SANS SECURITY AWARENESS

Iverksettelsesguide for sikkerhetsopplæring – Et trygt hjemmekontor

Sammendrag

Som et direkte resultat av koronaviruset er det mange bedrifter som nå legger til rette for at ansatte kan jobbe hjemmefra. Siden mange bedrifter mangler forskriftene, teknologien og opplæringen til å sikre en ekstern arbeidsstyrke, kan dette by på mange utfordringer. I tillegg kan de ansatte være ukjent med eller ukomfortable med det å jobbe fra sitt eget hjem. Formålet med denne guiden er at du raskt skal kunne trene disse personene til å bli så sikre som mulig. Om du har spørsmål vedrørende bruken av denne guiden, kan du kontakte oss på support@sans.org.

Fordi arbeidsstyrken din mest sannsynligvis opplever både stress og mange endringer, samtidig som bedriften mest sannsynligvis er underlagt tidspress og ressursbegrensninger, fokuserer denne guiden på at opplæringen skal være så enkel som mulig. Vi anbefaler at du fokuserer kun på de farene som har størst innvirkning. Disse har vi beskrevet nedenfor. Se på disse som et startpunkt. Legg gjerne til informasjon om andre risikoer eller temaer du føler er relevante. Ikke glem at jo flere rutiner, prosedyrer eller teknologityper du krever at de ansatte tar i bruk, desto mindre sannsynlig er det at alt blir gjennomført ordentlig.

Slik bruker du denne guiden

Vi anbefaler at du først leser materialene i selve guiden, for så å gjennomgå alle lenkene til de forskjellige ressursene. Dette for å gi deg en oversikt over hva som er tilgjengelig. Du vil oppdage at for hver risikotype byr vi på en rekke forskjellige typer hjelpemidler som du kan bruke når du skal lære opp de ansatte i bedriften. Dette lar deg selv velge hvilke moduler du føler vil være mest effektive for dine behov. Når du har lest deg gjennom dette dokumentet, kan du lese den tilhørende kommunikasjonsmalen og faktaskrivet som fulgte med i pakken. Dette vil gi deg en bedre forståelse for hva du prøver å oppnå. Så snart du har gjennomgått dokumentene, er det to hovedgrupper du må koordinere.

1. **Sikkerhetsteamet**: Koordiner med sikkerhetsteamet for å få en bedre forståelse for hvilke farer du prøver å håndtere. I denne guiden har vi lagt frem det vi føler er de mest relevante farene for ansatte som har hjemmekontor, men det kan hende dine farer er noe annerledes. Et lite tips: En vanlig feil mange sikkerhetsteam gjør, er at de prøver å håndtere alle farer og dermed overlesser de ansatte med utallige forskrifter og krav. Prøv å begrense farene du ønsker å håndtere, til et så lite antall som mulig. Så fort du har gjenkjent og prioritert disse farene, må du bekrefte de tiltakene som skal til for å håndtere dem. Som tidligere nevnt: Om bedriften ikke har tiden eller midlene til dette, kan du bruke dokumentasjonen nedenfor.

2. **Kommunikasjon**: Du kan samarbeide med kommunikasjonsteamet for å engasjere og lære opp de ansatte så fort du har identifisert de viktigste farene og de nødvendige tiltakene for å håndtere dem. Den mest effektive sikkerhetsopplæringen får du hvis forholdet til kommunikasjonsteamet er godt. Se om det lar seg gjøre å inkludere noen fra kommunikasjonsteamet i sikkerhetsteamet ditt. Når du kommuniserer med de ansatte, kan det være lurt å legge vekt på at opplæringen ikke bare vil sikre dem i arbeidslivet, men at den også vil hjelpe dem med å skape et cybersikkert hjem som kan beskytte både dem og familien deres.

Formålet ved å jobbe med disse to gruppene er å gjøre sikkerheten så enkel og motiverende som mulig for de ansatte. To viktige elementer for å skape adferdsendringer. Vi anbefaler at du oppretter et råd bestående av nøkkelpersoner hvis tilbakemeldinger du trenger for å gjennomføre planene. Det vil være andre grupper, bortsett fra sikkerhetsteamet og kommunikasjonsteamet, som du kanskje ønsker å samarbeide med og koordinere informasjon med. Sånn som personalavdelingen og den juridiske avdelingen.

Den digitale nedlastingspakken MGT433

SANS Institute leverer todagerskurset MGT433: Hvordan opprette, vedlikeholde og vurdere sikkerhetsopplæring med høy innvirkning. Dette intense kurset byr på alt av teori, ferdigheter, rammeverk og ressurser som trengs for å opprette sikkerhetsopplæring med høy innvirkning. Slik at du effektivt kan administrere og vurdere den menneskelige risikoen. Som en del av denne guiden byr vi på gratis tilgang til kursets digitale nedlastingspakke med maler og planleggingsmidler. Dette overgår sikkert behovene for dette tiltaket, men disse midlene kan ha stor verdi for større bedrifter eller utføringen av mer kompliserte tiltak.

Svare på spørsmål fra de ansatte

I tillegg til kommunikasjon og opplæringen av de ansatte anbefaler vi bruken av teknologi eller forum som lar deg svare på de ansattes spørsmål. Helst noe som lar deg gjøre dette i sanntid. Dette kan være en egen e-postadresse, et chatterom i Skype eller Slack, eller evt. et onlineforum via f.eks. Yammer. Et annet alternativ er å opprette en sikkerhetspresentasjon som du kan gjenta flere ganger i løpet av uken. Dette gjør at folk kan delta på det tidspunktet som passer dem best, og de kan stille de spørsmålene de måtte ha. Formålet er å gjøre sikkerhet så tilgjengelig som mulig og svare på de spørsmålene folk måtte ha. Dette er en fantastisk mulighet til å engasjere de ansatte, samtidig som du gir sikkerhet et vennlig ansikt. Prøv å få det meste ut av denne muligheten. Ha et åpent sinn. For at dette skal være effektivt, bør du dedikere midler til å moderere enhver sikkerhetskanal og aktivt svare på henvendelser.

Risikoer og opplæringsmaterialer

Vi har identifisert tre hovedrisikoer som du bør ta hånd om for alle som har hjemmekontor. Disse er et utgangspunkt og sannsynligvis de som vil ha høyest verdi for deg. Hver risiko nedenfor har lenker til flere midler som hjelper deg med å kommunisere og gi opplæring om temaet. Vi tilbyr flere forskjellige typer kommunikasjonsmaterialer. Dette gjør at du selv kan velge det som vil fungere best for dine ansatte. Det meste av hjelpemidlene finnes i tillegg på flere forskjellige språk. Om dette virker overveldende og du har begrenset med tid, anbefaler vi at du iverksetter bruken av de to hjelpemidlene som er oppført nedenfor.

1. Faktaskjemaet for Et trygt hjemmekontor (inkludert i distribusjonspakken).
2. Videoen Skape et cybersikret hjem (engelsk), også tilgjengelig på flere språk her

Sosialmanipulering

En av de største farene de med hjemmekontor kommer til å møte, spesielt i disse tider med store endringer og mye som haster, er sosialmanipuleringsbaserte angrep. Sosialmanipulering er et psykologisk angrep hvor angriperen lurer offeret til å gjøre en feil. Slike feil vil det være enklere å utføre i perioder med mange endringer og mye forvirrelse. Det viktigste er å lære de ansatte hva sosialmanipulering er, hvordan de gjenkjenner de vanligste tegnene på sosialmanipuleringsbaserte angrep, og hva de bør gjøre om de oppdager et slikt angrep. Pass på at du ikke retter fokus eksklusivt mot phishing-angrep via e-post, men at du også dekker andre metoder som telefonsamtaler, tekstmeldinger, sosiale medier eller falske nyheter. Du finner hjelpemidlene du trenger for å lære bort alt om temaet, i mappen Tilbehørsmaterialer for Sosialmanipulering. I tillegg finner du to SANS-videoer om sikkerhetsopplæring som du kan gi lenker til. Disse er tilgjengelige på flere språk.

- Sosialmanipulering (engelsk), også tilgjengelig på flere språk her
- Phishing (engelsk), også tilgjengelig på flere språk her

Sikre passord

Som nevnt i den årlige databruddsrapporten til Verizon er svake passord fortsatt en av primærfaktorene i sikkerhetsbrudd på verdensbasis. Det er fire viktige tiltak som gjør det enklere å håndtere farene. Disse finner du nedenfor. Du finner hjelpemidlene du trenger for å lære bort alt om temaet og de fire viktige tiltakene, i mappen Passord.

- Passordsetninger (obs: både Passordkompleksitet og Passordgyldighet er utgått).
- Bruk et unikt passord på hver av kontoene dine
- Passordverktøy

- FFV (Flerfaktorverifisering). Ofte referert til som tofaktorverifisering eller totrinnsverifisering

Oppdaterte systemer

Den tredje risikoen er å sørge for at enhver teknologi de ansatte bruker, kjører de nyeste utgavene av operativsystemer, applikasjoner og mobilapper. For de som bruker personlige enheter, kan dette medføre aktivering av automatiske oppdateringer. Du finner hjelpemidlene du trenger for å lære bort alt om temaet, i mappen Malware eller Skape et cybersikret hjem.

Andre temaer til vurdering

- **Wi-Fi**: Hvordan sikre ditt Wi-Fi-tilgangspunkt. Dette dekkes i hjelpemidlene i Skape et cybersikret hjem. Vurder også videoen Skape et cybersikret hjem (engelsk), også tilgjengelig på flere språk her.

- **VPN**: Hva er en VPN og hvorfor er dette noe du bør bruke. Vi anbefaler OUCH-nyhetsbrevet om VPN-er.

- **Jobbe ute**: Dette er for de som jobber et annet sted, men ikke på et hjemmekontor. Modulen tar for seg bl.a. kafeer, flyplassterminaler og hoteller. Vurder bruken av opplæringsvideoen Jobbe ute (engelsk), også tilgjengelig på flere språk her.

- **Barn/gjester**: For å bygge forståelse for at familie/gjester ikke skal bruke jobbrelaterte enheter, anbefales opplæringsvideoen Jobbe ute (engelsk), også tilgjengelig på flere språk her.

- **Gjenkjenne/handle**: Vil du at folk skal si ifra hvis de tror det har vært en hendelse mens de jobber på hjemmekontoret? Hva er det i så fall du vil at de skal rapportere, og når skal det rapporteres? Dette dekkes i hjelpemidlene underlagt temaet Hacket.

OUCH-nyhetsbrev

I tillegg bør du vurdere å bruke det offentlige nyhetsbrevet OUCH til å støtte opplæringsprogrammet. Hvert nyhetsbrev publiseres på over tjue språk. Oppført nedenfor er OUCH-nyhetsbrevene som vi føler best kan bidra til Et trygt hjemmekontor-initiativet. Du finner alle nyhetsbrevene i arkivet over OUCH-nyhetsbrev.

OVERSIKT

Four Steps to Staying Secure (Fire enkle sikkerhetstiltak)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Få et sikkert cyberhjem)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

SOSIALMANIPULERING

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

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

Personalized Scams (Persontilpasset svindel)
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 (Telefonsvindel)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

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

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

PASSORD

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

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

EKSTRA

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 (Smarthus-enheter)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Hurtigtips

Tips og knep du kan dele i et format som er lett å fordøye.

- De mest effektive stegene du kan ta for å sikre ditt trådløse hjemmenettverk, er å endre standardpassordet for administratorbrukeren, aktivere WPA2-kryptering og bruke et sterkt passord på det trådløse nettverket.
- Vær obs på alle enheter som kobler seg til hjemmenettverket ditt. Dette inkluderer baby-caller, spillkonsoller, TV-er, husholdningsapparater og t.o.m. bilen din. Sørg for at alle disse enhetene er beskyttet med sterke passord og/eller kjører nyeste utgave av operativsystemet sitt.
- En av de mest effektive måtene å beskytte datamaskinen din hjemme på er ved å sørge for at både operativsystemet og programmene er oppdatert med de nyeste oppdateringene. Aktiver også automatiske oppdateringer der dette lar seg gjøre.
- Til syvende og sist er sunn fornuft den beste beskyttelsen. Det kan være et angrep hvis en e-post, telefonsamtale eller melding på nett virker uvanlig, mistenkelig eller for god til å være sann.
- Sørg for at hver av kontoene dine har et separat og unikt passord. Klarer du ikke å huske på alle passordene/passordsetningene dine? Vurder bruken av et passordverktøy som lar deg lagre alle sammen på en sikker måte.

- Totrinnsverifisering er et av de beste tiltakene du iverksette for å sikre enhver konto.

Totrinnsverifisering er når du både må bruke et passord og en kode som sendes til eller opprettes i en egen applikasjon på mobilen din. Tjenester som bl.a. Gmail, Dropbox og Twitter støtter totrinnsverifisering.

- Phishing er når en angriper prøver å lure deg til å klikke på en farlig lenke eller åpne et vedlegg i en e-post. Vær mistenksom overfor enhver e-post eller melding på nett som skaper følelsen av at noe haster, har uvanlige stavefeil eller referer til deg som «Kjære kunde».

Målinger

Adferdsmålinger er vriene for slike situasjoner, siden det er vanskeligere å gjøre en vurdering av hvordan folk oppfører seg hjemme. I tillegg kan enkelte av disse ikke være jobbspesifikke (som f.eks. sikring av Wi-Fi-nettverk). Men du kan faktisk måle engasjement. Vi har oppdaget at personlige og følelsesmessige temaer som disse kan være veldig engasjerende, og vil derfor tiltrekke seg mer interesse enn andre temaer. Derfor kan målinger som dette ha en verdi.

- **Samhandling**: Hvor ofte stiller folk spørsmål, kommer med ideer eller ber om hjelp via de sikre kanalene eller forumene du har satt opp?
- **Simuleringer**: Bruk tekstmeldinger eller telefon til å utføre et simulert sosialmanipuleringsbasert angrep.

For mer omfattende målinger kan du laste ned den interaktive målingsmatrisen for sikkerhetsopplæring i den digitale nedlastingspakken MGT433.

Lisens

Distribusjonspakkens forfatter

Lance Spitzner har over 20 år med sikkerhetserfaring innen forskning på cybertrusler, sikkerhetsarkitektur og sikkerhetsopplæring. Han har vært en pioner innen svindel- og cyberetterretning med utviklingen av honeynet-løsninger og etableringen av The Honeynet Project. Som SANS-instruktør har han utviklet kursene MGT433: Sikkerhetstrening og MGT521: Sikkerhetskultur. I tillegg har Lance publisert tre bøker om sikkerhet, konsultert i over 25 land og hjulpet over 350 organisasjoner med å etablere et sikkert forsvar mot de mange menneskelige risikoene der ute. Lance har ofte presentasjoner, tweeter jevnlig (@lspitzner) og jobber på et stort antall av fellesskapets sikkerhetsprosjekter. Før han ble engasjert i informasjonssikkerhet, tjenestegjorde Mr. Spitzner som offiser i den amerikanske hærens Rapid Deployment Force, og han fikk sin MBA ved The University of Illinois.

Om SANS Institute

SANS Institute ble etablert i 1989 som en hybridorganisasjon for forskning og undervisning. SANS er den mest troverdige og utvilsomt største leverandøren av cybersikkerhetsopplæring og sertifikater til profesjonelle i regjeringer og kommersielle institusjoner på verdensbasis. De anerkjente SANS-instruktørene underviser over 60 forskjellige kurs ved over 200 cybersikkerhetstrening-arrangementer og på nett. GIAC, en av SANS Institutes partnere, godkjenner en utøvers kvalifikasjoner via over 35 tekniske sertifikater innen cybersikkerhet. SANS Technology Institute, et regionsbasert sertifisert og uavhengig datterselskap, tilbyr mastergrader innen cybersikkerhet. SANS tilbyr en rekke gratis midler til InfoSec-fellesskapet, som bl.a. konsensusprosjekter, forskningsrapporter og nyhetsbrev; det styrer også Internetts systemer for tidlig varsel – Internet Storm Center. I hjertet av SANS finner man mange sikkerhetsutøvere som representerer forskjellige globale organisasjoner, fra bedrifter til universiteter, som samarbeider for å hjelpe hele informasjonssikkerhetsfellesskapet. (https://www.sans.org)