SANS SECURITY AWARENESS

Implementeringsguide för säkerhetsmedvetenhet – Arbeta säkert hemifrån

Sammanfattning

På grund av Coronaviruset är det många organisationer som låter sin personal arbeta hemifrån. Detta kan vara en utmaning då många organisationer saknar policyer, teknologi och utbildning för att säkra en arbetsstyrka som arbetar på distans. Utöver det kan många anställda vara ovana och obekväma med att arbeta hemifrån. Syftet med denna guide är att göra det möjligt för dig att snabbt utbilda dessa personer till att vara så säkra som möjligt. Om du har några frågor om hur man använder denna guide, kontakta oss på support@sans.org.

Då din personal troligtvis upplever mycket stress och förändring, och din organisation sannolikt är begränsad när det kommer till tid och resurser, fokuserar denna strategiska guide på att göra utbildningen så enkel som möjligt. Vi rekommenderar att du fokuserar på de viktigaste riskerna som påverkar mest, vilka vi beskriver nedan. Tänk på dessa som en startpunkt. Skulle det finnas andra risker eller ämnen så kan du lägga till dem efter behov. Tänk bara på att ju mer beteenden, processer eller teknik som du lägger på din personal, desto mindre troligt är det att de kan implementera allt.

Så här använder du denna guide

Vi rekommenderar att du börjar läsa materialet i denna guide och besöker länkarna för att få mer information så att du kan få en uppfattning om vad som finns tillgängligt. Du kommer att upptäcka att vi för varje risk tillhandahåller en mängd olika material som du kan använda för att engagera och utbilda din organisation. Detta gör att du kan välja de modaliteter som du tror fungerar mest effektivt för din organisations behov och kultur. När du har läst klart detta dokument, fortsätt att läsa både den medföljande kommunikationsmallen och faktabladet för att bättre förstå vad du försöker uppnå. När du har läst dokumentationen finns det två nyckelgrupper som du behöver samordna med.

1. **Säkerhetsteamet**: Samordna med ditt säkerhetsteam för att få en bättre förståelse om vilka nyckelrisker du försöker hantera. I denna guide har vi identifierat vilka vi anser är de viktigaste och vanligaste riskerna för en arbetsstyrka som arbetar hemifrån, dina risker kan dock skilja sig åt. Så tänk dig lite för, ett vanligt misstag som säkerhetsteam gör är att försöka hantera alla risker och överösa personalen med mängder av policyer och krav. Försök att begränsa riskerna som du vill hantera till så få som möjligt. När du har identifierat och prioriterat dessa risker, bekräfta beteenden som hanterar dessa risker. Som redan nämnts, om din organisation inte har tid eller resurser för detta, använd det vi dokumenterar nedan.

2. **Kommunikationer**: När du har identifierat de största mänskliga riskerna och nyckelbeteenden för att hantera dessa risker, samarbeta med ditt kommunikationsteam för att engagera och utbilda din personal om dessa beteenden. De effektivaste programmen för säkerhetsmedvetenhet har ett nära samarbete med sitt kommunikationsteam. Se om möjligt till att inkludera någon från kommunikationsavdelningen i ditt säkerhetsteam. När du kommunicerar med din personal är ett effektivt sätt att engagera dem att betona att denna utbildning inte bara gör dem säkra på jobbet utan också gör det möjligt för dem att skapa ett cybersäkert hem för att skydda sig själv och sin familj.

Genom att arbeta med dessa två grupper försöker du göra säkerheten både så enkel som möjligt för din personal och samtidigt motivera din arbetsstyrka, vilka är de två viktigaste elementen om man vill förändra ett beteende. Vi föreslår även att du upprättar en rådgivande panel med nyckelpersoner vars feedback och input du behöver för att införa programmet. Utöver ditt säkerhets- och kommunikationsteam, kan andra avdelningar som du vill samarbeta och samordna med inkludera personalavdelningen och den juridiska avdelningen.

MGT433 Digitalt nedladdningspaket

SANS Institute erbjuder en två dagar lång utbildningskurs MGT433: Så här skapar, bibehåller och utvärderar du program för säkerhetsmedvetenhet med stor påverkan. Denna intensivkurs tillhandahåller alla teorier, färdigheter, ramverk och resurser som behövs för att skapa ett program för medvetenhet med stor påverkan som gör att du effektivt kan hantera och mäta din mänskliga risk. Som en del av denna guide tillhandahåller vi gratis tillgång till kursens Digitala nedladdningspaket med mallar och planeringsresurser. Även om dessa troligtvis täcker mer än behoven för detta initiativ, kan materialen vara värdefulla för större organisationer eller mer komplexa implementeringar.

Svara på personalens frågor

Utöver att kommunicera och utbilda personalen, rekommenderar vi starkt någon typ av teknologi eller forum där ni (helst i realtid) kan svara på personers frågor. Detta kan inkludera ett dedikerat e-postalias, chattkanalen Skype eller Slack, eller någon typ av online-forum, t.ex. Yammer. En annan idé är att vara värd för en webbsändning om säkerhet som du upprepar flera gånger i veckan. Personal kan på så sätt välja en tidpunkt som passar bäst för dem och delta i realtid, samt kanske till och med ställa frågor. Målet är att du vill göra säkerhet så lättillgänglig som möjligt och hjälpa människor få svar på sina frågor. Detta är en fantastisk möjlighet att engagera din personal och göra ämnet säkerhet trevligare, se därför till att utnyttja detta tillfälle. Tänk på att för att detta ska vara effektivt bör du avsätta en resurs för att moderera alla säkerhetskanaler och aktivt svara på frågor.

Risker och utbildningsmaterial

Vi har identifierat tre viktiga risker för personal som arbetar på distans som du bör hantera. Dessa är startpunkten och sannolikt de som är mest värdefulla för dig. Varje risk nedan har länkar till flera resurser för att hjälpa till att kommunicera och lära ut ämnet. Vi tillhandahåller flera olika kommunikationsmaterial så att du kan välja de som har störst påverkan på din kultur. Utöver det kommer alla material på flera olika språk. Om allt detta är överväldigande och din tid är extremt begränsad, rekommenderar vi att du helt enkelt använder och distribuerar de två materialen nedan.

1. Faktabladet Arbeta säkert hemifrån (medföljer i ditt implementeringskit).
2. Videon Skapa ett cybersäkrare hem (engelska) som även finns på andra språk här

Social manipulation

En av de största riskerna som anställda som arbetar på distans möter, särskilt just nu med både dramatisk förändring och en brådskande miljö, är sociala manipulationsangrepp. Social manipulation är psykologiska angrepp där angriparen lurar sina offer till att göra ett misstag, vilket blir lättare vid en tidpunkt med stor förändring och förvirring. Nyckeln är att utbilda personal om vad social manipulation är, hur man upptäcker de vanligaste tecknen på sociala manipulationsangrepp och vad man ska göra när man upptäcker dem. Se till att du inte bara fokuserar på nätfiske via e-post, utan också metoder som omfattar telefonsamtal, sms, social media eller falska nyheter. Du kan hitta det material du behöver för att utbilda och framhäva detta ämne i vår mapp Supportmaterial för social manipulation. Utöver det följer här två videor om säkerhetsmedvetenhet från SANS som du kan länka till. Återigen, dessa tillhandahålls på flera olika språk.

- Social manipulation (engelska) som även finns på andra språk här
- Nätfiske (engelska) som även finns på andra språk här

Starka lösenord

Som identifierats i den årliga Verizon DBIR är svaga lösenord en av de främsta anledningarna till överträdelser på en global nivå. Nedan följer fyra nyckelbeteenden som hjälper till att hantera denna risk. Du kan hitta det material du behöver för att utbilda och förstärka detta ämne och dessa fyra nyckelbeteenden i vår mapp Lösenord.

- Lösenordsfraser (observera, både lösenordskomplexitet och lösenordsutgång är dött).
- Unika lösenord för alla konton
- Lösenordshanterare
- MFA (multifaktorautentisering). Som ofta kallas tvåfaktorsautentisering eller tvåstegsverifiering

Uppdaterade system

Den tredje risken är att se till att all teknologi som din personal använder drivs med den senaste versionen av operativsystem, applikationer och mobilappar. För personal som använder personliga enheter kan detta kräva att man aktiverar automatisk uppdatering. Du kan hitta det material du behöver för utbildning och förstärkning av detta ämne i mapparna Malware eller Skapa ett cybersäkert hem.

Ytterligare ämnen att överväga

- **Wi-Fi**: Säkra din Wi-Fi-åtkomstpunkt. Detta täcks i materialen Skapa ett cybersäkert hem. Överväg även denna video om Skapa ett cybersäkert hem (engelska) som även finns på andra språk här.
- **VPN**: Vad är en VPN och varför ska man använda det. Vi rekommenderar OUCH nyhetsbrev om VPN.
- **Arbeta på distans**: Detta är för individer som arbetar på distans men INTE hemifrån, utan på ett café, en flygplats eller ett hotell. Överväg att använda vår utbildningsvideo Arbeta på distans (engelska) som även finns på andra språk här.
- **Barn/Gäster**: För att stärka budskapet att familj/gäster inte ska ha tillgång till arbetsrelaterade enheter, överväg att använda utbildningsvideon Arbeta på distans (engelska) som även finns på andra språk här.
- **Detektering/Respons**: Vill du att personer rapporterar om de tror en incident förekommit när de arbetade hemifrån? Om så är fallet, vad vill du att de rapporterar och när? Detta täcks i våra material Hackad.

OUCH nyhetsbrev

Utöver detta, överväg att använda de offentligt tillgängliga OUCH nyhetsbreven för att stödja ditt program, som alla finns översatta på tjugo olika språk. Nedanför listas OUCH nyhetsbrev som vi tror kan ge bäst support för ditt initiativ att arbeta säkert hemifrån. Du kan hitta alla nyhetsbrev online i arkiven OUCH nyhetsbrev om säkerhetsmedvetenhet.

ÖVERSIKT

Four Steps to Staying Secure (Fyra steg för att hålla dig säker)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Skapa ett cybersäkert hem)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

SOCIAL MANIPULATION

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

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

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

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

Phone Call Attacks / Scams (Angrepp/bedrägerier via telefon)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

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

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

LÖSENORD

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

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

ÖVRIGT

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

Smart Home Devices (Enheter för smarta hem)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Snabbtips

Tips och tricks som du kan dela i ett enkelt format.

- De effektivaste åtgärderna som du kan vidta för att säkra ditt trådlösa nätverk hemma är att ändra det fabriksinställda administratörslösenordet, aktivera WPA2-kryptering och använda ett starkt lösenord för ditt trådlösa nätverk.
- Tänk på att alla enheterna som är anslutna till ditt hemnätverk, inklusive babymonitorer, spelkonsoler, TV, apparater eller till och med din bil. Se till att alla dessa enheter är skyddade med ett starkt lösenord och/eller drivs med den senaste versionen av deras operativsystem.
- Ett av de mest effektiva sätten som du kan skydda din dator hemma på är att se till att både operativsystemet och dina apparater är patchade och uppdaterade. Aktivera automatisk uppdatering när det är möjligt.
- I slutändan är sunt förnuft ditt bästa skydd. Om ett e-postmeddelande, telefonsamtal eller onlinemeddelande är udda, verkar misstänkt eller bara för bra för att vara sant, kan det vara ett angrepp.
- Se till att vart och ett av dina konton har ett separat och unikt lösenord. Kan du inte komma ihåg alla dina lösenord/lösenordsfraser? Överväg att använda en lösenordshanterare för att säkert lagra alla lösenord för dig.
- Tvåstegsverifiering är en av de bästa åtgärderna du kan vidta för att säkra något konto. Tvåstegsverifiering är när du behöver både ett lösenord och en kod skickad till

eller genererad på din mobila enhet. Exempel på tjänster som stöder tvåstegsverifiering omfattar Gmail, Dropbox och Twitter.

- Nätfiske är när en angripare försöker lura dig till att klicka på en skadlig länk eller öppna en bilaga i ett e-postmeddelande. Var misstänksam mot alla e-post- eller onlinemeddelanden som skapar en brådskande känsla, är felstavade eller tilltalar dig som "Bästa kund".

Mätvärden

Mätvärden för beteende är mer komplicerade för denna situation, då det är svårare att mäta hur personal beter sig hemma. Utöver detta är vissa av dessa beteenden inte arbetsrelaterade (som att säkra sin Wi-Fi-enhet). Du kan dock mäta engagemang. Vi har märkt att personliga eller känslomässiga ämnen som dessa kan vara mycket engagerande och väcka betydligt mer intresse än andra ämnen. På så sätt kan mätvärden som dessa vara värdefulla.

- **Interaktion**: Hur ofta ställer personal frågor, lägger fram idéer eller begär hjälp på någon av de säkerhetskanaler eller forum som du är värd för?
- **Simulationer**: Utför någon typ av sociala manipulationssimuleringar, till exempel angrepp baserade på nätfiske, sms eller telefonsamtal.

För en mycket mer omfattande lista över mätvärden, ladda ner den interaktiva matrisen om säkerhetsmedvetenhet från MGT433 digitala nedladdningspaket.

Licens

Författare av implementeringskit

Lance Spitzner har mer än 20 års säkerhetserfarenhet inom cyberhotsforskning, säkerhetsarkitektur och medvetenhet och utbildning. Han hjälpte till att lyfta fram fälten bedrägeri och cyberintelligens genom skapandet av honeynets och grundandet av Honeynet Project. Som en SANS-instruktör utvecklade han kurserna MGT433: Säkerhetsmedvetenhet och MGT521: Säkerhetskultur. Dessutom har Lance publicerat tre böcker om säkerhet, konsulterat i över 25 länder och hjälpt mer än 350 organisationer att konstruera program om säkerhetsmedvetenhet och kultur för att hantera deras mänskliga risker. Lance är en frekvent presentatör, idog tvittrare (@lspitzner) och arbetar med ett flertal projekt om samhällssäkerhet. Innan Spitzner började arbeta med informationssäkerhet tjänade han som stridsvagnsofficer i snabbinsatsstyrkan i amerikanska armén och har en MBA från University of Illinois

Om SANS Institute

SANS Institute grundades 1989 som en kooperativ forsknings- och utbildningsorganisation. SANS är den mest betrodda och klart största leverantören av utbildning om och certifiering av cybersäkerhet till yrkesverksamma på myndigheter och kommersiella institutioner över hela världen. Skickliga SANS-instruktörer undervisar i över 60 olika kurser vid mer än 200 live-utbildningar om cybersäkerhet samt online. GIAC, en av SANS Institutes samarbetspartners, validerar en utövares kvalifikationer med mer än 35 praktiska, tekniska certifieringar om cybersäkerhet. SANS Technology Institute, ett regionalt ackrediterat oberoende dotterbolag, erbjuder magisterexamen i cybersäkerhet. SANS erbjuder ett hav av gratis resurser till InfoSec-communityn, inklusive konsensusprojekt, forskningsrapporter och nyhetsbrev. De driver också Internets tidiga varningssystem – Internet Storm Center. Hjärtat av SANS består av flera säkerhetsutövare som representerar olika globala organisationer från företag till universitet och arbetar tillsammans för att hjälpa hela informationssäkerhetscommunityn. (https://www.sans.org)