CYBERSIKKERHED

EN HÅNDBOG OM DE GRUNDLÆGGENDE PRINCIPPER

CYBERSIKKERHED...

... GÆLDER ALLE ORGANISATIONER.

Cyberkriminelle angriber organisationer af alle størrelser og typer, derfor kan ingen organisationer i dag se sig fri for truslen om cyberangreb.

Du kan beskytte din organisation mod truslen, ved at praktisere grundlæggende principper for cybersikkerhed.

TRUSTWORKS

RETHINKING IT AND BUSINESS

BESKYT FILER OG ENHEDER

Cyberkriminelle vil forsøge at få adgang til følsomme data i din organisation.

Her er seks grundlæggende måder at beskytte dine filer og enheder.

Hold øje med bokse markeret med  *i håndbogen. De indeholder konkrete sikkerhedstiltag du kan implementere i din organisation.*

Hold din software opdateret

Dette inkluderer apps, webbrowsere og operativsystemer på dine enheder. Indstil disse til automatisk opdatering, så du ikke går glip af vigtige sikkerhedsopdateringer.

Sikkerhedskopier dine data

Udfør regelmæssige sikkerhedskopier af vigtige filer. Opbevar dem på eksterne harddiske eller i skyen. Sørg for, at fysiske dokumenter opbevares sikkert.

Krypter dine enheder

Krypter alle enheder og medier, der indeholder følsomme data. Dette omfatter laptops, tablets, smartphones, eksterne drev, sikkerhedskopier og cloud-løsninger.

Brug stærke adgangskoder

Brug adgangskoder til alle laptops, tablets og smartphones. En stærk adgangskode skal som minimum bestå af 12 tegn og indeholder en kombination af store og små bogstaver samt tal og symboler. Begræns antallet af mislykkede loginforsøg.

Kræv multifaktorgodkendelse

Kræv multifaktorgodkendelse for at få adgang til områder af dit netværk med følsomme data. Dette tilføjer et ekstra lag sikkerhed ud over blot at logge ind med en adgangskode, som for eksempel en midlertidig kode sendt til en smartphone eller en fysisk sikkerhedsnøgle, der indsættes i en computer.

SÆT SIKKERHED PÅ DAGSORDENEN

Mange organisationers største sikkerhedsværdi ligger i medarbejderne.
For at styrke denne værdi er der flere forholdsregler man kan tage, herunder:

Træn dine medarbejdere

Afhold løbende træningssessioner for medarbejderne i din organisation. Opdater disse regelmæssigt, og vær opmærksom på nye risici og sårbarheder. Hvis en medarbejder er forhindret i at deltage, bør du overveje at begrænse adgangen til netværket, indtil træningen er gennemført.

Hav en handlingsplan

Hav en plan for hvis din organisation bliver udsat for cyberangreb.
Denne plan skal indeholde procedurer for sikkerhedskopiering af data og opretholdelse af drift, herunder kontakt til relevante interessenter ved databrud.

Gør rapportering nemt

Medarbejderne i din organisation skal være klar over, hvordan de skal reagere ved mistanke om cyberangreb. Det skal være nemt og let tilgængeligt for alle medarbejderne i organisationen at se hvem de skal rapportere til, og hvilke oplysninger de skal give.

BESKYT DIT TRÅDLØSE NETVÆRK

Beskyt din router

Skift standardnavnet og adgangskoden på routeren. Slå fjernadministration fra, og log ud som administrator, når routeren er opsat.

Brug som minimum WPA2 kryptering

Sørg for, at din router understøtter og har aktiveret WPA2 eller WPA3 kryptering. Kryptering beskytter trafikken mellem din router og dine enheder og forhindrer, at uvedkommende kan få adgang til dine data.

FORSTÅ

CIS 18 RAMMEVÆRKET V.8

Du har måske hørt om CIS 18, men hvad er det egentlig?

Og er det relevant for din organisation?

CIS 18 er et rammeværk, der tilbyder en systematisk tilgang til at forbedre cybersikkerheden i din organisation.

CIS 18 er udviklet af Center for Internet Security (CIS) og består af 18 specifikke sikkerhedskontroller. Rammeværket er særligt velegnet til organisationen, der har behov for at prioritere tekniske sikkerhedskontroller og ønsker en hurtig implementering.

BESKYT DIN ORGANISATION MED

CIS 18

CIS 18-kontrollerne fungerer som en vejledende ramme, der hjælper med at beskytte din organisations netværk, systemer og data mod almindelige cybertrusler.
Her er tre grunde til at implementere CIS 18 i din organisation.

En ramme for prioritering

CIS 18-kontrollerne giver en prioriteret liste over sikkerhedstiltag, som hjælper din organisation med at fokusere på de mest kritiske foranstaltninger. Desuden kræver CIS 18 færre ressourcer end andre anerkendte rammeværker, hvilket gør det særligt attraktivt for små og mellemstore organisationer.

En standardiseret tilgang til sikkerhed

CIS 18-kontrollerne tilbyder en ensartet og standardiseret tilgang til cybersikkerhed, hvilket sikrer, at hele organisationen arbejder ud fra et fælles udgangspunkt. Dette skaber afdelinger med fælles procedurer og sprog.

Branchespecifikke krav og standarder

Ved at gøre sikkerhed målbar kan du nemmere overvåge organisationens sikkerhedsmodenhed og implementere løbende forbedringer. CIS 18-kontrollerne kan på den måde understøtte overholdelse af branchespecifikke lovkrav og standarder.

FIND DET RETTE NIVEAU

CIS 18-kontrollerne er opdelt i implementeringsgrupper (IG'er), som guider din organisation i at prioriterer de mest kritiske sikkerhedsforanstaltninger først.

Implementeringsgruppe 1 (IG1)

Består af 56 sikkerhedstiltag og er rettet mod mindre organisationer med begrænsede ressourcer og få medarbejdere. Implementering af IG1 udgør den basale cybersikkerhed og danner minimumsgrundlaget for alle organisationer, uanset størrelse og kompleksitet.

Implementeringsgruppe 2 (IG2)

Omfatter yderligere 74 sikkerhedstiltag og er målrettet mellemstore og store organisationer med kompleks infrastruktur, mange medarbejdere og interne ressourcer til håndtering af cybersikkerheden. En stor del af danske organisationer og offentlige institutioner vil have behov for dette implementeringsniveau.

Implementeringsgruppe 3 (IG3)

Tilføjer yderligere 23 sikkerhedstiltag og er rettet mod store organisationer med høj risiko eller organisationer, der skal overholde særlige lovkrav og standarder. Tiltagene beskytter mod avancerede og målrettede cyberangreb og er velegnede til komplekse IT-systemer, der kræver ekstra sikkerhed.

FORSTÅ

NIST CSF 2.0

Skal du arbejde internationalt eller med amerikanske organisationer?

Så kan NIST CSF være det foretrukne rammeværk.

NIST CSF 2.0 er et rammeværk udviklet af den amerikanske organisation NIST til at hjælpe alle typer organisationer med at styrke cybersikkerheden – ikke kun kritisk infrastruktur, som rammeværket oprindeligt var tiltænkt.

Den nyeste version indeholder en vejledning og en samling af ressourcer, der støtter organisationer i at opfylde deres cybersikkerhedsmål med et særligt fokus på governance og leverandørstyring.

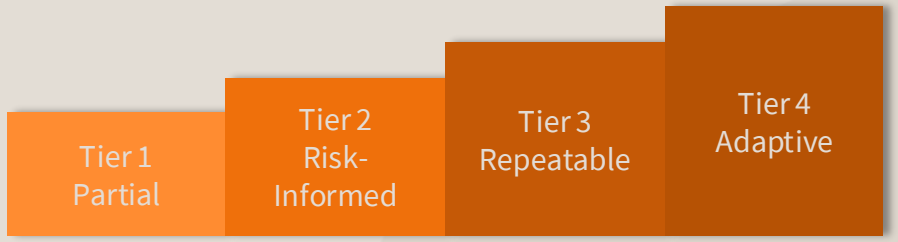
STYRK CYBERSIKKERHEDEN I DIN ORGANISATION MED NIST CSF 2.0

Oprindeligt blev NIST CSF udviklet til kritisk infrastruktur som energi og transport, men det er nu bredt anvendeligt og kan tilpasses forskellige typer organisationer, både offentlige og private.

NIST CSF kan tilpasses, så rammeværket ikke er en "one-size-fits-all"-løsning. I stedet kan det skræddersys til organisationers unikke risikoprofil, forretningsmål og ressourcer.

NIST CSF's modenhedsniveauer, eller *Tiers,* er designet til at hjælpe organisationer med at vurdere, hvor modent deres cybersikkerhedsniveau er og hvor effektivt de håndterer risici.

Der er fire niveauer, som spænder fra grundlæggende til avanceret modenhed. Disse hjælper organisationer med at forstå deres nuværende position og identificere mål for forbedring.



NIST CSF RAMMEVÆRKET BYGGER PÅ FEM TRIN

Govern omhandler det ISMS- eller governance-setup man har valgt at benytte i sin organisation. Det er også her man finder modenhedsstyring, leverandørstyring mv.

Identify vedrører organisationens behov for at have overblik over sine aktiver, forstå de risici, man står over for og planlægge, hvordan risici og trusler skal håndteres.

Protect beskriver de midler, man anvender for at beskytte sig mod risici og trusler.

Detect handler om de værktøjer og teknologier, organisationen bruger til at opdage trusler og potentielle brud på cybersikkerheden.

Respond omfatter de værktøjer, som organisationen har implementeret til at håndtere brud på cybersikkerheden, herunder beredskabsplanlægning.

Recover beskriver, hvordan organisationen genvinder eller genskaber aktiver og driftsstabilitet efter et brud på informationssikkerheden.

FORSTÅ

ISO 27001 V. 2022

Mangler din organisation en holistisk ledelsesramme til at styre informationssikkerheden?

Så kunne ISO 27001 godt være svaret.

ISO 27001 er en internationalt anerkendt standard udviklet af International Organization for Standardization (ISO). Standarden udgør en struktureret ramme for oprettelse og vedligeholdelse af et Information Security Management System (ISMS).

Rammeværket tilbyder en holistisk tilgang, der dækker både tekniske, organisatoriske, fysiske og menneskelige aspekter af informationssikkerhed. ISO 27001 kan anvendes af organisationer af alle størrelser og inden for alle brancher.

VÆRD AT VIDE OM ISO 27001

ISO 27001 består af 93 foranstaltninger fordelt på fire hovedområder, som din organisation kan implementere for at sikre en helhedsorienteret tilgang til informationssikkerhed.

Organisatoriske foranstaltninger

Disse foranstaltninger omfatter etablering af klare sikkerhedspolitikker, procedurer og processer i organisationen. Dette inkluderer dokumenterede roller og ansvar for informationssikkerheden.

Personrelaterede foranstaltninger

Disse foranstaltninger handler om at håndtere risici knyttet til menneskelige faktorer ved at sikre, at medarbejderne er bevidste om deres ansvar i forbindelse med at opretholde informationssikkerheden i organisationen. Dette omfatter blandt andet kontinuerlig træning af medarbejdere.

Fysiske foranstaltninger

Disse foranstaltninger retter sig mod at beskytte organisationen mod uautoriseret adgang. Dette omfatter sikring af lokaler, adgangskontrol, beskyttelse af serverrum, fysiske dokumenter og øvrige fysiske aktiver.

Teknologiske foranstaltninger

Disse foranstaltninger omfatter implementering af sikkerhedstiltag som adgangskontrol, kryptering og firewall-beskyttelse samt sikring af, at systemer og software løbende opdateres og har tilstrækkelig kapacitet til at imødekomme organisationens sikkerhedskrav.

Din organisation kan blive ISO 27001 certificeret

For at blive certificeret i ISO 27001 skal din organisation gennemgå sikkerheden med en ekstern audit, der kontrollerer, at organisationen overholder standardens krav.

En certificering sender et signal til kunder og samarbejdspartnere om, at organisationen tager informationssikkerhed alvorligt og overholder internationale standarder.

arba

Er du interesseret i at løfte informationssikkerheden i din organisation?

Prøv Arba-platformen!

Arba-platformen er en komplet værktøjskasse, der hjælper din organisation med at implementere og dokumentere sikkerhedsforanstaltninger i overensstemmelse med blandt andet CIS18, NIST CSF og ISO 27001.

Med en risikobaseret tilgang sikrer Arba-platformen at sikkerhedsniveauet i din organisation løftes og adresserer de unikke aspekter af din organisations risikolandskab.

Vil du vide mere?
Kontakt os eller book en demo: arba.dk

FYSISK SIKKERHED

Den fysiske sikkerhed i din organisation danner grundlaget for cybersikkerheden.

Hvis din organisation ikke formår at leve op til standarderne inden for fysisk sikkerhed, kan det resultere i brud på cybersikkerheden og dermed lækage af følsomme data.

Disse brud kan både opstå fra menneskelige fejl, for eksempel:

En medarbejder, der ubevidst lukker en uautoriseret person gennem en sikkerhedsdør.

En uautoriseret person, der under et besøg i organisationen får adgang til et serverrum.

En medarbejder, der smider fortrolige dokumenter i en skraldespand uden at makulerer dem.

En medarbejder, der forlader sin ulåste computer på sin arbejdsstation.

FOREBYG FYSISKE SIKKERHEDSBRUD

Uanset om det handler om harddiske, USB-nøgler, laptops eller andre enheder, der indeholder følsomme data, er det vigtigt aktivt at beskytte disse.
Her er nogle centrale måder, du kan minimere risikoen for brud på din organisations fysiske sikkerhed.

Sikker opbevaring

Opbevar fysiske dokumenter eller enheder, der indeholder følsomme data, i et aflåst skab eller rum.

Begræns fysisk adgang

Begræns adgangen til skabe og rum med følsomme data eller udstyr til de medarbejdere, med et reelt behov. Implementer adgangskontrolsystemer, såsom nøglekort eller adgangskoder.

Påmind dine medarbejdere

Mind regelmæssigt medarbejderne i din organisation om ovenstående. Påmind derudover om aldrig at efterlade dokumenter og enheder med følsomme data uden opsyn.

Hold overblik

Registrer og hold overblik over enheder, der indeholder følsomme data. Hold styr på, hvem der har adgang til disse. Opbevar kun følsomme data, så længe det er nødvendigt.

BESKYT DATA PÅ DINE ENHEDER

Selvom din organisation implementerer fornuftige foranstaltninger for fysisk sikkerhed, er der dog stadig en risiko for, at uvedkommende kan tilegne sig adgang til organisationen. Risikoen for databrud mindskes dog betydeligt, hvis følsomme data beskyttes på enheder. Her er nogle måder til at sikre dine data.

Kræv komplekse adgangskoder

Alle brugere bør oprette adgangskoder med en kombination af store og små bogstaver, tal og specialtegn. Overvej at bruge en adgangskodeadministrator.

Brug multifaktorgodkendelse

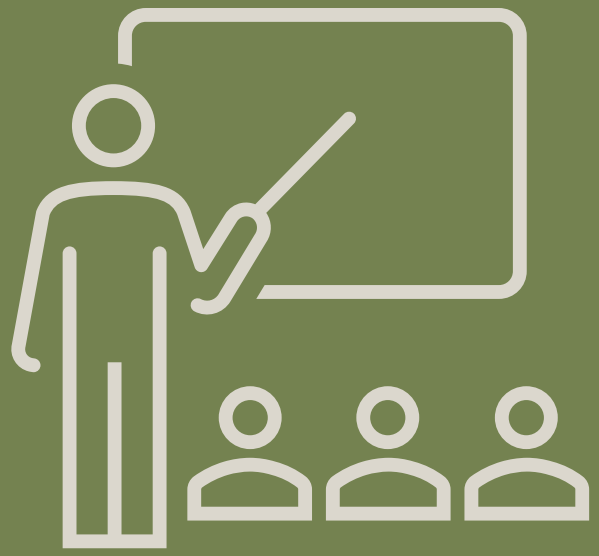
Implementer multifaktorgodkendelse for at få adgang til områder af dit netværket med følsomme oplysninger. Dette kræver et ekstra trin ud over blot at logge ind med en adgangskode, såsom en midlertidig kode på en smartphone eller en fysisk sikkerhedsnøgle, der indsættes i en computer.

Begræns loginforsøg

Indstil systemer til at begrænse antallet af mislykkede loginforsøg.

Krypter medier

Krypter alle bærbare medier, såsom computere og USB-nøgler, der indeholder følsomme oplysninger. Krypter også alle følsomme data, der deles uden for virksomheden, f.eks. med en revisor, eksterne konsulenter eller tjenesteudbyder.



UDDAN DINE MEDARBEJDERE

I FYSISK SIKKERHED

Inkluder fysisk sikkerhed i dine medarbejderes regelmæssige uddannelse og kommunikation. Mind dine medarbejdere om nedenstående punkter.

Makuler dokumenter

Alle skal være opmærksomme på, at fortrolige dokumenter bliver makuleret korrekt, før de smides ud.

Slet data korrekt

Instruer medarbejdere i at slette data korrekt fra deres enheder. Brug eventuelt software til at slette data, inden enheder doneres eller bortskaffes. Stol ikke blot på at 'slette' dokumenter, da dette ofte ikke fjerner dem permanent fra enheden.

Husk sikkerheden på alle lokationer

Fokus på sikkerhed i din organisation skal bibeholdes, uanset om medarbejdere arbejder hjemmefra eller er på forretningsrejse.

Kend handlingsplanen

Alle medarbejdere skal være bevidste om, hvad de skal gøre, hvis udstyr eller dokumenter mistes eller bliver stjålet. Dette omfatter at kende både de nødvendige skridt for at minimere skaden, samt de ansvarlige personer, der skal informeres.

LEVERANDØRSIKKERHED

Dine leverandører kan have adgang til følsomme oplysninger om din organisation.

Derfor skal dine leverandører også beskytte deres enheder og netværk. Overvej for eksempel, hvad der sker, hvis din revisor, som har adgang til alle dine finansielle data, mister sin computer, eller hvis en leverandør med adgang til dit netværk bliver hacket.

Konsekvensen kan være, at følsomme oplysninger om din organisation og dine kunder ender i forkerte hænder.

OVERVÅG
DINE LEVERANDØRER

Skriv det ned
Inkluder specifikke sikkerhedskrav og standarder i dine kontrakter med leverandører. Sørg for, at de sikkerhedskrav, der er afgørende for din organisation, ikke kan fraviges.

Tjek overholdelse
Gør det muligt at udføre sikkerhedsrevisioner på dine leverandører for at sikre, at de overholder dine krav. Stol ikke udelukkende på deres udsagn.

Foretag ændringer efter behov
Cybertrusler kan ændre sig. Sørg for, at dine leverandører holder deres sikkerhed opdateret.

BESKYT DATA I DIN ORGANISATION
MOD LEVERANDØR-FEJL

Begræns adgang
Implementer adgangskontroller på databaser med følsomme oplysninger. Begræns adgangen til et ”need-to-know”-princip og kun i den periode, hvor en leverandør har brug for adgang.

Kræv multifaktorgodkendelse
Få leverandører til at øge deres sikkerhed ved at kræve multifaktorgodkendelse. Ud over en adgangskode skal de bruge en midlertidig kode på en smartphone eller en fysisk sikkerhedsnøgle, der indsættes i en computer.

Beskyt dit netværk
Kræv, at dine leverandører bruger stærke adgangskoder med mindst 12 tegn og med en blanding af tal, symboler samt store og små bogstaver. Genbrug aldrig adgangskoder, del dem ikke, og begræns antallet af mislykkede loginforsøg for at reducere risikoen for at, adgangskoden kan gættes.

Krypter data
Krypter dine data, når de overføres mellem systemer, og når de opbevares på servere eller enheder.

HVIS DIN LEVERANDØR HAR ET DATABRUD

Bekræft at leverandøren har en løsning

Sørg for, at leverandøren retter op på sårbarhederne og sikrer, at dine oplysninger vil være beskyttede fremover, hvis din organisation beslutter sig for at fortsætte samarbejdet med leverandøren.

Rapporter angrebet

Undersøg, hvem du har rapporteringspligt til, og underret relevante interessenter.

Underret kunder

Hvis det er nødvendigt, underret dine kunder, partnere og andre interessenter om bruddet og de trin, du tager for at håndtere det.

RANSOMWARE

En medarbejder i din organisation modtager en e-mail.

Den ser legitim ud – men med ét klik på et link eller ét download af en vedhæftet fil bliver alle i dit netværk låst ude. Linket downloader software, der holder dine data som gidsel.

Du er nu blevet ramt af et ransomware-angreb.

De, der har angrebet din organisation, kræver penge eller kryptovaluta, men selv hvis du betaler, er der ingen garanti for, at de vil tilbagelevere dine data. I mellemtiden er nødvendige oplysninger for at opretholde organisationens drift samt følsomme oplysninger om dine kunder og medarbejdere nu i kriminelles hænder.

Ransomware-angreb kan ramme hårdt uanset størrelsen på din organisation.

RANSOMWARE, HVORDAN?

Cyberkriminelle kan starte et ransomware-angreb på forskellige måder. Dette sker ofte gennem:

Falske e-mails

Cyberkriminelle sender e-mails med skadelige links og vedhæftede filer, som kan kompromittere dine data og netværk. Disse phising-emails udgør størstedelen af ransomware-angreb.

Inficerede hjemmesider

Inficerede hjemmesider, der automatisk downloader skadelig software til din enhed, uden du er bevidst om det.

Sårbarhed i server

Cyberkriminelle kan udnytte sikkerhedshuller i din server til at få adgang til dit netværk og installere ransomware.

Online annoncer

Cyberkriminelle kan placere skadelige annoncer på online platforme, som downloader skadeligt software.
Disse kan forekomme selv på hjemmesider, du normalt har tillid til.

BESKYT DATA I DIN ORGANISATION

Hav en plan

Sørg for at have en plan for at holde din organisation kørende under et ransomware-angreb. Nedskriv planen, og del den med alle relevante medarbejdere.

Sikkerhedskopier dine data

Tag regelmæssige sikkerhedskopier af vigtige data, og opbevar dem sikkert, enten offline eller i en krypteret cloud-løsning.

Hold dine systemer opdateret

Installer altid de nyeste patches og opdateringer. Overvej yderligere sikkerhedsforanstaltninger såsom e-mail-godkendelse og firewalls, og sørg for, at disse er sat til automatisk opdatering på computere. På mobile enheder skal disse muligvis opdateres manuelt.

Uddan medarbejdere

Træn dine medarbejdere i at undgå phishing-svindel, og informer dem om de mest almindelige metoder, som hackere bruger til at inficere computere og enheder. Inkluder tips til at opdage og beskytte mod ransomware i regelmæssige træningssessioner.

HVIS DU BLIVER ANGREBET

Begræns skaden

Afbryd straks de inficerede computere eller enheder fra dit netværk. Hvis dine data er blevet stjålet, skal du handle hurtigt for at beskytte din organisation og underrette de personer eller organisationer, der kan være påvirket.

Rapporter angrebet

Undersøg, hvem du har rapporteringspligt til og underret relevante interessenter.

Underret kunder

Hvis dine data eller personlige oplysninger er blevet kompromitteret, skal du sørge for at underrette de berørte parter – de kan være i fare for identitetstyveri.

Hold din organisation kørende

Hvis din organisation er blevet angrebet, er det tid til at implementere den nedskrevne plan for at opretholde organisationens drift.

Skal jeg betale løsesummen?

Generelt anbefales det ikke at betale løsesummen. Dog er det er op til organisationen at vurdere, om risikoen og omkostningerne ved at betale er berettigede i forhold til muligheden for at få organisationens data tilbage.
Vær opmærksom på, at dette område kræver professionel advisering, da beslutningen indebærer overvejelse af mange faktorer og risici.

PHISHING

Du modtager en e-mail, der ser ud til at være fra en, du kender.

Det ser ud til at være fra en af dine leverandører, som beder dig om at klikke på et link for at opdatere din organisations kontooplysninger. Skal du klikke?

Måske ser det ud, som om at det er fra din chef, der beder om din adgangskode. Skal du svare?

I begge tilfælde er det sandsynligvis ikke en god idé,
da disse kan være forsøg på phishing.

SÅDAN FUNGERER PHISHING

Du får en e-mail eller SMS

Det ser ud til at være fra en, du kender, der beder dig om at klikke på et link eller give din adgangskode, forretningsbankkonto eller andre følsomme oplysninger.

Den ser ægte ud

Det er nemt at forfalske logoer og lave falske e-mailadresser. Cyberkriminelle bruger ofte kendte virksomhedsnavne eller udgiver sig for at være nogen i dit netværk.

Det er presserende

Beskeden opfordrer dig til at handle hurtigt – ellers vil det have alvorlige konsekvenser.

Hvis du klikker

Klikker du på et link, kan cyberkriminelle installere ransomware eller anden skadelig software, der kan blokere adgang til dine data og potentielt sprede sig til hele organisationens netværk.

HVAD DU KAN GØRE

FØR DU KLIKKER

Undersøg afsenderen nærmere

Slå hjemmesiden eller telefonnummeret op på virksomheden eller personen bag sms'en eller e-mailen. Sørg for, at du kontakter den rigtige virksomhed, så du undgår at downloade malware eller blive offer for svindel.

Tal med nogen

At tale med en kollega kan hjælpe dig med at afgøre, om beskeden er troværdig eller et forsøg på phishing. Del din oplevelse med dine kollegaer, da phishing-angreb ofte rammer mere end én medarbejder i organisationen.

Foretag et opkald, hvis du er i tvivl

Ring til den leverandør, kollega eller kunde, der står som afsender på e-mailen eller sms'en, for at få bekræftet, at de har brug for oplysninger fra dig. Det er vigtigt, at du benytter et nummer, du ved er korrekt, og ikke det nummer, der er oplyst i e-mailen eller sms'en.

BESKYT DATA I DIN ORGANISATION

Sikkerhedskopier din data

Lav regelmæssig sikkerhedskopier af dine data, og sørg for, at de opbevares på eksterne harddiske eller i skyen. På den måde sikre du, at du kan gendanne dine data i tilfælde af et phishing-angreb.

Informer dine medarbejdere

Del information om phishing med dine medarbejdere. Husk, at phishing-svindlere ofte ændrer deres metoder, så sørg for at inkludere tips til også at identificere nyeste phishing-forsøg i den regelmæssige træning.

Hold din sikkerhed opdateret

Installer altid de nyeste patches og opdateringer. Overvej yderligere sikkerhedsforanstaltninger, såsom e-mail-godkendelse eller Intrusion Prevention System (IPS), og sørg for, at disse er sat til automatisk opdatering på computere. På mobile enheder skal disse muligvis opdateres manuelt.

Brug e-mail-godkendelse

Brug e-mail-godkendelsesteknologi til at forhindre phishing-e-mails i at nå medarbejdernes indbakke i første omgang.

HVIS DU FALDER FOR ET PHISHING-ANGREB

Tal med dine kolleager

Del din oplevelse med dine kollegaer. Phishing-angreb sker ofte for mere end én medarbejder i organisationen.

Begræns skaden

Skift straks alle kompromitterede adgangskoder og afbryd forbindelsen fra netværket på alle computere eller enheder, der er inficeret med malware.

Følg organisationens procedure

Disse procedure skal inkluderer information omkring underrettelse til ansvarlige medarbejdere i din organisation eller leverandører, der hjælper dig med IT.

Underret kunder

Hvis dine data eller personlige oplysninger er blevet kompromitteret, skal du sørge for at underrette berørte parter – de kan være i fare for identitetstyveri.

Rapporter angrebet

Undersøg hvem du har rapporteringspligt til og underret relevante interessenter.

E-MAIL SPOOFING

En cyberkriminel opretter en e-mailadresse, der ser ud til at være fra din organisation.

En cyberkriminel kan manipulere e-mailadresser og få dem til at ligne en e-mailadresse fra din organisation. Dette får e-mails til at fremstå som troværdige, selvom afsenderen i virkeligheden er en cyberkriminel. Metoden bruges ofte i forbindelse med phishing-angreb.

Formålet med e-mail spoofing er at afsløre følsomme oplysninger såsom adgangskoder, bankoplysninger, eller at overføre penge direkte til den cyberkriminelles konto.

Hvis et angreb lykkes, kan det medføre betydelige tab for din organisation, både økonomisk og i form af mistet tillid fra kunder og samarbejdspartnere.

BESKYT DATA

I DIN ORGANISATION

Brug e-mail-godkendelse

Når du opsætter din organisations e-mail, skal du sørge for, at din e-mailudbyder tilbyder en e-mail godkendelsesteknologi. Dette betyder, at når du sender en e-mail fra din organisations server, kan modtagerens server bekræfte, at e-mailen rent faktisk er fra dig. Dette gør det sværere for cyberkriminelle af sende falske e-mails på dine vegne.

Hold din sikkerhed opdateret

Installer altid de nyeste patches og opdateringer og sæt dem til at opdatere automatisk. Du kan overveje at beskytte yderligere ved at benytte et Intrusion Prevention System (IPS), der overvåger dit netværk for mistænkelig aktivitet og sender dig advarsler, hvis det er tilfældet.

Uddan dine medarbejdere

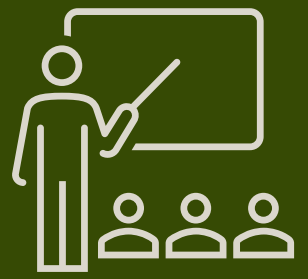
Uddan medarbejdere i at genkende og undgå e-mail spoofing ved at træne dem i nogle af de mest almindelige metoder, cyberkriminelle bruger for at komme i kontakt. Sørg for at inkludere tips til at opdage nye teknikker i e-mail spoofing.

HVIS DIN ORGANISATIONS E-MAIL ER SPOOFET

Underret kunder og samarbejdspartnere

Hvis du opdager, at nogen udgiver sig for at være fra din organisation, skal du underrette kunder og samarbejdspartnere så hurtigt som muligt – via telefonopkald, e-mail eller sociale medier.

Hvis du sender e-mails til dine kunder, skal du sørge for at sende disse uden links, for at undgå, at din e-mail ligner phishing-svindel. Påmind også dine kunder om ikke at dele personlige oplysninger via e-mail eller sms.



Rapporter det

Undersøg hvem du har rapporteringspligt til og underret relevante interessenter.

Brug oplevelsen

Brug denne oplevelse til at opdatere sikkerheden i din organisation og træne dine medarbejdere i at blive robuste overfor phishing-svindel.

TEKNISK SUPPORT-SVINDLERI

Du modtager et opkald, en pop-up eller en e-mail, der fortæller dig, at der er et problem med din computer.

Men det er sandsynligvis cyberkriminelle, der udgiver sig for at være teknisk supportpersonale fra velkendte virksomheder som Microsoft eller Apple. Deres mål er at få fat i dine penge, personlige oplysninger eller adgang til dine data.

SÅDAN FUNGERER

TEKNISK SUPPORT-SVINDLERI

Cyberkriminelle bruger mange tekniske termer for at overbevise dig om, at problemerne med din computer er reelle. De kan bede dig om at åbne filer eller køre en scanning på din computer – for derefter at fortælle dig, at resultaterne viser et problem … men der er i virkeligheden ikke noget.

Cyberkriminelle vil derefter:

Bede dig om at give dem fjernadgang til din computer, hvilket giver dem adgang til alle oplysninger, der er gemt på den, samt til de netværk computeren er forbundet til.

Installere skadelig software, der giver dem adgang til din computer og følsomme data. Det kan være brugernavne, adgangskoder og andre personlige oplysninger.

Prøve at tilmelde dig værdiløse antivirus- eller garantiprogrammer.

Bede om kreditkortoplysninger, så de kan fakturere dig for falske tjenester eller tjenester, der er tilgængelige gratis andre steder.

BESKYT DIN DATA

Vær opmærksom på uventede opkald

Hvis du modtager et opkald fra nogen, der påstår, at din computer har et problem, bør du straks lægge på. Uventede opkald om teknisk support er næsten altid svindel, selv hvis nummeret ser lokalt ud. Cyberkriminelle bruger ofte falske opkalds-id-oplysninger for at udgive sig for at være lokale eller betroede virksomheder.

Ignorér pop-up-beskeder

Hvis du modtager en pop-up-besked, der beder dig om at ringe til teknisk support, bør du ignorere den. Selvom nogle pop-up-beskeder om computerproblemer kan være legitime, bør du aldrig ringe til et nummer eller klikke på et link i en pop-up-besked, der advarer dig om et computerproblem.

Kontakt din udbyder direkte ved mistanke

Hvis du er bekymret for, at din computer har en virus, skal du kontakte sikkerhedsudbyder direkte ved at bruge telefonnummeret fra den officielle hjemmeside, din salgskvittering eller produktets emballage. Alternativt kan du kontakte en betroet sikkerhedsprofessionel.

Beskyt din enhed

Giv aldrig nogen din adgangskode, og tillad ikke fjernadgang til din computer for personer, der kontakter dig uopfordret.

HVIS DU BLIVER SVINDLET

Hvis uheldet er ude, er det vigtigste IKKE at ignorere situationen.

Efter at have kommunikeret hændelsen til den ansvarlige sikkerhedsprofessional i organisationen, er der visse handlepunkter, der skal gennemføres.

Skift din adgangskode

Hvis du har delt din adgangskode med en cyberkriminel, skal du ændre den på alle konti, der bruger denne adgangskode. Husk at oprette nye, unikke adgangskoder for hver konto. Overvej også, om du vil bruge en godkendt adgangskodeadministrator.

Kør antivirus-scanning

Kør en antivirus-scanning for at fjerne al skadelig software. Hvis du har brug for hjælp til dette, skal du kontakte en betroet sikkerhedsprofessionel.

Tjek din organisations netværk

Hvis den inficerede computer er forbundet til organisationens netværk, skal du eller en sikkerhedsprofessionel undersøge hele netværket for tegn på indtrængen.

Hold øje med kontoudtog

Hvis du har købt falske tjenester, skal du straks tjekke dine kontoudtog for betalinger, du ikke har godkendt. Fortsætmed at tjekke dine konti for at sikre, at cyberkriminelle ikke forsøger at opkræve dig på månedlig basis.

CYBERFORSIKRING

At komme sig efter et cyberangreb kan være rigtig dyrt!

Cyberforsikring er en mulighed, der kan beskytte din organisation mod tab som følge af et cyberangreb. Hvis du overvejer en cyberforsikring, bør du drøfte med din forsikringsagent, hvilken type forsikring der bedst passer til organisationens behov. Behovet afhænger af faktorer som antal medarbejdere, IT-systemer, og den potentielle effekt ved tab af data, herunder den skade, virksomheden kan lide efter et angreb.

Her er nogle generelle overvejelser ved indkøb af cyberforsikring:

OVERVEJ OM DIN POLICE SKAL DÆKKE:

- Juridisk rådgivning i forbindelse med overholdelse af datalovgivning.
- Gendannelse af mistede eller kompromitterede data.
- Dine data når de opbevares af tredjeparter.
- Juridisk rådgivning til at undersøge årsagen til bruddet.
- Gebyrer, bøder relateret til cyberhændelsen (f.eks. GDPR).
- Omkostninger og tabt fortjeneste i forbindelse med organisationens nedetid.
- Global dækning for cyberangreb, uanset hvor de finder sted i verden.
- Daglige backups af virksomhedens data
- Betaling af ransomware.
- Krisehåndtering i forbindelse med organisationens omdømme.

Herunder, første – eller tredjepartsdækning?

Førstepartsdækning

Førstepartsdækning omfatter din organisationens egne tab og omkostninger efter et cyberangreb.

Tredjepartsdækning

Tredjepartsdækning omfatter ansvar for tab og omkostninger, som en tredjepart pådrager sig på grund af et cyberangreb mod din organisation.

Overvej også om du hos din forsikring:

- Lever op til forsikringens krav for cybersikkerhed. Hvis ikke, er du muligvis ikke dækket.
- Kan blive forsvaret i en retssag eller regulerende undersøgelser efter databrud (se efter ordlyden ”pligt til at forsvare” hos forsikring).
- Har en hotline, der er tilgængelig 24 timer i døgnet, så du kan få øjeblikkelig hjælp, hvis du har mistanke om et cyberangreb.
- Har dækning ud over enhver anden relevant forsikring, du har, så du ikke står uden forsikring i tilfælde af overlap.

E-MAIL GODKENDELSE

E-mail godkendelse gør det sværere for cyberkriminelle at sende e-mails fra falske mailadresser.

Denne teknologi gør det muligt for modtagerserveren at bekræfte, om en e-mail virkelig stammer fra din organisation. E-mails, der ikke kan verificeres, kan enten blive blokeret, sendt til en karantænemappe eller rapporteret til dig. Dette hjælper med at mindske risikoen for e-mail spoofing og phishing-angreb ved at sikre, at kun legitime e-mails når dine medarbejdere.

VÆRD AT VIDE OM E-MAIL GODKENDELSE

Nogle webhostingudbydere giver dig mulighed for at opsætte din organisations e-mail ved hjælp af dit domænenavn.

Uden e-mail-godkendelse kan svindlere bruge din organisations domænenavn til at sende e-mails, der ser ud, som om de kommer fra din organisation.

Hvis din organisations e-mail benytter domænenavnet, skal du sikre dig, at din e-mailudbyder anvender følgende tre e-mail-godkendelsesværktøjer

Dit domænenavn kunne for eksempel være:

dinorganisation.com

Din e-mailadresse kunne dermed for eksempel være:

navn@dinorganisation.com

Det kræver tekniske færdigheder at indstille disse værktøjer korrekt, så de fungerer efter hensigten og ikke ved et uheld blokerer legitime e-mails. Hvis du ikke selv har den nødvendige tekniske viden, bør du sikre dig, at din e-mail-hostingudbyder kan opsætte dem for dig. Hvis udbyderen ikke tilbyder denne service eller hvis det ikke er inkluderet i deres serviceaftale, bør du overveje at skifte til en anden udbyder.

Sender Policy Framework (SPF)

SPF angiver, hvilke servere der har tilladelse til at sende e-mails ved din organisations domænenavn. Når du sender en e-mail fra navn@DinOrganisation.com, kan modtagerens server bekræfte, at afsenderens server er på en godkendt liste. Hvis serveren ikke er på listen, kan e-mailen blive markeret som mistænkelig.

Domain Keys Identified Mail (DKIM)

DKIM sætter en digital signatur på udgående post, så servere kan verificere, at en e-mail fra dit domæne rent faktisk blev sendt fra din organisations servere og ikke er blevet ændret undervejs.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

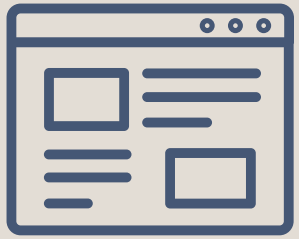
Hvor SPF og DKIM hjælper med at godkende afsenderadresser "bag kulisserne", sikrer DMARC, at den synlige "fra"-adresse stemmer overens med den faktiske afsenderdata. Det giver dig også mulighed for at bestemme, hvad der skal ske med mistænkelige e-mails fra dit domæne – om de skal afvises, markeres som spam, eller godkendes. Desuden kan DMARC sende dig besked, hvis der opstår problemer med sådanne e-mails.

ANSÆT EN WEB HOST

Har din organisation brug for en ny eller opgraderet hjemmeside?

Hvis du ikke selv har de nødvendige færdigheder til at opnå det ønskede resultat, kan du overveje at hyre en webhost-leverandør til at hjælpe med dette. Uanset om du vil opgradere din nuværende hjemmeside eller lave en ny, er der mange webhosting-løsninger at vælge imellem. Når du sammenligner disse tjenester, bør sikkerhed altid indgå som en vigtig faktor.

HVAD DU SKAL
KIGGE EFTER



E-mail godkendelse

Nogle webhostudbydere giver dig mulighed for at opsætte din e-mail ved hjælp af din organisations domænenavn.

Uden e-mail-godkendelse kan cyberkriminelle efterligne dit domænenavn og sende e-mails, der ser ud til at komme fra din organisation.

Hvis din organisations e-mail er opsat med dit domænenavn, skal du sikre dig, at din webhost tilbyder de førnævnte e-mail-godkendelsesværktøjer:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)

For mere se evt. kapitlet ”E-mail godkendelse”

Transport Layer Security (TLS)

TLS sikrer, at dine kunder lander på din ægte hjemmeside, når de indtaster din URL i søgefeltet.

Du har måske hørt om dens forgænger, Secure Sockets Layer eller SSL. TLS sørger også for, at de oplysninger, dine kunder deler med din hjemmeside, såsom personlige data, kreditkortnumre og adgangskoder, ikke kan opsnappes eller læses af uvedkommende under overførslen. Når TLS er korrekt implementeret på din hjemmeside, begynder din URL med https://.

Softwareopdateringer

Mange webhostudbydere tilbyder færdiglavede hjemmesider eller softwarepakker, der gør det hurtigt og nemt at opsætte en hjemmeside til din organisation. Det er dog afgørende, at din webhost bruger de nyeste versioner og holder sikkerhedsopdateringerne ajour. Sørg for at vide, hvordan du selv opdaterer hjemmesidens software, eller undersøg, om din webhost kan gøre dette for dig.

HVAD DU SKAL SPØRGE OM

Når du ansætter en webhost, bør du stille disse spørgsmål for at sikre at dine kunders oplysninger og din organisations data er beskyttet.

- Er TLS en del af hostingplanen? I så fald, hvem er ansvarlig for opsætningen?
- Er det muligt for min organisation at bruge eget domænenavn? I så fald, kan I hjælpe med opsætningen af SPF, DKIM og DMARC til e-mail-godkendelse? (Hvis ikke, bør du overveje at vælge en udbyder, der kan tilbyde denne support).
- Er de nyeste softwareversioner tilgængelige med din service, og hvem er ansvarlig for at holde softwaren opdateret? Hvis det er mit ansvar, er det nemt at udføre opdateringerne selv?
- Når hjemmesiden er opsat, hvem har mulighed for at foretage ændringer på hjemmesiden? Hvis jeg kan foretage ændringer selv, tilbyder I multifaktorgodkendelse for at sikre adgang?

SIKRET FJERNADGANG

Medarbejdere og leverandører kan have behov få adgang til dit netværk fra andre lokationer.

I disse situationer er dit netværks sikkerhed førsteprioritet. Sørg for, at medarbejdere og leverandører følger sikkerhedsstandarder, før de opretter forbindelse til dit netværk. Giv dem de nødvendige værktøjer for at gøre sikkerhed til en del af deres arbejdsrutine.

BESKYT DINE ENHEDER

Uanset om medarbejdere og leverandører bruger deres egne eller organisationens enheder til at oprette forbindelse til dit netværk fra andre lokationer, skal disse enheder være sikre. Sørg for, at dine medarbejdere og leverandører følger disse tips.

Skift standardnavn og adgangskode på din router

Skift altid forudindstillede adgangskoder og standardnavnet på din router. Sørg for at holde routerens software opdateret.

Overvej fulddiskkryptering

Når medarbejdere eller eksterne samarbejdspartnere bruger bærbare computere eller andre mobile enheder til at oprette forbindelse til din organisations netværk, er disse enheder ofte mere udsatte for tab eller tyveri. Overvej derfor fulddiskkryptering, og undersøg om denne mulighed findes i dit operativsystem.

Indstil din smartphone

Indstil din smartphone, så den ikke automatisk opretter forbindelse til offentlige Wi-Fi-netværk.

Installer antivirus

Installer antivirus på enheder, der opretter forbindelse til dit netværk, herunder også mobile enheder.

FORBIND SIKKERT

TIL NETVÆRKET FRA ANDRE LOKATIONER

Bruge mindst WPA2 kryptering

Sørg for at der bliver brugt en router med WPA2 eller WPA3 kryptering, når der oprettes forbindelse fra hjemmet. Kryptering beskytter information, der sendes over et netværk, så udefrakommende ikke kan læse den. WPA2 og WPA3 er de eneste krypteringsstandarder, der beskytter information sendt over trådløse netværk.

Kun bruge offentligt Wi-Fi i forbindelse med VPN

Dine medarbejdere bør kun bruge offentligt Wi-Fi, når de samtidig anvender et virtuelt privat netværk (VPN). Offentligt Wi-Fi giver ikke en sikker internetforbindelse alene. Medarbejderne kan få en personlig VPN-konto fra en VPN-udbyder, eller du kan overveje at hyre en leverandør til at oprette en virksomheds-VPN, som alle medarbejdere kan bruge.

FOREBYG MENNESKELIGE FEJL

Uddan dine medarbejdere.

Del organisationens politikker

Udarbejd politikker, der dækker grundlæggende aspekter af cybersikkerhed, og sørg for at dele dem med alle medarbejdere. Forklar vigtigheden af at følge disse politikker.

Informer om fjernadgang

Inkluder information om sikker fjernadgang i regelmæssige træninger, og informer nye medarbejdere om organisationens politikker for fjernadgang.

Sikre overholdelse af netværkssikkerhedskrav

Før en enhed – uanset om den er placeret hjemme hos en medarbejder eller på en leverandørs netværk – tilsluttes til dit netværk, skal du sikre, at den opfylder dine netværkssikkerhedskrav.

Informer om risiko

Fortæl dine medarbejdere om risikoen ved offentligt Wi-Fi

Giv dine medarbejdere værktøjer, der hjælper med at opretholde sikkerheden.

Kræv unikke, komplekse adgangskoder for at tilgå organisationens netværk, og undgå ubemandede, åbne arbejdsstationer.

Kræv multifaktorgodkendelse for at få adgang til områder af dit netværk, der indeholder følsomme oplysninger. Dette kræver yderligere trin ud over login med en adgangskode – såsom en midlertidig kode på en smartphone eller en nøgle, der indsættes i en computer.

Overvej at oprette en VPN, som medarbejdere kan benytte, når de opretter forbindelse eksternt til organisationens netværk.

Hvis du tilbyder Wi-Fi til gæster og kunder, skal du sikre, at dette er adskilt fra din organisations interne netværk.

Inkluder krav om sikkerhed i dine leverandørkontrakter, især hvis leverandøren skal oprette forbindelse til dit netværk eksternt.

HAR DU NOGLE SPØRGSMÅL?

Så står en af vores cybersikkerhedseksperter klar med et svar.

Kontakt os på hello@trustworks.dk

HÅNDBOG UDARBEJDET AF TRUSTWORKS CYBER SECURITY TEAM

Trustworks er en IT-transformationspartner, der skaber resultater i store og krævende digitale initiativer. Trustworks har omfattende erfaring med at levere strategisk udvikling og digitalisering indenfor grøn omstilling, den finansielle sektor, offentlig digitalisering og Pharma & Life science. Vi er en end-to-end partner fra idé til omstilling og implementering, og vores specialer er IT-arkitektur, forretningsanalyse, projektledelse, applikations modernisering, integrationer og systemudvikling.

TRUSTWORKS

RETHINKING IT AND BUSINESS