Leveret af:

MetaCompliance®

Cybersikkerheds-awareness

for dummies®

Ændr medarbejdernes sikkerhedskultur

Opbyg en mere sikkerhedsbevidst arbejdsstyrke

Følg denne playbook for cybersikkerheds-kampagner

Robert O'Brien

Geraldine Strawbridge

MetaCompliance Special Edition

Om MetaCompliance

MetaCompliance har over 14 års domæneekspertise inden for awareness-træning af medarbejdere om sikkerhed. Organisationen arbejder med kunder på tværs af alle brancher og hjælper organisationer med at beskytte deres data, træne medarbejdere og håndtere omdømme- og lovgivningsmæssige risici. I det tidsrum er den lovgivningsmæssige udfordring for organisationer vokset i takt med det trusselsbillede, der er knyttet til deres digitale aktiver.

Organisationen er førende inden for det "menneskelige aspekt" af cybersikkerhed og compliance. MetaCompliance-teamet arbejder hver dag med kunder i den offentlige og den private sektor for at indføre best practice-kampagner for at fremme medarbejdernes sikkerheds-awareness, få dem engageret og ændre deres adfærd.

Den grafisk tiltalende SaaS-platform giver kunder en integreret, flersproget pakke af funktioner, der omfatter simuleret phishing, cybersikkerhed og compliance e-learning, politikstyring, sikring af privatlivets fred og hændelsesstyring. Organisationer opnår større lovgivningsmæssig beskyttelse gennem en "one stop shop" til håndtering af privatlivets fred, compliance og cybersikkerheds-projekter, som gør det nemmere for medarbejdere at opfylde deres compliance-forpligtelser.

MetaCompliance's innovative MyCompliance cloud-arkitektur er bygget oven på Microsoft Azure-platformen og således udgør en global løsning for hele organisationen. MetaCompliance er baseret i London, Storbritannien, Dublin, Irland og Atlanta, GA, og har en voksende kundebase i både den offentlige og den private sektor.

Cyber-sikkerheds-awareness

for dummies®

Cyber-sikkerheds-awareness

MetaCompliance Special Edition

af Robert O'Brien, ekspert i cybersikkerhed og compliance
Geraldine Strawbridge, cybersikkerheds-redaktør

for dummies®

Cybersikkerheds-awareness For Dummies®, MetaCompliance Special Edition

Udgivet af: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate

Chichester, West Sussex, Storbritannien, www.wiley.com

Hjemsted

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, Storbritannien

Generelle oplysninger om vores andre produkter og tjenester, eller hvordan der fremstilles en brugertilpasset *For Dummies*-bog til din virksomhed eller organisation fås ved at kontakte vores Business Development Department i USA på 877-409-4177, skrive til info@dummies.biz eller besøge www.wiley.com/go/custompub. Oplysninger om licens til *For Dummies*-brandet for produkter eller tjenester fås ved at kontakte BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-89933-4 (pbk); ISBN 978-1-119-89934-1 (ebk)

Trykt i Storbritannien

10 9 8 7 6 5 4 3 2 1

Indholdsfortegnelse

Indledning

Inden for det sidste årti har cybersikkerhedslandskabet ændret sig dramatisk. Ifølge Cybersecurity Ventures forventes de globale omkostninger til cyberkriminalitet i 2021 at nå 6 milliarder dollars, hvilket gør sektoren mere rentabel end hele den globale handel med ulovlige stoffer. Organisationer af enhver størrelse og i enhver industri er blevet potentielle mål for cyberkriminelle. Nye trusler dukker op hele tiden, og organisationer kan ikke længere blot regne med deres teknologiske forsvar for at holde sig sikre.

Cyberkriminelle går efter det svageste punkt i en organisations forsvar, og det er i rigtig mange tilfælde dine medarbejdere. Hele 90 procent af alle databrud kan tilskrives menneskelige fejl, hvilket er grunden til, at organisationer er nødt til at have et program for cybersikkerheds-awareness, der gør alle medarbejdere i stand til at forstå og påtage sig den vigtige rolle, de spiller med hensyn til at beskytte følsomme organisationsdata.

Om denne bog

Cybersikkerheds-awareness For Dummies, MetaCompliance Special Edition, består af seks kapitler, der gennemgår det moderne cybersikkerhedslandskab (kapitel 1), behovet for cybersikkerheds-awareness (kapitel 2), anvendelse af cybersikkerhedskampagner til at opnå forandringer (kapitel 3), integration af politikstyring i sikkerheds-awareness-programmer (kapitel 4), de forskellige måder at udvikle en bedste praksis i en cyber-awareness-strategi (kapitel 5) og bedste praksis inden for sikkerheds-awareness (kapitel 6).

Hvert kapitel taler for sig selv, så hvis du ser et emne, der vækker din interesse, er du velkommen til at springe frem til det pågældende kapitel. Du kan læse denne bog i den rækkefølge, der passer dig bedst (vi anbefaler nu ikke at læse den på hovedet eller baglæns).

Tåbelige antagelser

Da vi skrev denne bog, antog vi, at du er en cybersikkerheds- eller it-professionel, såsom en informationschef (CIO), teknologichef (CTO), informationssikkerhedschef (CISO), privatlivschef (CPO),

databeskyttelsesansvarlig, it-direktør, it-chef, personalechef, uddannelseschef, forandringsleder eller endog en seniorleder.

Hvis nogle af disse antagelser beskriver dig, så er denne bog til dig. Hvis ingen af disse antagelser beskriver dig, skal du bare fortsætte med at læse alligevel. Når du er færdig, vil du have en øget cybersikkerheds-awareness.

Ikoner anvendt i denne bog

Vi bruger af og til særlige ikoner til at gøre opmærksom på vigtige oplysninger. Her er, hvad du kan forvente:

HUSK

Dette ikon påpeger vigtig information, som du bør gemme i din ikke-flygtige hukommelse, eller i din grå hjernemasse.

TIP

Vi håber, at du værdsætter disse nyttige informationsbidder.

ADVARSEL

Disse notifikationer giver praktiske råd for at hjælpe dig med at undgå potentielt dyre eller frustrerende fejltagelser.

Ud over denne bog

Der er grænser for, hvor meget vi kan dække på disse få sider, så hvis du har nået slutningen af denne bog og tænker: 'Det var dog en fantastisk bog, hvor kan jeg lære mere?', kan du kigge på `www.metacompliance.com`.

I DETTE KAPITEL

- **Undersøgelse af det trusselslandskab, som er under udvikling**
- **Kendskab til, hvad en cyberkriminel er ude efter**
- **Indarbejdelse af sikkerheds-awareness i den digitale transformation**
- **Fastsættelse af sikkerhedsrammer og databeskyttelse**
- **Indblik i lovgivningskrav**

Kapitel 1
Indsigt i det moderne cybersikkerheds-landskab

I dette kapitel vil du få indblik i, hvordan avancerede cybertrusler såvel som højere niveauer af it-governance, databeskyttelses-lovgivning og "security by design" har øget behovet for opmærksomhed på cybersikkerhed i den moderne organisation.

Et kig på cybertrusler mod mennesker i organisationer

Cyberkriminalitet har udviklet sig til en af de største trusler, der påvirker organisationer over hele verden. Angrebsvektorer er under forandring, og cyberkriminelle bruger en række forskellige taktikker til at få adgang til værdifulde organisationsdata.

Hvis organisationer vil minimere risikoen for et sikkerhedsbrud, skal de sætte sig ind i de forskellige typer cybertrusler, der kan bruges mod dem:

- **Phishing:** *Phishing* er en type social-engineering-angreb, hvor de kriminelle forsøger at narre ofre til at afsløre følsomme oplysninger eller installere malware. Cyberkriminelle bruger e-mail, sociale medier, telefonopkald og sms'er til at udgive sig for at være en betroet person for at manipulere deres offer til at udføre en bestemt handling. Det kan indebære, at de klikker på et ondsindet link, downloader en vedhæftet fil, besøger et forfalsket websted, eller at de cyberkriminelle forsætligt afslører følsomme oplysninger. Oplysningerne kan derefter anvendes til at få adgang til personlige konti eller begå identitetstyveri.
- **Malware:** *Malware* er en type ondsindet software, der er designet til at beskadige eller få adgang til et computersystem uden brugerens viden. Eksempler på malware omfatter vira, orme, trojanske heste, spyware, adware og ransomware. Malware installeres typisk på en computer, når en bruger klikker på et link, downloader en ondsindet vedhæftet fil eller åbner et uautoriseret softwareprogram. Når først malwaren er installeret, kan den stjæle, slette eller kryptere følsomme data. Den kan også blokere for centrale databehandlingsfunktioner, så systemet bliver ubrugeligt.
- **Insidertrussel:** En *insidertrussel* er en sikkerhedshændelse, der stammer indefra organisationen i stedet for fra en ekstern kilde. Det kan være en nuværende eller tidligere medarbejder, en entreprenør, en tredjepartsleverandør eller en hvilken som helst anden medarbejder, der har adgang til organisationens data og computersystemer. Insiderangreb kan være særligt farlige, fordi insidere, i modsætning til eksterne aktører, der forsøger at infiltrere et netværk, typisk har lov til at anvende en organisations computersystemer.
- **Forsyningskædeangreb:** Et forsyningskædeangreb, også betegnet et *tredjepartsangreb*, går ud på at skade en organisation ved at udnytte sårbarheder i dens forsyningskædenetværk. *Forsyningskædeangreb* har potentialet til at infiltrere et helt netværk gennem en enkelt kompromitterende handling. De kan være sværere at detektere end traditionelle malwareangreb.

ADVARSEL

Menneskets natur er en alvorlig sikkerhedsrisiko, og cyberkriminelle ved, hvordan de udnytter den.

Indsigt i cyberkriminelles angrebsprofiler og motivationer

Populærkulturen har skildret hackere på flere forskellige måder, ofte som en hætteklædt figur i en kælder eller en utilfreds teenager, der vil rette op på verden. Et af de mere bemærkelsesværdige Hollywood-eksempler er den fiktive hacker Lisbeth Salander, der er hovedpersonen i *The Girl with The Dragon Tattoo* (Millennium Trilogy) af Stieg Larsson. Første gang karakteren introduceres, anvender hun sine hackerfærdigheder på vegne af et privat sikkerhedsfirma. Men efterhånden som plottet bliver mere indviklet, bliver hendes hacking-evner motiveret af hævn, hvilket i sidste ende giver hende mulighed for at udføre et vovet økonomisk bedrageri mod en af hovedskurkene i historien. Denne historie illustrerer det faktum, at folk, der er beskæftiget med cyberkriminalitet, motiveres på vidt forskellig vis.

Det er vigtigt for din organisation at kende hackeres motivationer for at forstå, hvordan de håndteres. Følgende er nogle af årsagerne til, at hackere gør det, de gør:

- **Økonomisk kriminalitet:** Penge er den største motivationsfaktor for mange kriminelle aktiviteter, og det samme gælder cyberkriminalitet. Det er tyveri i den digitale tidsalder, og det er meget nemmere at gennemføre end at gå ind i en bank med en pistol. På trods af de meget omtalte hacks hos flere store organisationer fokuseres der i stigende grad på små og mellemstore organisationer, hvis sikkerhedspraksis er mindre solid. Virkeligheden er, at det er langt mere lukrativt for en hacker at angribe flere mindre organisationer frem for en Fortune 100-virksomhed, der har investeret millioner i at styrke sit teknologiske forsvar.
- **Spionage:** Hackere bruger ofte cyberspionage til at stjæle klassificerede oplysninger, intellektuel ejendom eller forretningshemmeligheder. Spionage udgør i dag en betydelig trussel mod alle organisationer, hvad enten det drejer sig om et angreb på en nationalstat eller organisationsspionage.

  Gentagne brud har vist, hvor aktive hackere er blevet inden for de to nøgleinformationsområder, der motiverer dem — politik og produktionsvirksomheder.

HUSK

Statsstøttede organisationer udviser også konstant opmærksomhed over for kritiske infrastrukturer som transport, vandforsyning, telekommunikation og energiforsyning. Bevæbningen af malware fra udenlandske statslige organers side vil være en kæmpe udfordring for alle undtagen de største organisationer med de bedste ressourcer, og det overraskende faktum er, at de primære formidlere af disse angrebsvektorer er mennesker. Social manipulation og udnyttelse af utilstrækkelig sikkerhedspraksis er de første områder, en cyberkriminel vil forsøge at udnytte. Det er derfor bydende nødvendigt, at organisationer mobiliserer deres egen arbejdsstyrke for at kunne forsvare sig mod disse trusler. Indførelsen af et egnet awareness-program for medarbejderne er et grundlæggende skridt, når du skal forsvare din organisation.

- **Sjov:** Mange hackere er motiveret af den spænding eller det "kick", de føler, når de infiltrerer en organisations computersystemer. Ved dette års Pwn2Own-konkurrence om etisk hacking stillede arrangørerne f.eks. en Tesla Model 3 til rådighed, som deltagerne kunne prøve at hacke sig ind i. I løbet af en dag afslørede to hackere en sikkerhedsfejl, der gjorde dem i stand til at hacke sig ind i bilens interne webbrowser. I stedet for at blive retsforfulgt gik duoen derfra med deres egen Tesla Model 3, 375.000 dollars i præmiepenge og, hvad der var allervigtigst, deres ligesindedes anerkendelse, hvilket er meget eftertragtet i hackermiljøet.
- **Hacktivisme:** *Hacktivisme* går ud på at hacke et computersystem eller netværk til politisk eller socialt motiverede formål. Der har og vil altid være mennesker, der engagerer sig i aktivisme for en bestemt sag, der går regeringsmagten imod. Det nye er den allestedsnærværende teknologi.

  Teknologien er blevet bevæbnet og anvendes i stigende grad til at fremme ideologiske mål. En af grundene til denne vækst er, at det er meget billigere at iværksætte et cyberangreb end en militæraktion.
- **Tyveri af ressourcer:** Det er blevet en rentabel forretning at udnytte offentlighedens computerressourcer til at udvinde bitcoins. Udvinding af bitcoins handler om elektricitet og processorkraft, og hackere udnytter enhver chance, de har, for at stjæle disse ressourcer. Selv multinationale organisationer som Starbucks er blevet ramt. En butik i Buenos Aires opdagede f.eks. for nylig, at dens wi-fi var blevet hacket, og at

svindlere brugte den til at mine bitcoins på intetanende kunders enheder.

- **Andet:** Denne kategori omfatter insidertrusler, utilsigtede datalækager, fejlkonfigurationer, brugerfejl og en række andre trusler, der ikke er relateret til hacking fra tredjeparter. De metoder, som med størst sandsynlighed anvendes til at kompromittere en organisation, er upatchet software og social engineering. Disse trusler udgør den største risiko for de fleste organisationer.

Sikkerhedsrammer og databeskyttelse

De vigtigste spørgsmål, som du skal stille din organisation, er følgende: ***Hvad er den bedste måde at etablere et sikkerhedsstyringssystem i min organisation på, og hvad består det af?***

Et svar er ISO27001-standarden, som opstiller en best practice-tilgang til informationssikkerhedsstyring.

ISO27001 – Den globale cybersikkerhedsstandard

Beskyttelse af personlige oplysninger og databeskyttelse er vigtige initiativer for moderne organisationer. Beredskabs- og vedligeholdelsesaktiviteterne for beskyttelse af personlige oplysninger er en betydelig opgave for enhver organisation, så det er vigtigt, at medarbejderne får den nødvendige tid og uddannelse til at forstå de daglige forpligtelser i forbindelse med beskyttelse af personlige oplysninger i deres arbejde.

ISO27001 er en ægte global sikkerhedsstandard, og det er samtidig den eneste, der er underlagt ekstern revision. Det gør organisationer i stand til at have en ensartet måde at dokumentere, at de anvender den bedste praksis i deres informationssikkerhedsprocesser. Mange af fordelene ved ISO27001 hænger sammen med, at certifikatet siger noget om organisationens beredskab, hvis noget skulle gå galt. Et ISO27001-certifikat er blevet et stadigt mere værdifuldt forretningsaktiv i forbindelse med, at kunder ser nærmere på deres forsyningskæde for at sikre sig, at der bliver taget hånd om cyberrisikoen.

Udnyttelse af fordelene ved ISO27001

Den indsats og ledelsesinvolvering, der er nødvendig for at opnå ISO27001-akkreditering, sikrer, at organisationen bliver mere moden, hvad angår cybersikkerhed. Andre fordele omfatter:

- Øget forretningsmæssig modstandsdygtighed og beskyttelse mod sikkerhedsfejl
- Forbedret kundetillid
- Øget pålidelighed af og sikkerhed i centrale systemer og informationsaktiver
- Øget fokus på risiko og dens indflydelse på organisationen

For at kunne opnå ISO27001-certificering skal der findes en passende ordning til at fremme opmærksomheden hos medarbejderne. Paragraf 7.2, 7.3 og 7.4 i ISO IEC 27001 handler om awareness og forståelse af det informationssikkerhedsstyringssystem (ISMS), der certificeres. Generel cybersikkerheds-awareness- træning opfylder ikke nødvendigvis kravene til overholdelse af ISO27001, særligt fordi alle organisationers ISMS er unikt med hensyn til det sæt risici og systemer, der ligger til grund for deres drift.

Det er afgørende, at medarbejderne gøres opmærksomme på, hvordan sikkerhedsprocesserne fungerer i deres organisationer, hvilket normalt involverer brugertilpasset oplæring i organisationens ISMS. En oplysningskampagne om bedste praksis vil dække vigtige cybertrusler fra phishing til fysisk sikkerhed og også understøtte deltagelse og forståelse af ISO27001-initiativet. Der kræves også specifik træning i forbindelse med organisationens ISMS, hvilket kan være så simpelt som et webinar for hele organisationen for at give indsigt i, hvordan det fungerer.

TIP

Ved at sikre, at dit ISMS ligger til grund for din cyberoplysningskampagne, undgår du brugertræthed ved at fokusere på de specifikke cybertrusler, der er relevante for din organisation og dine medarbejdere. Den respons, der er indbygget i dit ISMS, vil udvikle sig i trit med dit trusselslandskab. Det er vigtigt, at du involverer dine medarbejdere og, at de holdes underrettet om eventuelle ændringer undervejs.

Et andet højt respekteret framework, der er meget anvendt til at standardisere processer, reducere risici og forbedre cybersikkerhedsoperationer i organisationer over hele verden, er NIST Cyber Security Framework (se sidepanel).

NIST-FRAMEWORK FOR CYBERSIKKERHED

Det amerikanske National Institute of Standards and Technology (NIST) oprettede Cyber Security Framework (CSF) for at give organisationer vejledning i, hvordan de forebygger, opdager og reagerer på cyberhændelser. Dette internationalt anerkendte framework skitserer et sæt bedste praksisser, standarder og anbefalinger, der hjælper en organisation med at forbedre sin cybersikkerhedsstilling.

NIST CFS blev oprindeligt udformet med henblik på at forbedre kritiske infrastrukturtjenester, men er siden blevet indført i en række andre brancher og har hjulpet organisationer med at blive mere proaktive omkring risikostyring.

Dette framework er opdelt i følgende tre dele:

- **Framework Core** omfatter en række aktiviteter, der har til formål at opnå nogle bestemte cybersikkerhedsresultater. Framework Core er baseret på fem funktioner:
  - **Identificer:** Udvikle den organisatoriske forståelse omkring håndtering af cybersikkerhedsrisici for systemer, aktiver, data og kapaciteter.
  - **Beskyt:** Udvikle og gennemføre passende sikkerhedsforanstaltninger for at sikre levering af kritiske infrastrukturtjenester.
  - **Registrer:** Udvikle og gennemføre passende aktiviteter for at kunne registrere, når der forekommer en cybersikkerhedshændelse.
  - **Reager:** Udvikle og gennemføre passende aktiviteter for at kunne træffe de nødvendige foranstaltninger som reaktion på en registreret cybersikkerhedshændelse.
  - **Genopret:** Udvikle og gennemføre de relevante aktiviteter for at have robuste beredskabsplaner og for at genoprette eventuelle kapaciteter eller tjenester, der blev svækket på grund af en cybersikkerhedshændelse.

Disse funktioner er yderligere underopdelt i 22 kategorier og 98 underkategorier.

- **Implementeringsniveauer for dette framework:** Giver overblik over, hvordan organisationer anskuer risici, og hvilke processer, der kan indføres for at mindske disse.
- **Framework profil:** Beskriver de ønskede resultater ud fra kategorierne og underkategorierne.

Vigtigheden af opmærksomhed hos medarbejderne i digitale transformationsprojekter

Digitale transformationsprojekter er spændende initiativer i moderne organisationer. De giver organisationen mulighed for at udnytte nye teknologier og indføre produkter, der reducerer omkostningerne og øger omsætningen.

Digitale transformationsprojekter er typisk ambitiøse strategier til at ændre den måde, en organisation driver forretning på, ved hjælp af digital teknologi.

Disse change management projekter kræver betydelige investeringer i medarbejderkommunikation. Denne kommunikation har til formål at opnå støtte og engagement blandt medarbejderne. I disse initiativer fokuseres der ofte for lidt på den risiko, der er forbundet med ikke at udvise tilstrækkelig forsigtighed og omhu, hvad angår IT-sikkerhed og overholdelse af reglerne. Det er imidlertid lige det, der skal til for at finde en balance mellem transformation for enhver pris og opnåelse af passende kontrol og sikkerhedsforanstaltninger. Se kapitel 3 for at gå mere i dybden om, hvordan man kommunikerer med medarbejderne om dette.

I DETTE KAPITEL

- Forståelse af risikoprofilen
- Udfordringer forbundet med at gøre medarbejderne mere aware
- Opmærksomhed over for risici og bevarelse af relevansen af cybersikkerhed

Kapitel 2
Etablering af behovet for cybersikkerheds-awareness

Meget få vejledninger eller strategiplaner giver de nødvendige instruktioner i, hvordan man planlægger, udvikler og implementerer et awareness-program for cybersikkerhed. En af grundene er, at informationssikkerhedsindustrien har været fuldstændigt hengivet til brugen af traditionel teknologi såsom firewalls og anti-malware løsninger. Disse teknologiske forsvarsmekanismer har givet en falsk fornemmelse af, at sikkerheden er på plads.

På trods af denne store investering i teknisk sikkerhed har der været (og er der stadig) en form for "plausibel benægtelse" af, at en enkelt medarbejders handlinger helt kan omgå disse kontrolforanstaltninger.

Parallelt med de stadig mere almindeligt forekommende databrud hos velrenommerede organisationer er der en global erkendelse af, at konsekvenserne af disse hændelser er for alvorlige til at ignorere. Spørgsmålet er således kommet på dagsordenen i bestyrelser hos de fleste moderne organisationer. Tilsynsmyndigheder bruger desuden i stigende grad sanktioner og bøder til at fremme compliance for nye databeskyttelsesforordninger. Disse og andre

makropåvirkninger har betydet, at der er behov for en gennemgribende ændring i, hvordan medarbejderne arbejder, og hvordan de minimerer risikoen.

Når direktionen anerkender vigtigheden af cybersikkerhedsrisici som et legitimt forretningsansvar, har organisationen taget et vigtigt skridt i retning af større modenhed. Den vigtigste begrænsning af ethvert awareness-projekt om cybersikkerhed er, i hvilket omfang organisationens ledelse anerkender, at cyberrisici skal tildeles samme betydning og ressourcer som finansielle risici. Kapitel 5 fortæller mere om den øverste ledelses støtte til din kampagne.

Dette kapitel forklarer i nærmere detaljer, hvad du kan gøre for at sikre, at din organisation er opmærksom på cybersikkerhed.

Forståelse af risikoprofilen

Hvad ville der ske, hvis din organisation blev hacket? Hvor stor er sandsynligheden, og hvad ville indvirkningen være? For at forstå svarene på disse spørgsmål skal du sætte dig ind i den unikke risikoprofil, din organisation står over for. Det sårbarhedsniveau, som din organisation står overfor, bestemmes af, i hvor høj grad cybertrusler er relevante for din organisation. At få indblik i disse sårbarheder og udarbejde afhjælpningsplaner repræsenterer en bedste praksis for at begrænse, i hvor høj grad din organisation udsættes for cybersikkerhedsrisici. Dette er især relevant, når det vedrører dine medarbejdere og dine forsyningskæder, fordi de er almindelige angrebsveje for ondsindede tredjeparter.

Følgende afsnit indeholder konkrete skridt, som din organisation kan benytte til at reducere risikoen.

Gennemførelse af en risiko-awareness-kampagne

Det er vigtigt at fokusere på medarbejderadfærd i forbindelse med cybersikkerhed og databeskyttelse. En awareness-kampagne går ud på at afhjælpe de risici, der er knyttet til det menneskelige aspekt af cybersikkerhed.

Sikkerheds-awareness-kampagner, der udelukkende går ud på hurtigst muligt at levere cybersikkerhedstræning til medarbejderne, har dog haft begrænset succes. En virkelig adfærdsændring

kræver løbende træning kombineret med en stor indsats på organisationens vegne. Det tager også tid, for folk har en naturlig tendens til at modsætte sig forandringer.

Identifikation af dine medarbejderes forståelse af risici

Der er forskellige måder, hvorpå din organisation hurtigt kan bestemme medarbejdernes forståelse af sikkerhedsrisici. De omfatter følgende:

- **Send alle medarbejdere en simuleret phishing-email og se, hvor mange medarbejdere der falder for den.** Vær særlig opmærksom på de brugere, der indtastede legitimationsoplysninger eller reelle oplysninger efter at have modtaget en prompt fra en phishing-e-mail. Denne klikrate vil give dig et udgangspunkt.
- **Lav en hurtig analyse af hændelser i den forløbne 12-måneders periode.** Er der tilsvarende hændelser, der ligner en tendens eller gentagelse? Prioriter dit awareness-program omkring disse risici.

Disse oplysninger har også stor betydning, når det forklares for medarbejderne, hvorfor cybersikkerheds-træning er så vigtig. Eksempel: "I det forgangne år mistede denne organisation 20 bærbare computere. Få en større forståelse af bedste praksis inden for udstyrsadministration ved at tage den vedhæftede eLearning."

Fokuser træningen på dem, der har brug for den

Cybersikkerheds-awareness med kontekst og segmentering har øget effektiviteten. For eksempel er det ineffektivt at træne alle medarbejdere i, hvordan man fører kontrol med bærbare computere og udstyr, hvis kun et lille antal medarbejdere har en bærbar computer. Kun de medarbejdere, der har udstyret, har brug for den slags træning. At lade alle medarbejderne gennemgå den samme sikkerhedstræning virker mod hensigten. Din organisation bør så vidt muligt tilpasse awareness-træning til en medarbejders særlige rolle og risikoprofil.

Awareness-kampagner om cybersikkerhed har større effekt, hvis de omhandler forståelige risici, og når folk kan identificere de

konsekvenser i den virkelige verden, som uagtsom cybersikkerhedspraksis giver anledning til.


TIP

Organiser informationssikkerhedsrisici omkring mennesker og teknologiaktiver. Sidstnævnte vedrører en organisations kritiske forretningssystemer og de data, der ligger på disse systemer. Fra et awareness-synspunkt er det vigtigt at sikre, at de rigtige mennesker får de rigtige budskaber på det rigtige tidspunkt. Vær også opmærksom på, at forskellige brugere og forskellige data har større betydning med hensyn til risiko.

Økonomiafdelingen har f.eks. større risiko for et cyberangreb end en medarbejder i cafeteriet. Vægtningskonceptet er vigtigt i forbindelse med udformningen af en awareness-kampagne, fordi det hjælper dig med at fokusere på dine højrisikomedarbejdere i stedet for samtlige medarbejdere.

Forståelse af, hvem der har brug for mere træning

Det er yderst effektivt at bruge tid på at formulere målrettet kommunikation eller give relevant træning til disse medarbejdergrupper, især hvis det foregår på et sprog, som de er fortrolige med.

Det tager tid at identificere sårbare medarbejdergrupper. Men de tre vigtigste grupper, der har brug for yderligere risikotræning, er følgende:

- **Økonomiafdelingen:** Denne afdeling er normalt den mest udsatte afdeling, der rammes i en organisation, fordi den har kontrol med pengene.
- **Teknisk priviligerede brugere:** Disse brugere rammes, fordi de kan bruges til at eskalere et cyberangreb på grund af deres privilegerede adgang til sikre systemer.
- **Seniorledere i organisationen:** Den øverste ledelse rammes, fordi de har bemyndigelse, der kan bruges til at eskalere et cyberbrud.

Glem ikke hele din forsyningskæde og dit partnernetværk. Det er også en stor del af din risikoprofil. I kapitel 3 ses der nærmere på, hvordan du kan identificere kritiske tredjeparter, den risiko, de udgør i en moderne agil organisation, og hvordan du kan inddrage dem i dine cybersikkerhedsaktiviteter.

Varigheden af medarbejdernes ansættelse i organisationen har desuden betydning for, hvor nemt det er at ændre deres adfærd. Nye brugere kan bedre acceptere politikker og lære nye arbejdsmetoder, fordi de har en mere fleksibel tankegang. Medarbejdere med længere anciennitet kan dog være mere problematiske, når det gælder om at lære nye metoder.

Det er også vigtigt at bestemme, hvor mange almindeligt anvendte regionale sprog der findes i din organisation, når du skal udarbejde din risikoprofil. Flere sprog vil ikke blot gøre det vanskeligere at indføre et awareness-program til medarbejderne, men det øger også det antal trusselsvektorer, som din organisation skal håndtere.

En organisation, der arbejder i Brasilien, skal f.eks. bekymre sig om phishing-e-mails på portugisisk såvel som engelsk. Det er vigtigt at identificere dine vigtigste kulturelle og sproglige målgrupper, hvis du skal gøre sikkerheds-awareness-programmet relevant for medarbejderne.

Prioritering af sikkerhedsrisici

I mange organisationer har man ikke prioriteret sikkerheden over for medarbejderne på samme måde som den finansielle risiko. Sikkerhed blev ikke betragtet som en nødvendig del af den almindelige forretningsgang, og brugerne har derfor udviklet dårlige vaner gennem en årrække. Det har gjort det sværere at gennemføre en sikkerheds-awareness-kampagne. Kampagnen skal oplyse brugerne om sikkerhed, men den skal også overvinde dårlige vaner, der har hobet sig op med tiden. Din organisation kan kun overbevise dine medarbejdere ved at være konsekvent og gentage dine kampagnebudskaber.

Brug af gamle systemer, der er svære at lave om på, bruges ofte som begrundelse for, at adfærdsændringer ikke er nødvendige. Du har muligvis hørt sætningen: "I vores system gør man det på den måde, så der er ingen grund til at prøve at lave om på det." Det er ikke nemt at overvinde denne tankegang.

Sikkerhedsudfordringer i forbindelse med ældre systemer kan give en følelse af håbløshed i den måde, man anskuer sikkerhedstrusler på. Hvis et adgangskontrolsystem f.eks. administreres på et udgået Windows-operativsystem, er det forståeligt, at det måske ikke er den bedste investering at udskifte alle låse i et system, der ellers fungerer perfekt, med elektroniske låse.

Alle sådanne gamle systemer skal imidlertid udbedres hurtigst muligt. Medarbejderne har brug for at vide, at organisationen har identificeret disse udfordringer og aktivt har taget hånd om dem. Selv om disse aktiviteter er baggrundsaktiviteter og ligger uden for rammerne af et sikkerhedsprogram for medarbejdere, er det vigtigt at gøre fremskridt på disse områder for at sikre integriteten af en awareness-kampagne til medarbejderne.

Virkeliggørelse af cybersikkerhed for folk i din organisation

Programmer for cybersikkerheds-awareness vil sandsynligvis ikke vække begejstring hos medarbejdere eller ledelse.

Når du overvejer at sammensætte et program til at forbedre medarbejdernes opmærksomhed omkring informationssikkerhed, skal du huske på, at de fleste bruger meget lidt eller slet ingen tid på at tænke over dette spørgsmål. Cybersikkerhed er et tungt emne, der er svært at gøre interessant. Det er imidlertid organisationens ansvar at gøre sikkerhedskommunikationen fordøjelig og måske endda interessant for medarbejderne.

En af de vigtigste mål for succes er at få brugerne til at deltage i dine programmer for cyber-awareness. Hvis du f.eks. sender en risikovurdering eller et stykke eLearning ud, og kun 50 % af dine medarbejdere deltager ved at udfylde indholdet, sidder du med et stort problem. En væsentlig del af brugerne er mentalt fraværende. Hvad der er endnu vigtigere, din organisation kan ikke påvise, at den overholder cybersikkerhedsreglerne. Det er også sandsynligt, at "problembørnene" i dit cybersikkerhedsprogram indgår i de 50 procent af medarbejderne, som ikke reagerede på kommunikationen, og således ikke fuldførte programmet.

Din organisation kan reagere på tre måder:

- Ledelsen kan ignorere de personer, der ikke har deltaget, og håbe på det bedste. Denne fremgangsmåde vil muligvis være populær, men den er i sidste ende dømt til at fejle. Tilsynsmyndighederne vil forvente, at du kan dokumentere din indsats for at få disse brugere med i awareness-programmet.

- Ledelsen kan begynde den langtrukne proces med at slå ned på brugere, der ikke har opfyldt deres forpligtelser med hensyn til cyber-awareness. Det er en arbejdskrævende indsats, som blot vil irritere ledelsen og sende informationssikkerheden til den organisatoriske pendant til den sibiriske front.
- Teknologiløsninger kan lokke, irritere, chikanere, skubbe på og i sidste ende få brugerne til at færdiggøre sikkerhedsopgaven.

Kampagnen for cyber-awareness skal i sidste ende engagere brugeren, hvilket indebærer brug af god mediekommunikation, grafik og eLearning. Så få den bedste eLearning-kvalitet, du har råd til, få dækket de vigtigste sprog i din organisation, og giv brugerne mulighed for selv at administrere det sprog, som de helst vil konsumere indholdet på.

Håndtering af risici og opnåelse af relevans

Næsten alle organisationer har en eller anden form for digitalt transformationsprojekt. Samtidig med, at der forskes i større effektivitet og indtægtsmuligheder, fremkommer der nye forretningsmodeller på grund af markedsændringer og indførelse af teknologier som cloud, datastyring og mobil teknologi. Disse projekter er højt profilerede i alle organisationer og har typisk bestyrelsens og direktionens opmærksomhed og støtte.

Databeskyttelseslovgivning som f.eks. den generelle forordning om databeskyttelse (GDPR) har sat privacy-by-design og security-by-design i centrum for nye digitale initiativer. I nogle regioner skal organisationer foretage en konsekvensanalyse for at vurdere, hvilke konsekvenser et nyt system eller en ny proces eller forretningsmodel har for databeskyttelsen. Databeskyttelses- og informationssikkerhedseksperter spiller en meget vigtig rolle med hensyn til at sikre, at de digitale transformationsteams er opmærksomme på dette krav, og for at sikre, at det nye system eller den nye tilgang omfatter passende kontrolforanstaltninger og medarbejderkommunikation.

HUSK

Når du inkluderer kommunikation vedrørende et digitalt transformationsprojekt som en del af dit årlige awareness-projekt for cybersikkerhed, bliver det mere relevant for organisationen og hjælper med at øge sikkerhedsprofilen hos ledelsen. Ved at være på forkant med disse nye digitale projekter kan medarbejderne desuden se informationssikkerhed som en katalysator i stedet for en hindring, der uundgåeligt følger efter den sene indførelse af sikkerhedskontrol i forbindelse med denne type initiativer.

Når den øverste ledelse overvejer gyldigheden af et digitalt transformationsprojekt, betyder det, at de allerede er i gang med at vurdere diverse forretningsrisici og potentielle fordele. Udfordringen er at angribe projektet fra et risikoperspektiv og forsøge at sikre, at sikkerheds- og databeskyttelsesrisici prioriteres på samme måde som finansiel og anden forretningsmæssig eksponering. Digitale transformationsprojekter giver mulighed for at øge cybersikkerheds-awareness i forbindelse med et meget større initiativ på tværs af organisationen.

I DETTE KAPITEL

- **Brug af effektiv kommunikation**
- **Modarbejdelse af apati**
- **Stol på, at medarbejdere i din organisation kan hjælpe med at få budskabet ud**
- **Overvejelse af relationer med tredjeparter**

Kapitel 3
Ændring af organisationskulturen med awareness-kampagner om cybersikkerhed

Din organisation kan være fristet til at få travlt med dets sikkerheds-awareness-program og udsende eLearning og simulerede phishing-angreb til brugere. Disse tilgange er imidlertid dømt til at mislykkes, medmindre de tager hensyn til det vigtigste mål – at ændre folks adfærd i forhold til cyberrisici. Når du begynder at overveje idéen om at ændre adfærd, befinder du dig inden for change management. Som enhver organisation ved, er change management-programmer notorisk vanskelige at gennemføre. De bedste sikkerheds-awareness-programmer griber opgaven an på samme måde som andre organisatoriske forandringsprojekter. De samler en tværfaglig gruppe for at udnytte organisationens viden, herunder projektledere og medarbejdere fra intern marketing, HR og it-sikkerhed.

Forandring er ikke en selvfølge. Det tager tid og kræver en betydelig mængde viljestyrke og indsats. Ledelsen kan ikke undgå at føle en vis fortvivlelse og spekulere på, om awareness-projektet overhovedet er nødvendigt, og om det nogensinde vil blive færdigt.

Denne irritation opstår normalt, når awareness-kampagnen falder sammen med andre kommunikationsinitiativer i organisationen. Det er almindeligt, at brugerne modsætter sig under disse omstændigheder. I planlægningsfasen kan organisationen imødegå denne friktion ved at reducere mængden og hyppigheden af awareness-kommunikation i en begrænset periode. Det vigtige er ikke at stoppe programmet. Hvis du gør det, vil du aldrig få det i gang igen.

Dette kapitel hjælper dig med at sikre, at awareness-kampagnen bliver vellykket med råd om, hvordan du kommunikerer effektivt, hvordan du fortsætter, når du støder på apati, hvordan du kan regne med, at folk i din organisation vil hjælpe med at sprede budskabet, og hvordan du kan udnytte dine tredjepartskontrahenter.

Kommuniker som om, du mener det

Din organisations awareness-kampagne skal være skræddersyet specifikt til din organisation. For at sikre, at din kampagne kommunikerer det budskab, du ønsker, skal du gøre følgende:

- **Sørg for, at det er forsynet med dit logo for at give det genkendelighed og vægt i dine brugeres awareness.** Da dine medarbejdere bruger så meget audiovisuelt indhold i deres privatliv, skal du sikre dig, at uddannelsens indhold giver et vigtigt og relevant indtryk. Ikke desto mindre er enhver træning i cyber-awareness bedre end slet ingen træning.
- **Sørg for, at dine budskaber passer til de trusler, som dine medarbejdere udsættes for i dagligdagen.** Undgå at bruge awareness-træning for syns skyld, bare for at kunne sige, at I har et awareness-program.
- Hvis folk forstår risiciene og konsekvenserne for dem selv og for organisationen, vil langt de fleste af dine medarbejdere reagere positivt og ændre deres adfærd. Brug tid på at formulere det rigtige budskab. Hvis det ikke er noget, som du eller dit team er specialiseret i, kan du bede dit marketingteam om hjælp. Alternativt kan der søges hjælp udefra.


HUSK


TIP

Dine brugere kan kun klare en begrænset mængde kommunikation om dette emne. Start stille og roligt og opbyg din kampagne over 12 måneder. Tænk over det, hvor mange eLearning-kurser ville du tage på en måned, selv om de var korte? Hvis din målgruppe ikke

har fået denne type træning før, skal du give dem et stykke eLearning om måneden i de første seks måneder, så medarbejderne ikke bliver trætte af det.

HUSK

Før du øger den mængde træning, medarbejderne får, skal du desuden spørge dig selv, hvor mange cybersikkerheds-politikker, simulerede phishing-angreb og risikovurderinger dine brugere kan klare i de første seks måneder? Det bidrager alt sammen. For at sikre, at awareness-kampagnen ikke slutter for tidligt, skal du tale med ledelsesteamet om, hvor hårdt de vil presse brugerne til at fordøje dette indhold. Erfaringen viser, at en god tommelfinger-regel er, at mindre er bedre. Det er vigtigt, at du får dit publikum med dig på rejsen.

Mange sikkerhedskampagner forsømmer at træne brugerne i, hvorfor sikkerheden er vigtig for dem, og hvorfor der findes et informationssikkerhedsstyringssystem (ISMS) til at mindske risiciene ved cybertrusler. Sørg for at kommunikere dette overordnede initiativ til brugerne, så de kan se, at cybersikkerhed er en kritisk del af den almindelige forretningsgang i nutidens digitale verden.

Opretholdelse af momentum under apati

Det er normalt nemt at få ledelsens opbakning til at uddanne dine brugere med et sikkerheds-awareness-projekt. Den øverste ledelse er fuldt ud opmærksom på truslerne mod organisationen i form af bøder og skader på omdømmet. Det er dog ret almindeligt, at kampagnen seks måneder efter at være sat i gang rammes af træghed og udviser dårlige resultater. I awareness-projekter er det ret almindeligt, at det ikke lykkes at etablere og gennemføre en forudsigelig kommunikationscyklus.

De fleste medarbejdere og den øverste ledelse skal lige fra starten informeres om, at sikkerhedskampagnen er en del af en langsigtet strategi, som går ud på at forbedre organisationens cyberforsvar. Det er yderst vigtigt, at folk ikke blot forventer et enkeltstående initiativ. Du skal derfor udforme en gentagelig kommunikation, så brugerne forstår, hvor vigtig kampagnen er, gennem regelmæssige udsendelser af centrale budskaber, uddannelse og vurderinger. Indbyg desuden et feedback-loop i din kommunikation, så ledelsen får rettidige udtalelser fra medarbejderne. Ledelsen kan bruge denne feedback til at forbedre det overordnede awareness-initiativ over tid og til at tilpasse rytmen i dine løbende awareness-kampagner.

Det er svært for ledelsen at fokusere på medarbejdernes awareness i årets løb på grund af hyppigheden af aktive cybertrusler. Cybersikkerhed indebærer så meget "brandslukning", at det er næsten umuligt at få tid til at formulere budskaber til awareness-programmet.

HVORDAN ET DATABRUD KAN GIVE ANLEDNING TIL FORANDRINGER

Der kan ikke siges noget positivt om at være modtager af et målrettet cyberangreb, der resulterer i et brud på datasikkerheden. Den oplevelse ser ikke godt ud på dit CV, hvis du er sikkerhedsmedarbejder. Det skal dertil siges, at erfaring med at håndtere en større cyberhændelse en stor begivenhed for enhver leder, der er beskæftiget med informationssikkerhed.

Forskellen på en organisation, der har haft et databrud (eller næsten-uheld) er, at den erfarne organisation har en målrettet beredskabsplan klar til brug, hvorimod en organisation, der ikke har prøvet det før, ofte har en afventende tilgang. Hvis organisationen har en erfaren ledelse, har passende hændelsesplanlægning sandsynligvis allerede fundet sted.

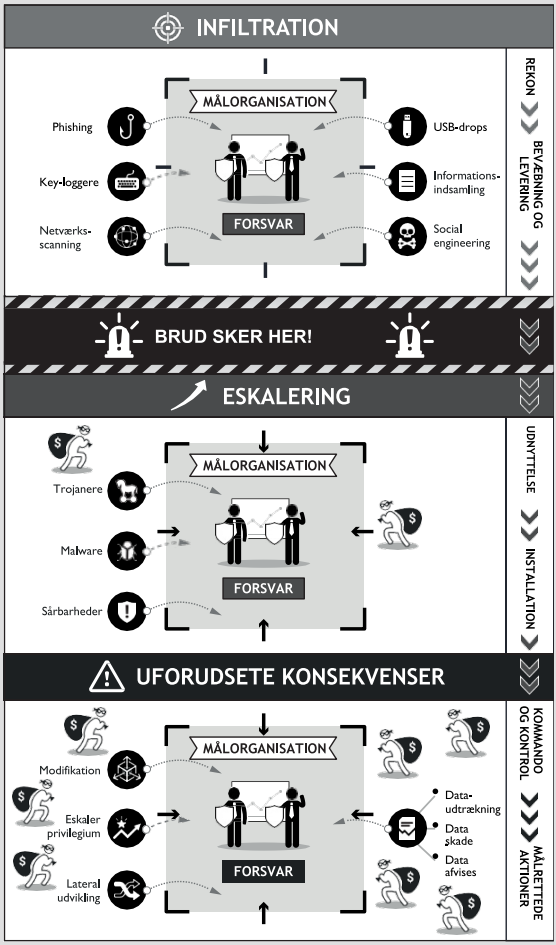
Her er den eneste gode ting, som et databrud eller et næsten-uheld kan forårsage: Den øverste ledelse kan ikke længere hengive sig til ønsketænkning eller plausibel benægtelse. De er nødt til at gå i aktion.

Selv om alle er opmærksomme på truslerne og er enige i, at der er stor chance for, at deres organisation bliver offer for et cyberangreb, er investeringer i cybersikkerheds-awareness stadig upopulære, og ledelsen er fristet til at komme med en minimumsløsning. Sikkerhedsbranchen må tage et vist ansvar for at promovere den nyeste perimeterteknologi som et universalmiddel mod alle sikkerhedsproblemer. Den glemmer altid, at den nemmeste vej uden om forsvaret er via den person, der sidder bag firewallen.

Fagfolk inden for databeskyttelse, compliance og informationssikkerhed bør som gruppe være forsigtige med at forsøge at skræmme ledelsen til at handle med trusler om bøder. Fremhæv hellere de forretningsmæssige fordele ved at skille sig ud fra de mindre sikre organisationer eller organisationer, der er mindre omhyggelige med overholdelse. Opmærksomheden på den deraf følgende

konkurrencedygtige markedsværdi skal fremmes internt som begrundelse for investeringer, især i forbindelse med ændring af medarbejderkulturen.

Ledelsen har en enestående mulighed for at forpligte ledelsesgruppen til informationssikkerhedsopgaven og opnå den nødvendige støtte kort tid efter et sikkerhedsbrud eller et næsten-uheld, og før hændelsen er blevet efterrationaliseret. Denne investering er som regel i mennesker og løsninger, men det er i sidste ende den tid, som denne gruppe afsætter til formålet, der er den mest værdifulde. Nedenstående figur viser tidslinjen for et typisk databrud.



TIP

Brug en uge i starten af året på at fastlægge de nødvendige awareness-aktiver (politikker, vurderinger, eLearning, simulerede phishing-angreb, blogs, konkurrencer, events på grundlag af nationale cyberdage), der er nødvendige i de kommende 12 måneder. Bestem kommunikationens hyppighed ud fra bedste skøn. Få derefter opbakning til din plan fra den øverste ledelse og før den ud i livet. Undgå en fragmenteret tilgang, som f.eks. planlægning for de næste tre måneder. Hvis du gør det, kan du ikke undgå at komme ud af kurs senere på året. Planlæg i stedet en 12-måneders kampagne og gennemgå processen med jævne mellemrum.

Inddragelse af Cyber Security Champions

Det er yderst vigtigt at sikre, at folk i organisationen ikke udelukkende betragter it-afdelingen som ansvarlig for at skabe opmærksomhed på informationssikkerhed og databeskyttelse. Organisationen skal derimod acceptere, at organisationens digitale sikkerhed er *alles* ansvar.

En awareness-kampagne om cybersikkerhed har brug for så mange venner som muligt. Din organisation har allerede medarbejdere, som er aktivt involveret. De rapporterer om hændelser, simulerede phishing-angreb og giver feedback. De forstår den fare, som cyberrisici udgør for organisationen. Gå disse brugere i møde. For at sikre, at alle forstår deres ansvar, skal du støtte dig til disse brugere i organisationen. Disse *champions* kan kommunikere, er tiltalende og har gode sociale færdigheder. De er værdifulde aktiver for din kampagne. Få kolleger i andre afdelinger til at hjælpe med at identificere potentielle medarbejdere.

TIP

Ledelsen bør med andre ord skabe et ambassadørprogram, der henter støtte fra disse champions, de personer i din organisation der er mest ambitiøse og interesserede. Dit ambassadørprogram har brug for støtte og opbakning fra ledelsesniveauet i hele organisationen. Du kan bruge denne ledelsesstøtte til formelt at lancere dit ambassadørprogram og dermed give den anerkendelse fra organisationens side, som folk elsker at modtage.

Du har måske allerede folk i frontlinjen i dine informationssikkerheds- og privatlivsaktiviteter. Disse personer kan være blevet identificeret som ejere af informationsaktiver ud fra et ISO27001-perspektiv eller som indehavere af en databehandlingsaktivitet. De kan allerede have modtaget relevant uddannelse i databeskyttelse eller informationssikkerhed.

Prøv at fejre gode resultater. Byg din kampagne på et positivt grundlag. Kommuniker anerkendelse af en vellykket re-certificering af ISO27001 og andre lignende præstationer på dette område.

TIP

Dit program for Cyber Security Champions bør så vidt muligt have en særlig kommunikationskanal i et internt beskedværktøj, f.eks. Microsoft Teams eller Slack, for at sikre en regelmæssig strøm af feedback om, hvordan det går med dit cyber-awareness-projekt. Brug i det mindste denne kommunikationskanal til at opdatere disse champions om eventuelle brud på datasikkerheden og næsten-uheld.

Det er en tilfredsstillende del af en vellykket awareness-kampagne at få et Cyber Security Champion-program i gang. Det giver reel opbakning til dit forandringsinitiativ i hele organisationen. Det fungerer også som et tidligt advarselssystem, når kampagnen er begyndt at vakle eller har ramt ved siden af.

Disse champions kan gennem deres handlinger og deres fortalervirksomhed vise, at programmer for cybersikkerheds-awareness gør det nødvendigt for hele organisationen at inddrage denne bedste praksis som en del af den almindelige forretningsgang.

Udvidelse af cybersikkerheds-awareness til relationer med tredjeparter

Det har ofte været vanskeligt for de fleste organisationer at håndtere leverandør- og tredjepartsrisici i de sidste 20 år. Efterhånden som organisationer har ændret sig og udviklet sig, har de outsourcet specialiseringer og aktiviteter, der ligger uden for deres hovedaktiviteter, til betroede partnere. I visse moderne organisationer er op til 50 % af medarbejderne ikke fuldtidsansatte. Brugen af underleverandørordninger giver en skalerbar og smidig organisation. Det har imidlertid konsekvenser for gennemførelsen af en sikkerheds-awareness-kampagne. I disse afsnit diskuteres det, hvilke underleverandører du skal inddrage i din sikkerheds-awareness-plan, og hvilke teknologiske udfordringer de eventuelt imødegår.

Vid hvem der skal medtages

Underleverandørernes grad af integration i din organisation er afgørende for, i hvilket omfang de skal deltage i dit awareness-program. De tredjepartsforbindelser, der har kontakt med dine informationsaktiver, databehandlingsaktiviteter og netværk, bør i det

mindste indgå i planlægningen af din awareness-kampagne. Hvis det er relevant, bør din organisation identificere særligt vanskelige eller risikofyldte relationer med tredjeparter og derefter fastlægge den nødvendige kommunikation for hvert segment. Alle, der har adgang til dine interne systemer, bør som minimum underskrive din politik for acceptabel brug. Derefter kan du så udarbejde yderligere krav til politikker og træning.

Professionelle rådgivere og tekniske eksperter fra betroede tredjeparter kan f.eks. have adgang til fortrolige data og have brug for adgang til vigtige systemer, især finans-, HR- og organisationsdækkende datalagre. Sørg for, at disse typer tredjepartsmedarbejdere får undervisning i de nødvendige forpligtelser i forbindelse med adgang til dine digitale aktiver.

Som det er tilfældet med fastansatte medarbejdere, bør ledelsen skelne mellem tredjepartskontrahenter ud fra den risiko, de udgør for organisationen. Jo større risiko, jo flere kontrolforanstaltninger skal der til. Sørg for, at du opnår enighed om disse kontrolforanstaltninger med underleverandøren på det tidspunkt, hvor kontrakten indgås, hvad enten det drejer sig om træning eller attestering af politikker. Disse forudsætninger bør indgå i dine standardbetingelser og bør udgøre en vigtig del af dit forhold til leverandører, der har adgang til dine it-systemer.

Potentielle teknologiske udfordringer

Nogle gange kan din organisation have brug for at overvinde reelle teknologiske udfordringer for at få tredjeparter med i dit awareness-initiativ. Fjerntliggende tredjeparter kan måske ikke få adgang til et lokalt læringsstyringssystem (LMS) for at gennemføre den nødvendige eLearning. Det samme kan være tilfældet ved overholdelse af vigtige politikker, der regulerer forholdet mellem organisationen, leverandøren og den person, der rent faktisk udfører tjenesten. Tidligere har organisationer ofte undladt at inddrage tredjeparter i denne type sikkerhedsinitiativer. Men styring af leverandører og den cyberrisiko, der er forbundet med interaktioner med tredjeparter, har givet anledning til bekymring for it-ledere og er blevet et fokusområde for international lovgivning om beskyttelse af personlige oplysninger.

Gradvis introduktion af cybersikkerheds-awareness til tredjeparter

En trinvis tilgang til inddragelse af tredjeparter i dine cyber-awareness-kampagner er den mest fornuftige metode til at fremme dit forhold til dine leverandører. Find først en måde at administrere dine vigtigste politikker på og hav en pålidelig måde at opnå attestering på. Der bør ideelt set være en elektronisk løsning til forvaltning af politikker, som kan automatisere denne proces. Papir er en rigtig dårlig idé, især når man forsøger at bringe underskrevne dokumenter tilbage til en central mappe. Bestem de væsentligste risici, som en underleverandør kan udgøre, og giv derefter passende træning, ideelt set gennem et cloud-baseret LMS, som underleverandøren kan få adgang til, enten fra en fjernplacering eller gennem dine systemer, før de ankommer.

ADVARSEL

Du kan også finde alle de dårlige adfærdsmønstre, som dine medarbejdere udviser i interaktioner med leverandører. Det er f.eks. lige så sandsynligt, at en underleverandør uforvarende lader uautoriserede personer slippe ind (tailgating), som om de er en af dine egne medarbejdere. Din interne awareness-kampagne dækker imidlertid den fysiske sikkerhed via politikker og uddannelse. Sørg for, at underleverandøren også trænes i disse emner.

Når du udvider dækningen af din awareness-kampagne, skal du vurdere, i hvor høj grad en leverandør afholder awareness-træning og forvaltning af medarbejderpolitik i sit eget miljø. Denne vurdering er en del af din due diligence-undersøgelse af leverandøren, og bør udgøre en integreret del af din organisations proces for onboarding af leverandørerne. Mange organisationer sender leverandøren en risikovurdering, før der indgås kontrakt. I denne vurdering skal du evaluere leverandørens cyber-awareness i forbindelse med de spørgsmål, som din organisation stiller om generel informationssikkerhed, f.eks. firewall og anti-virusforsvar. En leverandør, der ikke kan fremlægge dokumentation for en politik eller træningsordning for informationssikkerhed, vil have svært ved at opfylde kravene til din awareness-kampagne.

I DETTE KAPITEL

- Forståelse af, hvor vigtige politikker er i en kampagne for sikkerheds-awareness
- Hjælp med at identificere risici
- Træning af erfarne medarbejdere og nye medarbejdere i politikker
- Overvejelse af fordelene ved en centraliseret teknologiarkitektur

Kapitel 4
Integration af politikstyring i dit sikkerheds-awareness-program

En politik er: Et sæt idéer eller en plan for, hvad der skal gøres i bestemte situationer, som en gruppe mennesker, en virksomhed, en organisation, en regering eller et politisk parti officielt er blevet enige om.

Politikker er en plan for, hvad der skal gøres i bestemte situationer. Din sikkerheds-awareness-kampagne har brug for klare politikker. Ledelsen har angivet, hvad medarbejderne skal bruge i bestemte situationer. Politikker skal kommunikeres til medarbejderne, for hvis du ikke fortæller medarbejderne, hvad de skal gøre i bestemte situationer, hvordan kan man så være sikker på, at de gør det rigtige?

I dette kapitel fokuseres der på betydningen af den rolle, som politikker spiller for at styrke din organisations sikkerheds-awareness-kampagne.

Forståelse af politikkers rolle i en kampagne

Politikker i en organisation er som en lovsamling, der gør en regering i stand til at regere sit samfund. De er rygraden i organisationens reaktion på cybersikkerhedstrusler (sociale mediepolitikker, adgangskodepolitikker, netværkspolitikker og så videre) og for lovmæssig beskyttelse (politik for acceptabel brug, privatlivspolitikker, politikker knyttet til adfærdskodekser og så videre). De er et vigtigt element i en bedste praksis-kommunikation med medarbejderne. Træningsaktiviteter og -politikker er mest effektive, når de er på linje med hinanden. Hvis de behandles hver for sig, hober de sig op, øger mængden af medarbejderkommunikation og giver i sidste ende brugertræthed.

HUSK

Betragt politikker som din organisations love. Ingen regering ville tillade, at deres love blev lavet hurtigt og spontant, og relevante myndigheder ville føre nøje tilsyn i forbindelse med godkendelse af love, politikker og kommunikation. Alligevel ignorerer den øverste ledelse i mange organisationer ofte politikstyring for informationssikkerhed og databeskyttelse.

Når du udarbejder et awareness-program, skal du sørge for at se på alle de centrale elementer, der skal kommunikeres til medarbejderne, f.eks. politikker, eLearning, risikovurderinger og simulerede phishing-angreb. Udfordringen består i at finde den rigtige balance mellem disse elementer for at nå målene for awareness-strategien.

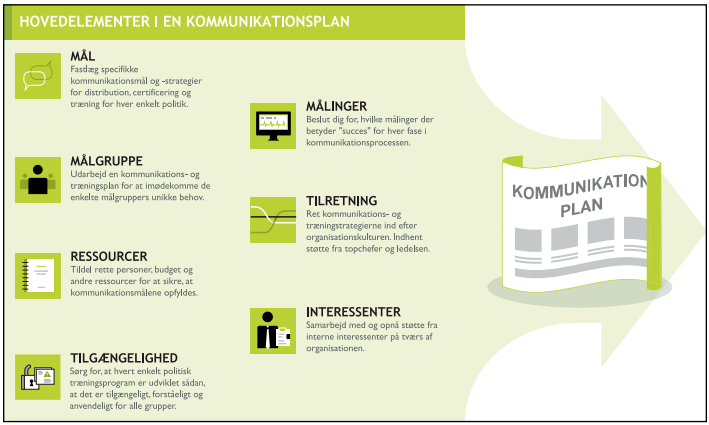
HUSK

Ligesom i alle andre awareness-initiativer er mennesker i centrum. Få medarbejderne til at tilslutte sig politikkerne, så medarbejderne accepterer, hvordan de skal handle i bestemte situationer. Denne accept baner vej for personlig ansvarlighed hos de enkelte medarbejdere, og det er et vigtigt skridt i retning af adfærdsændringer.

Politikker er den dokumenterede organisatoriske standard, som medarbejderne pålægges at overholde. Det er afgørende, at medarbejderne har nem adgang til en central politikportal, som udgør organisationens kilde til sandheden. Denne portal skal være beskyttet mod manipulation for at give organisationen "bevismæssig vægt", hvis politikkerne anfægtes ved en domstol.

Derudover bør politikkerne være underlagt streng revisionskontrol, så alle politikændringer over tid registreres og er tilgængelige og kan gennemgås i forbindelse med revision. Politikker ændrer sig

konstant for at opfylde organisationens behov. Change management-processen for politikker i organisationen bør gennemgås for at sikre, at den politiske tilgang er egnet til formålet. Det vigtigste er, at politikkerne kommunikeres til medarbejderne på en måde, der understøtter overholdelse af cybersikkerhedsregler og lovkrav. Den bedste måde at opnå denne kommunikation på er at udarbejde en kommunikationsplan for politikken som vist i figur 4-1.



FIGUR 4-1: Hovedelementerne i en kommunikationsplan (Kilde: OCEG og GRC 20/20).

Politikstyring: Træning af medarbejdere til at identificere risici

En organisation udarbejder politikker for at mindske identificerede risici inden for compliance eller informationssikkerhed. Politikker udarbejdes, når risici er så store, at der skal foreligge en formel skriftlig politik. En politik vil desuden angive de nødvendige kontrolforanstaltninger til at håndtere risikoen. Politikken er imidlertid kun ét trin i awareness-processen. Medarbejderne skal også uddannes i politikkens indhold.

Den træning, der er knyttet til politikken, kan udgøre en mere kortfattet udgave af politikkens indhold. Lad politikdokumentet dække de mange forskellige eventualiteter i forbindelse med risikoafhjælpning. Træningen bør dække de vigtigste punkter, som medarbejderne forventes at kende, og ikke være en ordret gengivelse af politikdokumentet.

HUSK

Politikker spiller en stor rolle med hensyn til at ændre organisationskultur. Når en medarbejder bliver bedt om at bekræfte en politik, enten elektronisk eller ved at underskrive et stykke papir, bekræfter medarbejderen, at denne er klar over betydningen af sine handlinger. Politikker hjælper med at øge betydningen af cybersikkerhed på arbejdspladsen. Politikker hjælper med at tilpasse den personlige ansvarlighed til organisationens risici, procedurer og regler.

Disse afsnit indeholder flere oplysninger om træning af både eksisterende og nye medarbejdere.

Træning af medarbejdere i politikker

Selv om politikken indeholder retningslinjer for medarbejdere, har de ofte brug for uddannelse i, hvordan den føres ud i livet. Den risiko, som politikken søger at imødegå, og den risiko, der er blevet vurderet, hænger direkte sammen med, hvor mange instruktioner brugeren har brug for. Højere risici vil have politikker, der kræver et højere uddannelsesniveau for at sikre, at den pågældende kontrolforanstaltning forstås og anvendes. Derudover kan du være nødt til at anvende en hybrid tilgang til politik, eLearning og klasseundervisning i forbindelse med højere risici for at sikre maksimal accept og forståelse. (Kapitel 5 handler om en hybrid tilgang i større detaljer.)

Der er en klar sammenhæng mellem den tid og energi, der bruges på politik, træning og awareness, og den faktiske indvirkning på organisationen. Compliance-aktiviteter, der er højt profilerede med opbakning fra ledelsen, har tendens til at få større opmærksomhed blandt medarbejderne og give anledning til med udbredt gennemførelse af politikker, fuldførelse af træning og relaterede test.

Se figur 4-2 for vigtige spørgsmål, som bør stilles i forbindelse med træning af medarbejdere i nye politikker.

Bestemmelse af, hvorfor politikker er vigtige for at gøre nye medarbejdere aware

Mange organisationer indfører en tilgang til nye medarbejdere, som indebærer, at de skal underskrive politikker og se eLearning i op til tre timer om dagen i den første uge af deres ansættelse. Dette er ikke en effektiv brug af den nye medarbejders tid. Denne type læring svarer til at drikke fra en brandslange.

FIGUR 4-2: Spørgsmål, som bør stilles (Kilde: OCEG og GRC 20/20).

Alle organisationer kæmper med at håndtere nye medarbejdere i de første par uger af deres ansættelse, mens de kravler op ad indlæringskurven. Organisationer er nødt til at udarbejde en introduktionsplan, der passer til formålet. Forestil dig, at du skulle træne i to eller tre timer hver dag. Det ville være overvældende. Problemet med nye medarbejdere er, at der er så meget, de skal lære. Når du træner dem i cybersikkerhed, skal du tage hensyn til menneskers evne til at bevare opmærksomheden og forstå, hvad de lærer.

HUSK

Planlæg vigtige politikker for nye medarbejdere sammen med den relevante eLearning på en velovervejet måde. Sæt begrænsninger for, hvor meget eLearning den nye medarbejder forventes at gennemføre den første måned. Højst tre timer om ugen i den første måned er optimalt. Dette tidsrum giver den nye medarbejder mulighed for at gennemføre de vigtigste politikker og eLearning-lektioner, der afspejler behovet for at lære den organisatoriske tilgang at kende, uden at blive træt. Efter den første måned skal du skære ned på antallet af politikker og eLearning for at give medarbejderen mulighed for at blive produktiv i sin nye rolle.

Anerkendelse af vigtigheden af en centraliseret teknologiarkitektur for dine politikker

Politikforvaltning og eLearning i en moderne organisation er blevet for kompliceret til, at medarbejdere kan forvalte det manuelt på en effektiv måde. Et centraliseret system til forvaltning af politikker

kan støtte udfordringen med at imødegå de konstant skiftende krav fra organisationen, lovgivningen og forretningsmiljøet.

Det er vanskeligt at administrere politikkens livscyklus på regneark og i fildelingssystemer. Det viser en mangel på overordnet modenhed med hensyn til compliance i en organisation. Det viser også en ad hoc-tilgang til forvaltning af sikkerhed og compliance.

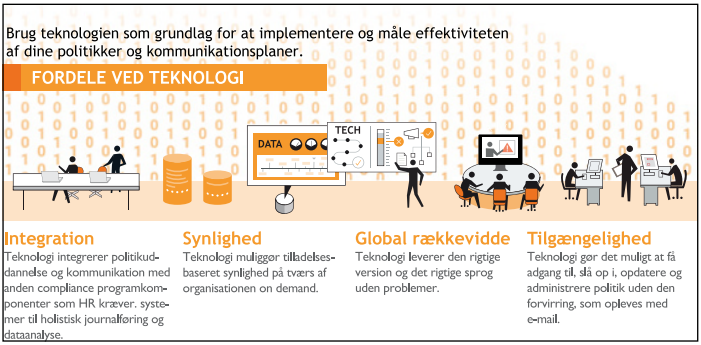
I de følgende afsnit drøftes det, hvordan et centraliseret politikstyringssystem kan hjælpe din organisation, og hvem i din organisation der kan bruge systemet.

Identifikation af fordele ved et centraliseret system

Her er nogle af hovedfordelene ved at bruge et centraliseret system:

- **Det garanterer 100 % deltagelse.** At sikre, at alle modtager, forstår og bekræfter politikken, er en afgørende fordel ved et centraliseret system til forvaltning af politikker.
- **Det giver adgang til træning og politikker ét sted.** Det er vigtigt for alle medarbejdere, at der kan knyttes relevant træning til dine politikker.
- **Det reducerer byrden for ledelsen.** Et omfattende tilsyn fra ledelsens side kan undgås ved at automatisere håndhævelse af politikker. Det er teknologien og ikke ledelsen, der informerer og minder brugerne om, at de skal opfylde deres forpligtelser med hensyn til politikker ogtræning.
- **Alt indhold om politikker og træning befinder sig på samme sted.** Den vigtigste værdi af en teknologiløsning er at have én kilde til sandheden i forbindelse med dine compliance-aktiviteter, navnlig i forhold til politikker, træning og interaktion med dine medarbejdere.

Figur 4-3 viser, hvordan centraliseret teknologi kan gavne din organisation.



FIGUR 4-3: Fordele ved teknologi (Kilde: OCEG og GRC 20/20).

Forståelse af, hvem der anvender dette system

Der er tre hovedgrupper, som anvender denne type politikstyrings-system. De er:

- **Administratorer, der opretter systemet og stiller politik-ker og træning til rådighed:** De har deres egen administra-tive grænseflade til at oprette, målrette, offentliggøre og administrere organisatoriske politikker.
- **Brugerne der anvender træningen og politikken:** De kan opfylde deres forpligtelser til at underskrive politikker, tage træningen, selv administrere deres interaktion med indholdet og hente det frem, hvis de har brug for at få genopfrisket deres viden.
- **Systemets ledelses- eller oversigtsportal:** Her kan ledelsen gennemgå systemet for at sikre, at medarbejderne gennem-fører de nødvendige kommunikationskampagner om compliance. Revisorer og tilsynsmyndigheder kan få adgang til systemet for at sikre, at organisationen har opfyldt deres forpligtelser til at udvise omhu og føre tilsyn.

I DETTE KAPITEL

- Opnåelse af støtte fra ledelsen
- Udarbejdelse af en plan for kampagnen
- Oprettelse af en baseline for din strategi
- Forståelse af hvad der udgør et godt resultat
- Overvejelse af en hybrid tilgang

Kapitel 5
Udvikling af bedste praksis for en cyber-awareness-strategi

Hvis din cyber-awareness-kampagne skal blive en succes, har din organisation brug for en klar handlingsplan. I dette kapitel får du råd og vejledning om, hvordan du formulerer en sådan plan, og hvordan du sikrer dig, at du har din organisations ledelse bag dig. Når din plan er klar, skal du kunne måle, om den virker. Om nødvendigt kan din organisation overveje en hybrid tilgang.

Opnåelse af støtte fra ledelsen

Et vellykket awareness-program afhænger ofte af, om ledelsen i din organisation støtter det. Uden ledelsens støtte er det svært at opnå tilstrækkelig finansiering og ressourcer, og uden dem er det begrænset, hvad et sikkerheds-awareness-projekt kan opnå.

Cyber-awareness-programmer har til formål at ændre medarbejdernes adfærd, og det indebærer et aspekt af menneskelig psykologi. Hvis der er støtte fra ledelsesteamet, kan du fjerne forhindringer, og

der kan hurtigt træffes beslutninger. Det er vigtigt, at man fra starten kender ledelsens holdning. Hvad mener ledelsen f.eks. om upassende cybersikkerhedsadfærd? Er det træd forsigtigt eller nul tolerance? Hvor mange simulerede phishing-øvelser skal en medarbejder have ikke bestået, før der træffes disciplinære foranstaltninger? Hvis ledelsen ikke sætter tonen, betyder det, at hver enkelt leder potentielt set selv kan fortolke gennemførelsen af awareness-kampagnen.

At ændre medarbejdernes adfærd involverer noget menneskelig psykologi. Folk synes f.eks. godt om at få anvisninger fra deres ledere. Så det er meget effektivt at starte en awareness-kampagne med et budskab fra toppen. Det kunne være i form af en e-mail eller en kort besked foran kameraet.


TIP

Når du forbereder din awareness-kampagne, skal du sikre dig, at du har fuld opbakning fra din ledelsesgruppe. Det er en god idé at afholde et par timers træning, der specifikt er rettet mod lederfunktionen. Dette bør være skræddersyet træning som foregår ansigt til ansigt og understøttes af eLearning på ledelsesniveau.

Sammensætning af en kampagneplan

En planlægningsproces, der er baseret på risikobegrænsning, er den bedste måde at udvikle en egnet kampagne for cyber-awareness på. Ved planens udarbejdelse skal du sørge for, at den passer til tidshorisonten (normalt 12 måneder) og omfatter de vigtigste risici, som organisationen står over for på det pågældende tidspunkt. Vær beredt på at genevaluere dine risici, da de ændrer og udvikler sig med tiden.


ADVARSEL

Organisationer er ofte afhængige af, at en informationssikkerhedsekspert tilrettelægger planlægningen af en awareness-fremmende kommunikationsplan. Det er vigtigt at støtte denne funktion med kommunikationsekspertise fra organisationens side. Når det er sagt, er fagfolk inden for informationssikkerhed og databeskyttelse afgørende for, at en kampagne for cybersikkerheds-awareness bliver en succes. Deres viden kan lede og informere programmet.

Risiko er kernen i enhver awareness-kampagne, og sådanne eksperter kan identificere og prioritere de forskellige typer risici, der skal afhjælpes.

HUSK

Det kan dog være nødvendigt, at en person i organisationens projektledelse eller én, som er beskæftiget med kommunikation på tværs af organisationen, indgår i dette team for at sikre, at budskabet bliver delt effektivt og virkningsfuldt. Teamet har brug for flere forskellige færdigheder for at kunne skabe en vellykket awareness-kampagne.

Det er fristende at sende et par simulerede phishing-e-mails og tro, at du har opfyldt kravet til cybersikkerheds-awareness. Der er ingen tvivl om, at denne metode fremhæver risikoen forbundet med social engineering over for medarbejderne. Men awareness-programmet skal tage hensyn til alle truslerne mod organisationen. Et awareness-program bør også optage afhjælpningsøvelser og dokumentere opfølgende aktiviteter. Disse registreringer er vigtige, når compliance og governance skal påvises.

Nøglen til at skabe et vellykket cyber-awareness-projekt er at oprette en playbook (se figur 5-1) eller en kampagne af aktiviteter for det kommende år. Øvelsen tvinger én til at identificere vigtige risici. Organisationen skal afgøre, om medarbejderne er i stand til at forstå budskaber om compliance og sikkerhed. Ledelsen skal beslutte, hvilken slags og hvor mange meddelelser der kan udsendes pr. uge, pr. måned og i sidste ende pr. år. Udfordringen er at afbalancere risici og brugertræthed. Det team, der gennemfører denne kampagne, skal passe på ikke at være for ambitiøse med gennemførelsen af sikkerhedsprogrammet.

HUSK

Det tager lang tid at ændre folks adfærd og forbedre arbejdsstyrkens modstandsdygtighed over for cybersikkerhedstrusler.

FIGUR 5-1: En 12-måneders planlægningskalender for sikkerheds-awareness.

Fastlæggelse af en baseline

Nøgleresultatindikatorer (KPI'er) viser, om et projekt er vellykket eller ej. Du bør forvalte informationssikkerheds-awareness på samme måde. Fremhæv de KPI'er, du har identificeret, for at

fastlægge en baseline. Du kan derefter bruge disse data til at måle, hvilken fremgang der er opnået.

Dine awareness-programmer skal være baseret på de aktuelle risici, som din organisation står over for. Som udgangspunkt udgør de seneste hændelser, der er registreret, en glimrende rettesnor for de problemstillinger, som programmet søger at imødegå og de risici, der skal afhjælpes.


TIP

Den bedste måde at finde ud af, hvor godt dine brugere kender til disse risici, er ved at spørge dem gennem et spørgeskema eller lignende undersøgelse, der afholdes online. Spørgsmålene i undersøgelsen bør være baseret på de risici, som organisationen står over for. Sørg for, at undersøgelsen er så kort og koncis som mulig.

Resultaterne af undersøgelsen vil derpå påvirke et eventuelt efterfølgende træningsprogram. Hvis undersøgelsen f.eks. viser, at der er mangler i medarbejdernes viden om fysisk sikkerhed, er der brug for kommunikation om uddannelse eller politikker for at afhjælpe problemet. Vi anbefaler, at din organisation tackler en nøglerisiko en gang om måneden. Det betyder, at det i undersøgelsen tjekkes, hvad dine medarbejdere ved om mindst 12 spørgsmål/risici.


HUSK

En anden hurtig måde at fastlægge en baseline på er ved at gennemføre et simuleret phishing-angreb på medarbejdere. Det hjælper med at fastslå, hvor modtagelig organisationen er over for falske phishing-e-mails, og giver et realtidsbillede af, hvor stor en del af medarbejderne ville være faldet for den, hvis angrebet reelt havde fundet sted. Det ville være endnu værre for de brugere, der havde afgivet deres legitimationsoplysninger, når de blev bedt om det.

Politikker udgør en integreret del af medarbejdernes sikkerheds-awareness. Helt i starten skal du afholde en øvelse for at identificere de vigtigste politikker, som medarbejderne skal overholde. Husk, at en politik kun bør eksistere, hvis den er knyttet til en risiko. Hver af dine vigtigste risici bør derfor være forbundet med en organisatorisk politik. Det er vigtigt at registrere, hvornår dine politikker sidst blev revideret, og om de stadig er egnede til formålet.


ADVARSEL

Undgå at afholde en omfattende revision af organisationens politikker, da det har en tendens til næsten at sætte awareness-kampagnerne helt i stå. Den bedste praksis er at gøre det nødvendige med den relevante politik mindst en måned, før risikoen indføjes i din awareness-plan.

Fastlæggelse og måling af succes

Når en baseline er aftalt og dokumenteret, er det vigtigt at spore dine KPI'er hver måned for at måle, hvor vellykket awareness-planen er. Områder, der skal gennemgås, omfatter følgende:

- Procentdel af brugere, der overholder vigtige politikker
- Procentdel af brugere, der klikker på et simuleret phishing-angreb
- Antal vurderinger af leverandørrisici
- Antal databehandlingsaktiviteter
- Antal fuldførte medarbejderundersøgelser
- Antal sikkerhedshændelser
- Antal medarbejderrapporterede phishing-e-mails

De sidste tre målinger er vigtige, fordi de vedrører, i hvor høj grad medarbejdernes er bevidste om de vigtigste af organisationens sikkerhedsudfordringer. ***Bemærk:*** Antallet af indberettede sikkerhedshændelser kan stige, efterhånden som medarbejderne bliver opmærksomme på de forskellige risici.

Disse målinger danner grundlag for rapporteringen til styringsudvalget for informationsstyring (Information Governance Steering Committee) og vil bidrage til at informere dem om risikoreduktion og fremskridt i awareness-kampagnen.

En hybrid awareness-tilgang

Gode markedsføringskampagner bruger mange forskellige metoder til at gøre kunderne opmærksomme på deres produkt eller tjeneste. De bruger en kombination af digitale kanaler, e-mail og sociale medier sammen med traditionelle metoder såsom kampagner og gaver i butikkerne. Så dit sikkerheds-awareness-program bør ligesom markedsføringskampagner bruge en hybrid tilgang for at tiltrække og fastholde brugernes opmærksomhed. Når du har opnået denne awareness, er det næste skridt at skabe en adfærdsændring.

I de følgende afsnit forklares det, hvordan du kan bruge storytelling og andre metoder til at formidle dit budskab på en effektiv måde.

Lad storytelling indgå i dit program

Der findes ikke nogen "one size fits all", når det drejer sig om markedsføring eller sikkerheds-awareness. Forskellige interne parter kæmper om medarbejdernes opmærksomhed i den organisatoriske kommunikationsverden. Det inddrager et godt awareness-program. Det betyder, at du skal bruge flere forskellige kommunikationskanaler for at få din målgruppes opmærksomhed, herunder fysiske, digitale og storytelling-kanaler.

HUSK

Mennesker har en mundtlig tradition. Så udnyt denne tradition og fortæl en historie, eller hav et tema, som folk kan relatere til, for at få dit budskab igennem. Det kan f.eks. være et godt tema for dine medarbejdere, at de påtager sig rollen som regeringsagenter, der forsøger at overvinde skurkenes bestræbelser. Tænk på James Bond eller Wonder Woman!

Vær innovativ i din kommunikation

Fysiske metoder at kommunikere med medarbejderne på omfatter forskellige opfindsomme metoder. Her er forskellige måder at kommunikere med din organisation om kampagnen på:

- **Plakater:** Den billigste og mest effektive måde er en plakatkampagne, der styrker dine vigtigste budskaber og temaer. Du kan bruge alle former for plakater, herunder digitale skilte i receptionen og små plakater i elevatorer. Sørg for at tilpasse dine plakater til den risiko, som du vil promovere, og skift plakater hver fjerde til sjette uge, så folk ikke bliver blinde for budskaberne.
- **Digitale metoder:** Digitale metoder er den mest almindelige metode til at kommunikere og imødegå den risiko, der er forbundet med manglende medarbejdertræning. Nogle organisationer har selvstændige simulerede eLearning-systemer vedrørende phishing, politikstyring eller cybersikkerhed, som bruges til at formidle vigtige budskaber til medarbejderne.

AUTOMATISERING AF KAMPAGNEN

Automatiser hele din 12-måneders awareness-kampagne om sikkerhed, og sørg for, at vigtige elementer formidles til den rette målgruppe på det rigtige tidspunkt. Disse elementer bør omfatte en kombination af skræddersyet eLearning, kritiske politikker, relevante blogs, simulerede phishing-e-mails, risikovurderinger og undersøgelser.

En automatiseret tilgang til sikkerheds-awareness gør det muligt at registrere revisionsoplysningerne for at understøtte det lovmæssige forsvar, der kan være nødvendigt i tilfælde af et databrud eller en revision.

I DETTE KAPITEL

- Sådan sætter ledelsen tonen
- Engagering af medarbejderne
- Forberedelse på et databrud
- Gennemgang af dine awareness-initiativer

Kapitel 6
Ti bedste praksisser for cybersikkerheds-awareness

Her er ti gode råd om bedste praksis, der kan hjælpe dig med at skabe den mest effektive awareness-kampagne om cybersikkerhed for din organisation.

Start med den administrerende direktør

Cybersikkerhed er endelig ved at få den opmærksomhed, den fortjener i bestyrelseslokalet. I takt med at antallet af højt profilerede databrud fortsætter med at stige, er der lagt større vægt på at håndtere cyberrisikoen for at mindske risikoen for angreb.

Cybersikkerhed er alles ansvar, men modstandsdygtige organisationer har brug for et stærkt lederskab fra den administrerende direktør. En engageret administrerende direktør vil gennemføre de rigtige sikkerhedsforanstaltninger, der er nødvendige for at beskytte organisationens digitale aktiver, medarbejdere, kunder og brandets omdømme. Hvis den administrerende direktør tager cybersikkerhed alvorligt, vil det smitte af på hele organisationen og bidrage til at skabe en kultur med øget awareness om cybersikkerhed.

Se kapitel 5 som kan hjælpe dig med at få støtte fra din administrerende direktør.

Kend dine organisatoriske tolerancer

For at skabe et effektivt program for sikkerheds-awareness skal din organisation evaluere trusselslandskabet og identificere de største risici. Det giver dig bedre indsigt i de reelle trusler, der kan kompromittere din organisations sikkerhed.

Din risikotolerance skal fastlægges fra starten, så du kan gennemføre de rigtige sikkerhedsforanstaltninger på grundlag af de reelle trusler, du står over for. Derved undgår du at bruge ressourcer på trusler, der sandsynligvis ikke vil opstå, eller som vil have ringe eller måske slet ingen indvirkning på din organisation.

Du skal foretage regelmæssige risikovurderinger for at sikre, at din tilgang til cybersikkerhed er i overensstemmelse med lovrammer, standarder for informationssikkerhed og love som f.eks. den generelle forordning om databeskyttelse (GDPR).

Hvis du tager dig tid til at identificere risiciene korrekt, kan det bidrage til at udforme budskaberne, leveringen og den effektive målretning af dit program for awareness om cybersikkerhed.

Forsvar dine informationsaktiver

For at kunne udvikle en omfattende cybersikkerhedsstrategi og identificere risici på effektiv vis er man nødt til at foretage en grundig revision af organisationens informationsaktiver.

Et informationsaktiv er et stykke information, som er værdifuldt for din organisation. Dette kan omfatte personligt identificerbare oplysninger (PII), finansielle oplysninger, intellektuelle ejendomsrettigheder eller andre oplysninger, der har stor betydning for din organisation.

Du skal fastslå, hvad de mest værdifulde informationsaktiver er, hvor de befinder sig, og hvem der har adgang til dem. Alle aktiver skal klassificeres (f.eks. offentlige, private eller fortrolige) og beskyttes på grundlag af deres værdi. Det er vigtigt at gøre, når man skal identificere risici og prioritere de områder, der skal forsvares.

Når du har identificeret disse områder, kan du fokusere på, hvordan hvert enkelt informationsaktiv potentielt kan kompromitteres. Uanset om der er tale om et systembrud, malware eller endog en insidertrussel, kan du tage informerede skridt til at forbedre disse processer og reducere risikoen for, at en cyberkriminel får adgang til kritiske systemer.

Fokus på højrisikogrupper

Nøglen til et effektivt sikkerheds-awareness-program er at sikre, at den rigtige træning leveres til de rigtige personer. Alle brugere kan blive udsat for cybertrusler, men visse medarbejdere har en højere trusselsprofil end andre. F.eks. vil dine personale- og finansafdelinger ofte blive angrebet på grund af deres privilegerede adgang til følsomme data.

Din administrerende direktør, økonomidirektør og andre medlemmer af topledelsen er også populære mål på grund af deres særlige adgang til værdifulde oplysninger. De vil ofte blive udsat for sofistikerede BEC-angreb (Business Email Compromise). I denne type phishing-angreb udgiver cyberkriminelle sig for at være en højtstående leder for at overtale en medarbejder, kunde eller leverandør til at overføre penge til en falsk konto eller videregive følsomme oplysninger. Hvis en højtstående leder falder for svindelnummeret, kan det få katastrofale følger og underminere hele organisationens sikkerhed.

Se kapitel 2 for flere oplysninger om, hvilke grupper der er mest udsatte, og hvordan du kan give dem målrettet uddannelse.

Gør det engagerende med effektiv storytelling

Storytelling er en af de mest effektive måder, hvorpå du kan puste liv i din awareness-kampagne om cybersikkerhed. Det må indrømmes, at cybersikkerhed kan være et tørt emne, men det er afgørende, at du finder en måde at engagere dine medarbejdere på, hvis du ønsker at påvirke adfærden i din organisation positivt. Budskabet er simpelthen for vigtigt til at gå tabt i formel kommunikation på organisationsniveau.

Historier spiller en grundlæggende rolle for, hvordan man lærer. De er med til at skabe en følelsesmæssig reaktion, som gør det lettere at huske det, der læres. Du kan puste liv i cybersikkerhedsbudskaberne og gøre dem nemmere for folk at forholde sig til i deres dagligdag. Ved at gøre historien relevant for slutbrugeren øger du i høj grad chancen for, at den pågældende husker oplysningerne, og din organisations overordnede sikkerhedstilstand forbedres. Kapitel 5 forklarer mere indgående, hvordan du kan inddrage storytelling i din kampagne.

Få opdateret din politikstyring

Politikker er afgørende for at fastlægge grænser for acceptabel adfærd for enkeltpersoner, processer, relationer og transaktioner i din organisation. De giver en governance-ramme, identificerer risici og hjælper med at fastlægge compliance, hvilket er vigtigt i nutidens stadig mere komplekse lovgivningsmæssige landskab.

Et effektivt system til forvaltning af politikker er et system, der har en konsekvent metode til at udforme politikker, giver struktur til organisationens procedurer og gør det nemmere at spore attestering og medarbejdernes svar. Dette system kan således hjælpe dig med at strømline interne processer, påvise overholdelse af lovkrav og på effektiv vis fokusere på de områder, der udgør den største risiko for datasikkerheden.

Start nu med forberedelserne til et databrud

Hvis du endnu ikke er begyndt at forberede dig på et brud på datasikkerheden, så er tiden inde. Milliarder af fortrolige oplysninger er blevet eksponeret, og ifølge IBM er de globale gennemsnitlige omkostninger ved et databrud steget til hele 3,92 millioner dollars.

Det er ikke længere et spørgsmål om, "hvorvidt" din organisation vil blive angrebet, men "hvornår". Du skal begynde at forberede dig på det uundgåelige og udarbejde en plan, der sikrer, at de nødvendige skridt træffes, når der opstår brud på sikkerheden.

Etablering af en effektiv responsplan hjælper med at uddanne og informere medarbejderne, forbedre organisationsstrukturerne, øge kundernes og interessenternes tillid og reducere potentielle økonomiske skader eller skader på omdømmet efter et brud.

TIP

Du skal jævnligt teste din beredskabsplan for databrud for at identificere eventuelle svagheder og sikre, at alle i dit team forstår, hvilket ansvar de har, både når de skal forberede sig på og reagere på et brud på datasikkerheden.

Inddrag Cyber Security Champions

Cybersikkerhed handler ikke bare om teknologi. Dine medarbejdere spiller en vigtig rolle med hensyn til at forsvare din organisation og identificere trusler, der kan udgøre en trussel mod sikkerheden.

At udnævne Cyber Security Champions er en god måde at give medarbejderne mere indflydelse og forsyne dem med de færdigheder, der er nødvendige for at forhindre et cyberangreb. Ifølge National Cyber Security Centre har halvdelen af alle organisationer, der har været udsat for et cyberangreb, konstateret, at de mest forstyrrende trusler blev rapporteret direkte af medarbejderne i stedet for at blive opfanget automatisk af software.

Cyber Security Champions behøver ikke at være tekniske eksperter. Deres bidrag handler mere om at sætte det menneskelige præg på din sikkerhedsstrategi og få hjælp fra medarbejdere, der er engageret i at øge awareness og gennemføre god praksis for cybersikkerhed.

Kapitel 3 giver specifikke tips til, hvordan du identificerer og udnytter din organisations champions.

Tænk på din forsyningskæde

For mange organisationer er forsyningskæden det svageste led i deres cybersikkerhedsforsvar. I stedet for at angribe en organisation direkte vil cyberkriminelle forsøge at kompromittere en organisations kritiske netværk og systemer ved at udnytte huller i dens forsyningskædeprocesser og -systemer.

Forsyningskæder er en vigtig del af forretningsaktiviteterne, men ofte er disse netværk store og forskelligartede og strækker sig over en lang række forskellige lande. Disse leverandører har typisk ikke det samme robuste cybersikkerhedsforsvar, hvilket betyder, at de har mange svage punkter, som cyberkriminelle kan udnytte.

Nogle af de største brud på datasikkerheden i nyere tid er sket som følge af angreb på forsyningskæden. Et godt eksempel er databruddet hos Target i 2014, hvor over 70 millioner kunders personlige oplysninger blev kompromitteret. Ved at iværksætte et phishing-angreb på en af organisationens serviceleverandører kunne angriberne få adgang til Targets betalingskortlæsere.

Alle leverandører, der har forbindelse til din organisation, udgør en potentiel risiko, så det er vigtigt, at du foretager detaljerede risikovurderinger af tredjeparter for at afhjælpe eventuelle mangler, der kunne udgøre en trussel mod organisationens sikkerhed. Det kan hjælpe med at afgøre, hvilke sikkerhedsforanstaltninger der skal træffes for at beskytte dine data.

I kapitel 3 undersøges det, hvordan du kan udvide din kampagne til også at omfatte leverandører.

Udfør passende opsyn og regelmæssig gennemgang

Trusselslandskabet udvikler sig hele tiden, så dit program for cybersikkerheds-awareness skal udvikle sig i takt hermed. Det er vigtigt at foretage en regelmæssig gennemgang af medarbejdernes parathed for at identificere eventuelle svage punkter og fastslå, om de nuværende politikker og træningsudbuddet skal opdateres.

For at sikre compliance i forhold til tilsynsmyndighederne er bedste praksis at dokumentere resultaterne af alle gennemgange og sørge for at følge op på alle anbefalinger til afhjælpning af risici. Uden disse regelmæssige revisioner afspejler dit program for cybersikkerheds-awareness måske ikke rigtigt trusselslandskabet og kan gøre din organisation sårbar over for angreb.

CYBER SECURITY AWARENESS THAT YOUR STAFF WILL LOVE

www.metacompliance.com

Opret en kultur med forbedret sikkerheds-awareness

Sikkerhedstrusler udvikler sig og bliver mere og mere avancerede. Traditionelle teknologiske forsvarsmekanismer er ikke nok til at gøre en organisation sikker mod sit svageste sikkerhedsled – den menneskelige faktor. Menneskets natur er en alvorlig sikkerhedsrisiko, og cyber-kriminelle ved, hvordan de udnytter den. Hjælpen er lige ved hånden i *Cybersikkerheds-awareness For Dummies*, din vejledning til strategier, udfordringer og de bedste måder at ændre brugeradfærd i en organisation, så den kan genkende og håndtere cybersikkerhedstrusler og beskytte værdifulde oplysninger og aktiver.

Inde i...

- Find ud af, hvordan du kan skabe cybersikkerheds-awareness
- Overhold strenge lovmæssige krav
- Få medarbejderne engageret med relevant og rollespecifik træning
- Integration af politikstyring i sikkerheds-awareness-programmer
- Sørg for at få ledelsesmæssig støtte til sikkerheds-awareness-kampagner

MetaCompliance®

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-89933-4
Not For Resale

for dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.