SANS SECURITY AWARENESS

Kursus i sikkerhedsbevidsthed – Sådan arbejder du sikkert hjemmefra

Opsummering

På grund af coronavirus har mange virksomheder været nødt til at bede deres ansatte om at arbejde hjemmefra. Det kan være udfordrende, eftersom mange virksomheder mangler politikker, teknologi og træning til at sikre medarbejderne ordentligt. Derudover er mange ansatte ikke vant til at arbejde hjemmefra og synes måske ikke om det. Formået med denne guide er at gøre det muligt for dig at træne disse personer, så de kan sikres bedst muligt. Hvis du spørgsmål vedrørende brugen af denne guide, er du velkommen til at kontakte os på support@sans.org.

Eftersom dine ansatte skal forholde sig til en hel del stress og ændringer, og din virksomhed sikkert er begrænset af både tid og ressourcer, fokuserer denne strategiske guide på at gøre træningen så enkel som muligt. Vi anbefaler, at du fokuserer på de vigtigste risici som beskrevet nedenfor, så du kan maksimere træningens effektivitet. Du kan opfatte dem som et udgangspunkt. Hvis der er andre risici eller emner, du gerne vil dække, er du meget velkommen til at gøre det. Så længe du bare holder dig for øje, at det bliver mindre sandsynligt, at dine ansatte vil implementere alle de nye adfærdsregler, processer og teknologier, jo flere du implementerer af dem.

Sådan bruger du denne guide

Vi anbefaler, at du begynder med at læse alt materialet i denne guide igennem og følger alle links til yderligere materialer, så du får et overblik over de tilgængelige ressourcer. Du vil bemærke, at vi leverer forskellige materialer til hver risikotype, som du kan bruge, når du skal træne og engagere dine ansatte. Det giver dig mulighed for at vælge de fremgangsmåder, der passer bedst til din virksomheds behov og kultur. Når du er færdig med at læse dette dokument, bør du også læse kommunikationsskabelonen og faktaarket, der medfølger, så du er helt klar over, hvad du forsøger at opnå. Når du har læst dokumentationen, skal du koordinere med to nøglegrupper.

1. **Sikkerhedsteamet**: Koordinér med dit sikkerhedsteam for at opnå en bedre forståelse af, hvilke risici du forsøger at imødegå. Vi har i denne guide identificeret, hvad vi mener er de mest typiske risici for ansatte, der arbejder hjemme, men du vil muligvis opleve andre risici. Vi må også advare om den typiske fejltagelse, der begås, når sikkerhedsteams forsøger at imødegå alle risici og kommer til at overvælde folk med for mange politikker og krav. Prøv at begrænse de risici, du vil imødegå, til så få som muligt. Når du har identificeret og prioriteret disse risici, skal du gennemgå de adfærdsændringer, der vil imødegå dem. Som nævnt tidligere, kan du altid bruge det, vi fremlægger herunder, hvis din virksomhed hverken har tid eller ressourcer til dette.

2. **Kommunikation**: Når du har identificeret de vigtigste menneskelige risikofaktorer og de adfærdsændringer, der kræves for at imødegå dem, bør du arbejde sammen med jeres kommunikationsteam om at engagere og træne de ansatte til at følge disse anvisninger. De mest effektive programmer for sikkerhedsbevidsthed er dem, der fremlægges i samarbejde med kommunikationsteamet. Om muligt kan du også prøve at overføre personer fra kommunikationsafdelingen til dit sikkerhedsteam. Når du kommunikerer med dine ansatte, kan det være en god idé at understrege over for dem, at træningen ikke kun vil sikre dem i forhold til arbejde, men også hjælpe dem med at cyber-sikre deres hjem og beskytte både dem selv og deres familie.

Ved at arbejde sammen med disse to grupper kan du forsøge at gøre det så let som muligt for dine ansatte at forstå sikkerhedsbehovet og samtidig motivere dem – to af de vigtigste faktorer, når du vil indføre adfærdsændringer. Vi anbefaler dig at etablere en rådgivningsgruppe, der indeholder nøglepersoner, hvis feedback du har brug for, når du skal implementere programmet. Ud over dine sikkerheds- og kommunikationsafdelinger kan det også være oplagt at arbejde sammen med og koordinere med HR-afdelingen og den juridiske afdeling.

MGT433 – Digital downloadpakke

SANS Institute leverer todags-træningskurset MGT433: Sådan opbygger du, fastholder og måler et effektivt program for sikkerhedsbevidsthed. Denne intensive træning rummer al teorien, evnerne, frameworket og ressourcerne, der er nødvendige for at rulle et effektivt bevidstprogram ud, så du opnår kontrol din virksomheds menneskelige risikoelement og måle på den. Som led i denne guide giver vi gratis adgang til kursets digitale downloadpakke med skabeloner og planlægningsredskaber. Disse materialer rækker sikkert langt ud over, hvad der er nødvendigt til dette formål, men de kan være meget nyttige for større virksomheder eller mere komplekse anvendelsessituationer.

Reaktion på spørgsmål fra ansatte

Ud over at kommunikere til og træne dine ansatte, anbefaler vi kraftigt, at du også gør en form for teknologi eller forum tilgængeligt, hvor du kan besvare folks spørgsmål – meget gerne løbende. Det kan for eksempel foregå via et dedikeret mail-alias, Skype eller en Slack-kanal eller i et onlineforum som Yammer. Det kan også være en god idé at hoste en sikkerheds-webcast, som du gentager flere gange om ugen, så folk kan vælge det tidspunkt, der passer dem bedst, og deltage live og få mulighed for at stille spørgsmål. Målet er i sidste ende at gøre sikkerhed så tilgængeligt som muligt og besvare folks spørgsmål. Det er en fantastisk mulighed for at engagere dine ansatte og give sikkerhed et menneskeligt ansigt, så prøv at udnytte den så meget som muligt. Husk også, at du bør dedikere en ressource til at moderere sikkerhedskanaler og aktivt besvare henvendelser.

Risici og træningsmaterialer

Vi har identificeret tre primære risici, som du bør imødegå på vegne af dine ansatte. De udgør et udgangspunkt og er formentlig dem, der vil være vigtigst for dig. Hver af de risici, der er beskrevet herunder, har links til forskellige ressourcer, der kan hjælpe dig med at kommunikere og træne folk i emnet. Vi gør en række forskellige kommunikationsmaterialer tilgængelige, så du kan vælge dem, der er mest effektive i forhold til din virksomheds kultur. Derudover er næsten alle materialerne også oversat til en række forskellige sprog. Hvis alt dette virker overvældende, og din tid er ekstremt begrænset, anbefaler vi, at du bare arbejder videre med de to materialer herunder.

1. Faktaark om at arbejde sikkert hjemmefra (medfølger i dit informationssæt).
2. Et cyber-sikkert hjem (engelsk) er også tilgængelig på andre sprog her

Social engineering

En af de største risici ved at arbejde uden for kontoret, særligt i denne tid med dramatiske forandringer og behovet for at handle hurtigt, er social engineering-angreb. Social engineering er et psykologisk angreb, hvor angriberne snyder deres ofre til at begå fejl, og de er lettere at udføre på tidspunkter med store forandringer og forvirring. Det vigtige er at træne folk i forståelse af social engineering, så de kan identificere de mest almindelige tegn på social engineering-angreb, og vide, hvad de skal gøre, hvis de opdager dem. Sørg for ikke kun at fokusere på phishing-mailangreb, men også andre metoder, der omfatter telefonopkald, sms-beskeder, sociale medier eller misinformation. Du kan finde de materialer, du skal bruge for at træne dine ansatte i dette emne i mappen Social Engineering-hjælpematerialerne. Derudover kan du også linke til to SANS-videoer om sikkerhedsbevidsthed, som også er tilgængelige på flere sprog.

- Social Engineering (engelsk) er også tilgængelig på andre sprog her
- Phishing (engelsk) er også tilgængelig på andre sprog her

Stærke adgangskoder

Som beskrevet i Verizons årlige DBIR, er svage adgangskoder stadig en af de primære årsager til sikkerhedsbrud over hele verden. Fire primære adfærdstyper, som er påkrævet for at imødegå denne risiko, er beskrevet herunder. Du kan finde de materialer, du skal bruge for at træne og repetere dette emne og disse fire vigtige adfærdstyper i vores Adgangskoder-mappe.

- Kodesætninger (bemærk, at både adgangskode-kompleksitet og adgangskode-udløb ikke er relevante længere).
- Unikke adgangskoder til alle konti

- Password-managers
- MFA (Flerfaktorgodkendelse). Også kaldet tofaktor-godkendelse eller totrins-bekræftelse

Opdaterede systemer

Den tredje risikofaktor kræver, at du sikrer, at alle teknologier, dine ansatte anvender, kører med den nyeste version af deres respektive operativsystemer, applikationer og mobile apps. Det kan kræve, at automatisk opdatering bliver aktiveret for folk, der bruger deres personlige enheder. Du kan finde de materialer, du skal bruge for træne ansatte i dette emne, i mapperne Malware og Et cyber-sikkert hjem.

Yderligere emner, du kan overveje

- **Wi-fi**: Sikring af dit trådløse adgangspunkt. Dette er dækket i Sådan cyber-sikrer du dit hjem-materialerne. Overvej også at se videoen Et cyber-sikkert hjem (engelsk), som du også kan finde på andre sprog her.

- **VPN-forbindelser**: Hvad er en VPN-forbindelse, og hvorfor skal du bruge den? Vi kan anbefale dig at læse OUCH-nyhedsbrevet om VPN-forbindelser.

- **Arbejde væk fra kontoret**: Dette er til personer, der arbejder væk fra kontoret, men IKKE hjemmefra, som for eksempel på caféer eller i lufthavnsterminaler eller hoteller. Overvej at bruge vores Arbejde væk fra kontoret-træningsvideo (engelsk) , som også er tilgængelig på andre sprog her.

- **Børn / Gæster**: Hvis du vil understrege, at familie / gæster ikke må få adgang til arbejdsrelaterede enheder, kan du overveje at bruge Arbejde væk fra kontoret-træningsvideo (engelsk), som også er tilgængelig på andre sprog her.

- **Identifikation / Reaktion**: Vil du gerne have folk til at melde det, hvis de mener, at der har været en hændelse, mens de arbejdede hjemmefra? Og hvad vil du i så fald have dem til at melde, og hvornår? Dette er dækket i vores Hacket-materialer.

OUCH-nyhedsbreve

Herudover kan du også vælge at benytte de offentligt tilgængelige OUCH, som er oversat til over 20 forskellige sprog, i forbindelse med dit program. Herunder kan du se de OUCH-nyhedsbreve, som vi mener er bedst egnede til dit "Arbejd sikkert hjemmefra"-initiativ. Du kan se alle nyhedsbrevene online i OUCH-sikkerhedsnyhedsbrevets arkiv.

Overblik

Four Steps to Staying Secure (Fire trin, der sikrer dig)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

(Creating a Cybersecure Home) Et cyber-sikkert hjem
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

Messages / Smishing (Beskeder / Smishing)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

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

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

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

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

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

ADGANGSKODER

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

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

YDERLIGERE

Yes, You Are a Target (Ja, du er et mål)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Enheder i det smarte hjem)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Hurtige tips

Tips og tricks, du kan dele i et let overskueligt format.

- Det mest effektive, du kan gøre for at sikre dit trådløse netværk derhjemme, er at ændre din standard-administrator-adgangskode, aktivere WPA2-kryptering og bruge en stærk adgangskode til dit trådløse netværk.
- Vær opmærksom på alle enheder, der har forbindelse til dit hjemmenetværk, blandt andet babyalarmer, spillekonsoller, fjernsyn, køkkenapparater og din bil. Sørg for, at alle disse enheder er beskyttet af en stærk adgangskode og/eller kører den nyeste version af deres operativsystem.
- En af de mest effektive måder at beskytte din computer derhjemme på er at sikre dig, at både operativsystemet og dine applikationer er patchede og opdaterede. Slå altid automatisk opdatering til, hvis det er muligt.
- I sidste ende er sund fornuftigt din bedste beskyttelse. Hvis en e-mail eller et opkald virker sært, mistænkeligt eller for godt til at være sandt, kan det være et angreb.
- Sørg for at have separate, unikke adgangskoder til alle dine konti. Kan du ikke huske alle dine adgangskoder/kodesætninger? Så kan du overveje at bruge en password-manager til dem.
- Totrinsbekræftelse er en af de bedste ting, du kan gøre for at sikre din konto. Totrins-bekræftelse består af både en adgangskode og en kode, der bliver sendt til eller genereret af din mobile enhed. Gmail, Dropbox og Twitter er nogle af de tjenester, der

understøtter tofaktorgodkendelse.

- Phishing er et angreb, der forsøger at snyde dig til at klikke på et ondsindet link eller åbne en vedhæftet fil i en mail. Vær mistænksom over for alle e-mails og onlinebeskeder, der forsøger at få dig til at skynde dig, som er dårligt stavet, eller som tiltaler dig som "Dear Customer" (Kære kunde).

Adfærdsmåling

Det kan være vanskeligt at måle adfærd i denne situation, fordi det er sværere at finde ud af, hvordan folk arbejder derhjemme. Derudover er nogle af disse adfærdstyper ikke arbejdsspecifikke (som for eksempel sikring af trådløse netværk). Men du kan måle engagement. Det er vores erfaring, at personlige eller følelsesmæssige emner som disse kan være meget engagerende og vække langt større interesse end andre emner. Derfor kan følgende målinger være værdifulde.

- **Interaktion**: Hvor ofte stiller folk spørgsmål, deler idéer eller anmoder om hjælp på en af de sikkerhedskanaler eller forummer, du står for?
- **Simulationer**: Udfør simulationer af social engineering, for eksempel phishing-, sms- eller telefonbaserede angreb.

Du kan downloade interaktiv matrix med sikkerhedsbevidsthedsmålinger fra den digitale MGT433-downloadpakke for at se en længere liste over målinger.

Licens

Forfatter

Lance Spitzner har over 20 års sikkerhedserfaring inden for forskning i cyber-trusler, sikkerhedsarkitektur og bevidsthed og træning. Han har stiftet Honeynet Project og er med idéen til "honeynets" en pionér inden for bedrageri og cyber-efterforskning. Som SANS-instruktør har han udviklet MGT433: Sikkerhedsbevidsthed- og MGT521: Sikkerhedskultur-kurserne. Derudover har Lance udgivet tre bøger om sikkerhed, fungeret som konsulent i over 25 lande og hjulpet over 350 virksomheder med at opbygge sikkerhedsbevidstheds- og kulturprogrammer, der hjælper dem med at begrænse deres menneskelige risikoelement. Lance afholder ofte præsentationer, tweeter jævnligt (@lspitzner) og arbejder på adskillige sikkerhedsprojekter. Før han begyndte at arbejde med informationssikkerhed, fungerede han som arsenalofficer i hærens Rapid Deployment Force og tog en MBA på University of Illinois.

Om SANS Institute

SANS Institute blev etableret som forsknings- og uddannelsesorganisation i 1989. SANS er den mest betroede og største leverandør af cyber-sikkerhedstræning og certificering til ansatte i regeringer og virksomheder over hele verden. Kendte SANS-instruktører underviser i over 60 forskellige kurser i mere end 200 cyber-sikkerhedstræning-livebegivenheder samt online. GIAC er partner med SANS Institute og godkender deltagernes kvalifikationer med over 35 tekniske certificeringer i cyber-sikkerhed. SANS Technology Institute er et regionalt akkrediteret uafhængigt firma, der tilbyder mastergrader i cyber-sikkerhed. SANS tilbyder et væld af gratis ressourcer til InfoSec-fællesskabet, blandt andet konsensusprojekter, forskningsrapporter og nyhedsbrev; vi fungerer også som internettets tidlige advarselssystem med The Internet Storm Center. Kernen i SANS er de mange sikkerhedseksperter, som repræsenterer forskellige internationale organisationer, lige fra firmaer til universiteter, der arbejder sammen om at hjælpe hele verdens sikkerhedsfællesskab. (https://www.sans.org)