer u communiceert met uw personeel, dan kan een effectieve methode om hen te betrekken zijn om te benadrukken dat deze training hen niet alleen op het werk beveiligt, maar dat ze hiermee ook een Cyberveilig thuis kunnen creëren, en zo zichzelf en hun familie kunnen beschermen.

Door met deze twee groepen samen te werken, probeert u uiteindelijk zowel beveiliging zo simpel mogelijk te maken voor uw personeel en uw personeel te motiveren, de twee essentiële elementen voor gedragsverandering. We stellen zelfs voor om een adviesraad op te zetten met belangrijke mensen wiens feedback en input u 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 aan genaamd MGT433: Zo bouwt, onderhoudt en meet u een effectief beveiligingsbewustzijnsprogramma. Deze intensieve cursus bevat alle theorie, vaardigheden, kaders en middelen om een effectief bewustzijnsprogramma op te bouwen waarmee u uw menselijke risico's op efficiënte wijze kunt managen en meten. Als onderdeel van deze handleiding geven we u gratis toegang tot het Digitale downloadpakket van deze cursus, met daarin templates en planningsmateriaal. Hoewel dit waarschijnlijk de behoefte van dit initiatief ver overschrijdt, kan dit materiaal toch waardevol zijn voor grotere organisaties of complexere uitvoeringen.

Vragen van personeel beantwoorden

Naast het communiceren naar en trainen van uw personeel, raden we u sterk aan om een bepaalde vorm van technologie of forum op te zetten, waar u vragen van uw personeel kunt beantwoorden, bij voorkeur in realtime. Dit kan zijn via een hiervoor aangemaakt e-mailadres, Skype- of Slack-chatkanaal of een soort online forum zoals Yammer. Een ander idee is om een livestream over beveiliging te organiseren die u een aantal keer gedurende de week herhaalt, zodat mensen zelf kunnen bepalen op welk moment ze hem live willen bijwonen en mogelijk zelfs vragen kunnen stellen. Het doel is dat u beveiliging zo laagdrempelig mogelijk wilt maken en mensen wilt helpen met hun vragen. Dit is een

uitgelezen kans om uw personeel te betrekken en beveiliging in een vriendelijker daglicht te zetten, dus probeer hier gebruik van te maken. Houd er rekening mee dat om dit efficiënt te laten werken, u mensen moet inzetten om de veiligheidskanalen te modereren en actief vragen te beantwoorden.

Risico's en trainingsmateriaal

We hebben drie kernrisico's geïdentificeerd die u zou moeten beheren voor uw thuiswerkende personeel. Deze vormen een beginpunt en zijn waarschijnlijk de risico's die voor u het meest waardevol zijn. Ieder risico hieronder heeft links naar meerdere materialen om te ondersteunen in het communiceren en trainen van het onderwerp. We bieden meerdere communicatiematerialen aan, zodat u zelf degene kunt kiezen die de grootste impact hebben in uw bedrijfscultuur. Daarnaast zijn bijna alle materialen beschikbaar in meerdere talen. Mocht dit allemaal te overweldigend zijn en hebt u zeer beperkt tijd, dan raden we u aan om gewoon de twee hieronder genoemde materialen in te zetten.

1. Thuis veilig werken-factsheet (onderdeel van uw implementatiekit)
2. Beveiliging tegen cybercriminelen thuis-video (Engels) ook beschikbaar in andere talen

Social engineering

Een van de grootste risico's die werknemers op afstand lopen, vooral in deze tijd vol dramatische veranderingen en een sfeer van urgentie, zijn social engineering-aanvallen. Social engineering is een psychologische aanval waarbij aanvallers hun slachtoffers misleiden om een fout te maken, wat een stuk eenvoudiger is in een tijd vol verandering en verwarring. Het belangrijkste is om mensen te leren wat social engineering is, hoe ze de meest voorkomende aanwijzingen van een social engineering-aanval herkennen en wat ze moeten doen wanneer ze een aanval signaleren. Zorg ervoor dat u zich niet uitsluitend richt op phishing e-mails, want andere methodes zijn onder andere telefoontjes, sms'en, sociale media of nepnieuws. U vindt de materialen die u nodig hebt om dit onderwerp te trainen in onze map Social Engineering ondersteuningsmateriaal. Daarnaast zijn hier twee SANS Security Awareness-video's waarnaar u kunt linken, wederom 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

gedragingen die dit risico kunnen helpen beheersen. U vindt de materialen die u nodig heb om dit onderwerp te trainen in onze map Wachtwoorden.

- Wachtwoordzinnen (opmerking: zowel wachtwoordcomplexiteit als wachtwoordverloop zijn niet langer actief).
- Unieke wachtwoorden voor elk account
- Wachtwoordmanagers
- Multifactor-verificatie. Vaak ook twee-factor-authenticatie of twee-staps-verificatie genoemd

Bijgewerkte systemen

Het derde risico is ervoor zorgen dat de technologie die uw personeel gebruikt, is bijgewerkt met de nieuwste versies van het besturingssysteem, programma's en mobiele apps. Voor mensen die persoonlijke apparaten gebruiken, kan dit betekenen dat ze automatisch updaten moeten inschakelen. U vindt de materialen die u nodig hebt om dit onderwerp te trainen in onze map Malware of Beveiliging tegen cybercriminelen thuis.

Andere onderwerpen ter overweging

- **Wifi**: het beveiligen van uw wifi-netwerk. Dit wordt behandeld in het materiaal van Beveiliging tegen cybercriminelen thuis. Bekijk ook deze video over Beveiliging tegen cybercriminelen 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 individuen die telewerken maar NIET thuiswerken, bijvoorbeeld mensen die werken vanuit een café, het vliegveld of een hotel. Overweeg hiervoor onze Telewerken-trainingsvideo (Engels) ook beschikbaar in andere talen.

- **Kinderen/gasten**: Om de noodzaak te benadrukken dat familie/gasten geen toegang mogen hebben tot werkgerelateerde apparatuur, kunt u onze Telewerken-trainingsvideo (Engels) overwegen, ook beschikbaar in andere talen hier.

- **Detectie/reactie**: Wilt u dat mensen het melden wanneer ze vermoeden dat er een incident heeft plaatsgevonden terwijl ze thuiswerken? En zo ja, wat wilt u dat ze melden en wanneer? Dit wordt behandeld in ons Gehackt-materiaal.

OUCH-nieuwsbrief

Overweeg daarnaast 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 vermeld waarvan wij denken dat ze het beste uw Thuis veilig werken-initiatief kunnen ondersteunen. U kunt alle nieuwsbrieven terugvinden in ons OUCH Beveiligingsbewustzijn-nieuwsbriefarchief.

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 (Beveiliging tegen cybercriminelen 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 meest efficiënte stappen die u kunt ondernemen om uw draadloze netwerk thuis te beveiligen, is door het standaard admin-wachtwoord te veranderen, WPA2-versleuteling in te schakelen en een sterk wachtwoord te gebruiken voor uw draadloze netwerk.
- Wees u bewust van alle apparaten die verbinding maken 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 meest effectieve manieren om uw computer thuis te beveiligen is ervoor te 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 online-bericht 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.
- Twee-staps-verificatie is één van de meest effectieve stappen die u kunt ondernemen

om uw accounts te beveiligen. Twee-staps-verificatie betekent dat u zowel uw wachtwoord nodig hebt, als een code die wordt verstuurd of gegenereerd door uw mobiele apparaat. Voorbeelden van diensten die twee-staps-verificatie 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 online-berichten die een gevoel van urgentie creëren, taalfouten bevatten of u aanspreken als "Geachte klant".

Metingen

Gedragsmetingen zijn lastig in deze situatie, aangezien het lastiger te monitoren is hoe mensen zich thuis gedragen. Daarnaast zijn bepaalde gedragingen niet werkspecifiek (zoals het beveiligen van een wifi-netwerk). Maar u kunt wel betrokkenheid meten. Wij hebben bemerkt dat persoonlijke of emotionele onderwerpen als deze zeer sterke betrokkenheid oproepen 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**: voer een soort social engineering-simulatie uit, zoals phishing, tekstberichten 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

Auteur voorbereidingskit

Lance Spitzner heeft meer dan 20 jaar beveiligingservaring in cyberdreigingsonderzoek, beveiligingsarchitectuur en bewustwording en training. Hij heeft pionierswerk verricht in de werkvelden deceptie en cyberintelligentie met zijn creatie honeynets en het oprichten van 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 leger en behaalde hij zijn MBA bij de universiteit van Illinois.

Over SANS Institute

Het SANS Institute is in 1989 opgericht als een coöperatieve onderzoeks- en onderwijsorganisatie. SANS is de meest betrouwbare en veruit grootste aanbieder van cyberbeveiligingstrainingen en certificering voor professionals bij overheden en commerciële instituten wereldwijd. Erkende SANS-instructeurs geven meer dan 60 verschillende trainingen op meer dan 200 live cyberbeveiligingstrainings-evenementen en ook online. GIAC, 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 een groot aantal gratis middelen aan de

InfoSec-gemeenschap aan, 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)