Erhvervshusene

E-bog: Sådan beskytter du din virksomhed mod de største cybertrusler

Sikkerhed i en digital verden

Med verdens ustabilitet og autoritære stater bag mange angreb, er truslen fra cyberkriminalitet større end nogensinde før. Danmark, som er et digitaliseret og tillidsbaseret land, er særligt sårbart, og nye teknologier gør hele tiden angreb lettere.

Spørgsmålet er derfor ikke længere, om din virksomhed bliver angrebet – men hvornår og hvordan, og om det også vil ramme den værdikæde, du er en del af.

Hvem gider at hacke en mindre virksomhed?

Tænker du, at din virksomhed er for lille eller for uinteressant til at blive hacket? Det er desværre en farlig misforståelse, som mange små og mellemstore virksomheder deler. Virkeligheden er nemlig den, at cyberkriminelle går efter alle i dag – både den enkelte borger, myndigheder og virksomheder i alle størrelser. De skelner ikke, om du har 5 eller 500 ansatte. Hackere ser digitale værdier – og ikke hvem du er. I nogle tilfælde kan SMV'er endda være et nemmere mål, fordi sikkerhedsforanstaltningerne ofte er ikke-eksisterende eller mangelfulde.

Cybertrusler kan lyde overvældende, men det værste, du kan gøre, er at ignorere problemet.

Du behøver ikke selv at være ekspert i cybersikkerhed. Det vigtigste er, at du tager de første skridt og allierer dig med nogen, der har erfaring og indsigt i, hvad der skal gøres. Cybersikkerhed handler ikke om at fjerne alle trusler, men om at være bedre forberedt og skabe tryghed for dine medarbejdere og din værdikæde.

Det kigger vi nærmere på i denne e-bog. Du får et indblik i de største trusler, SMV'er står overfor lige nu. Og du får konkrete råd til, hvordan du skaber en stærk sikkerhedskultur, og en køreplan for, hvordan du kommer i gang med at sikre din virksomhed.

De 3 største cybertrusler og sårbarheder

Et hackerangreb starter længe før, det faktisk sættes i gang – nogle gange måneder eller endda år i forvejen. Det starter med, at hackere finder interessante svagheder i virksomhedens systemer. Dernæst indsamler de relevante oplysninger og skaffer sig adgang. Først herefter aktiveres selve angrebet. Hver af disse faser udgør en potentiel sårbarhed, men det er også her, dit forsvar kan gøre en forskel.

Cybertruslerne udvikler sig i et hastigt tempo, og nye trusler kommer hele tiden til. Men overordnet er der tre typer af angreb, som går igen og igen.

PHISHING-ANGREB
RANSOMWARE ANGREB
FINANSIEL SVINDEL

1. Phishing-angreb

Phishing kan bruges i alle angrebets faser og sigter generelt mod at narre og manipulere mennesker til at udlevere oplysninger eller klikke på links, der giver hackeren adgang til dine data. Det er ofte e-mails, men det kan for eksempel også ske via SMS eller telefonopringninger.

Jo flere oplysninger hackerne har indsamlet, jo mere troværdige (og dermed farlige) kan phishing-angrebene blive.

Fx vil e-mailen kunne se ud til at komme fra en kendt medarbejder eller en kendt leverandør. Hackere bruger også AI til at få teksten til at fremstå professionelt, så det kan være vanskeligt at skelne phishing fra ægte e-mails.

Sådan kan du (måske) opdage en phishing-mail:

- Tjek sammenhængen: Virker beskeden troværdig? Er det en forespørgsel, du ville forvente? Er der indbygget et stress-element (kort tidsfrist)?
- Undersøg afsenderen: Kig nøje på e-mailadressen. Matcher den medsenderens identitet, eller ser den mærkelig ud? Læg mærke til ord der ligner – men er forkert stavet (f.eks. www.brobizz.com og www.brobizzz.com).
- Fører links derhen, hvor de siger: Hold musen over links (også gemt i billeder og videoer) i e-mailen uden at klikke. Se, om linket fører til et kendt og troværdigt domæne.

OBS - Mailen kan også komme fra den rigtige mailadresse, hvis afsenderen er blevet kompromitteret.

2. Ransomware-angreb

Ransomware er en af de største trusler i Danmark, som både kan have store økonomiske og operationelle konsekvenser. Ransomware er en form for malware (virus), som er designet til at kryptere dine data og gøre dem og dine systemer utilgængelige for dig.

Hackerne tilbyder "hjælpsomt" at låse dine data op igen – mod betaling af en stor løsesum. Disse angreb kan føre til alvorlige driftsforstyrrelser og i værste fald få virksomheden til at bukke under, hvis den aldrig formår at komme op at køre igen.

Hvordan beskytter du dig mod ransomware?

- Effektiv backup af essentielle data er altafgørende. Hvilke data, der er essentielle, og hvor ofte, der skal tages backup afhænger af den enkelte virksomheds situation. Sørg for at backuppen er adskilt fra driftssystemerne, så den ikke bliver inficeret sammen med dem og test backuppen regelmæssigt.
- Brug stærke adgangskoder og aktiver to-faktor-godkendelse på alle brugere.
- Sørg for, at dine systemer og software altid er opdaterede og beskyttede, så kendte sårbarheder er lukket.
- Alle forholdsregler om phishing gælder også her.

3. Finansiel svindel

Finansiel svindel er en alvorlig cybertrussel, der kan resultere i store økonomiske tab og skader på din virksomheds omdømme. Det kan ramme alle virksomheder – uanset størrelse og branche. Her forsøger hackere at manipulere sig til penge gennem avancerede svindelnumre, der udnytter teknologi, uklare interne procedurer og menneskelige fejl.

Et eksempel er "CEO fraud," hvor cyberkriminelle udgiver sig for at være en leder i virksomheden og f.eks. sender falske betalingsanmodninger til økonomiafdelingen.

Andre eksempler på finansiel svindel er falske fakturaer eller ændringer af bankoplysninger på modtagne købsfakturaer eller afsendte salgsfakturaer. De cyberkriminelle benytter sig både af oplysninger, de har fundet på sociale medier, insiderviden (eventuelt fra tidligere angreb) og AI til at gøre svindelen mere troværdig. Se også afsnittet om phishing og angrebets faser.

Sådan beskytter du dig mod finansiel svindel:

- Styrk interne procedurer for kritiske processer (herunder betaling): robuste processer sikrer en balance mellem effektiv drift og risikoafgrænsning (ikke kun ved hackerangreb). Klare beløbsgrænser for hvilke beløb, der kræver ekstra godkendelser kombineret med klare processer for, hvordan betalingsanmodninger skal foregå (f.eks. ikke via en SMS fra "chefen") kan forebygge mange problemer.
- Lav et ekstra tjek, når samarbejdspartnere beder om ændring af konto nr. (ring evt. til firmaets hovednummer). Check ligeledes, når der er forskel mellem kontonummer på faktura og kontonumre i økonomisystemet.
- Brug teknologiske værktøjer: opsæt alarmer og overvågning, der kan identificere mistænkelig/unormal aktivitet på kritiske systemer og netværk.

Er din værdikæde en åben dør for hackere?

Cybertrusler stopper ikke ved din virksomheds dør. Faktisk er den til stede gennem hele din værdikæde – fra leverandører og samarbejdspartnere til kunder. Ét sårbart led i din værdikæde kan give hackere adgang til data eller systemer, som de kan bruge direkte eller sælge videre (se igen angrebets faser).

Har du for eksempel adgang til en af dine leverandørers systemer, kan adgangen fungere som en bro, hackerne kan udnytte til at trænge ind i dine systemer og data. Det betyder samtidig, at du også kan være bro til dine samarbejdspartnere, hvis du ikke har styr på din cybersikkerhed. Denne type trussel kan udfordre din virksomhed, og den værdikæde du er en del af. Derfor har alle et ansvar for at beskytte data, systemer og adgange, så de cyberkriminelle ikke møder åbne døre.

IT-sikkerhed – det har vores IT-leverandør da styr på?

Du er ikke den eneste, hvis du tænker, at IT-sikkerhed er noget din IT-leverandør har styr på. Og så har du og dine medarbejdere jo sikkerhedsforanstaltninger på jeres PC'er, og I opdaterer løbende jeres systemer. Den barske virkelighed er bare, at det ikke er nok. IT-sikkerhed handler ikke kun om teknologi – det handler i den grad også om menneskelig adfærd.

Forestil dig, at du køber en splinterny bil med alle de nyeste sikkerhedsfunktioner og -foranstaltninger. Det lyder trygt. Men hvad hjælper det, hvis føreren ikke kender trafikreglerne eller ikke ved, hvordan bilen skal betjenes? På samme måde er teknologi kun en del af løsningen, når det kommer til cybersikkerhed.

Fakta er, at 95 % af cyberangreb sker som følge af menneskelige fejl – altså som følge af medarbejdernes handlinger*.

Det betyder, at rigtigt mange cyberangreb kan undgås og effekten reduceres, hvis du uddanner medarbejderne i potentielle trusler og sikrer en god sikkerhedsadfærd.

*World Economic Forum: "The Global Risks Report 2022"

Sådan skaber du en stærk sikkerhedskultur

En stærk sikkerhedskultur starter altså med mennesker. Selv de mest avancerede sikkerhedssystemer er sårbare, hvis medarbejderne ikke er bevidste om truslerne og forstår, hvordan de skal agere i forhold til IT-sikkerhed.

Vil du skabe en stærk sikkerhedskultur, må cybersikkerhed blive en naturlig del af hverdagen, hvor alle tager ansvar. Vi har her samlet en række gode råd til, hvordan du sikrer, at cybersikkerhed bliver en integreret del af din virksomheds arbejdsrutiner – fra ledelsens prioriteringer til den enkelte medarbejders adfærd.

Start fra toppen

Ledelsen skal gå forrest og vise, at cybersikkerhed prioriteres højt. Når ledelsen engagerer sig og efterlever sikkerhedsprocedurerne, smitter det af på resten af organisationen.

Gør det konkret

Tal om cybersikkerhed på en måde, der er konkret og giver mening for medarbejderne. Del eksempler fra virkeligheden, der viser, hvordan trusler kan påvirke deres arbejde, og hvordan deres indsats gør en forskel.

Skab en god sikkerhedskultur

Cybersikkerhed er ikke noget, du lærer én gang for alle. Truslerne ændrer sig hele tiden. Gør det til en fast del af jeres dialog med medarbejderne og arranger løbende træning, hvor medarbejderne kan opdatere deres viden – for eksempel om phishing eller sikker password-praksis.

Fjern frygten for at fejle

Ingen skal føle sig bange for at indrømme fejl. Skab en kultur, hvor det er bedre at rapportere en fejl end at forsøge at skjule den. Hvis en medarbejder for eksempel er kommet til at klikke på et forkert link eller åbne en kompromitteret fil, skal man føle sig tryg ved straks at rapportere det.

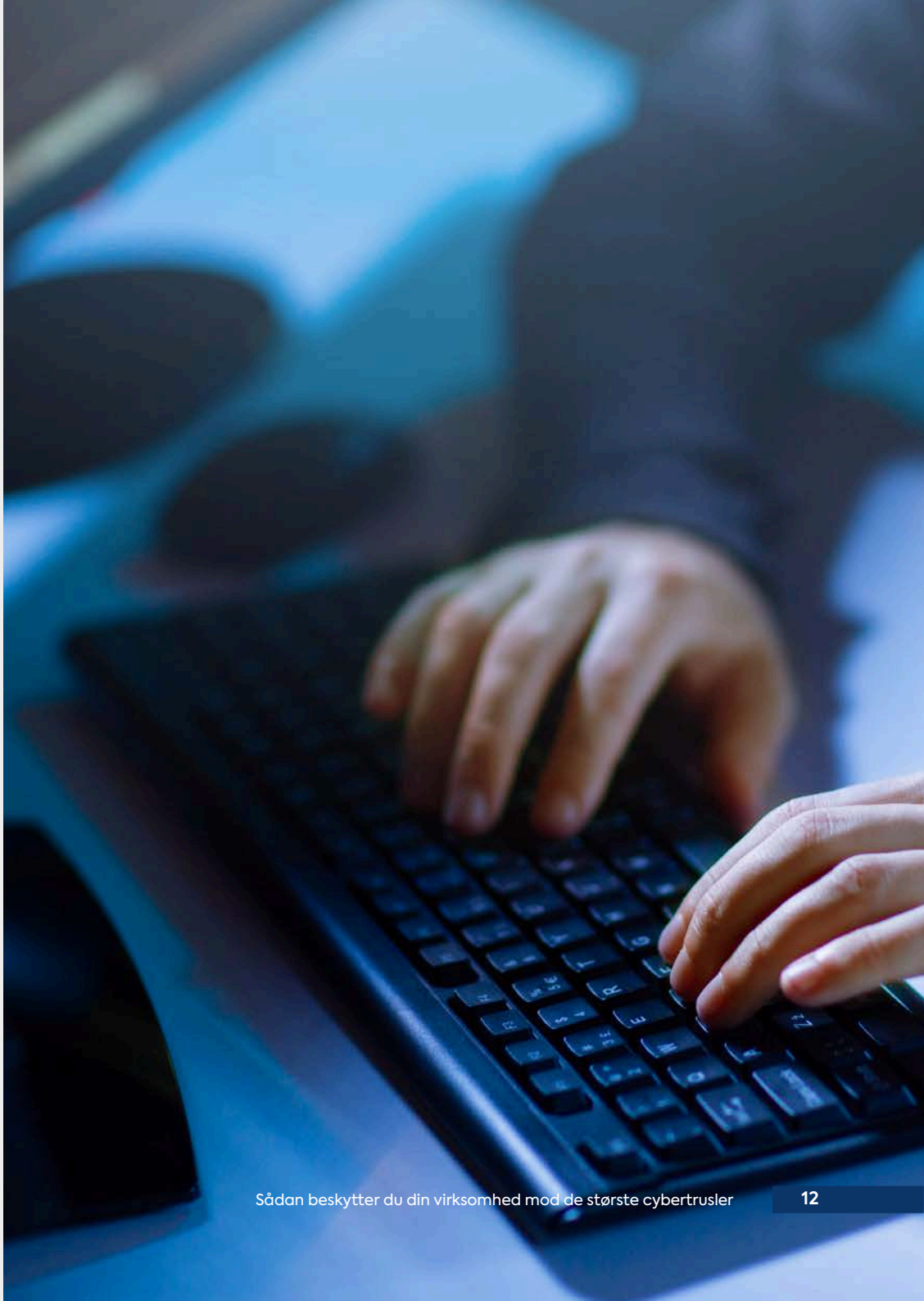
Brug din IT sikkerhedsekspert

Kend din egne begrænsninger og sikr dig adgang til kompetencer (internt eller eksternt), som kan være med både i det daglige arbejde med IT-sikkerhed og når angrebet kommer.

Adskillelse mellem private og virksomhedsrelaterede aktiviteter

God IT-sikkerhedsadfærd handler også om at sikre adskillelse mellem private og virksomhedsrelaterede aktiviteter. Hvis der er et overlap, er angrebsfladen langt større for de IT-kriminelle og muligheden for at opdage "unormal" adfærd langt vanskeligere.

Også medarbejdernes rettigheder er afgørende for, hvor let det er for de IT-kriminelle – hvis alle brugere har administrationsrettigheder, så åbner hele din digitale verden for de kriminelle, hvis du bliver angrebet.



Små men effektive tiltag

Ved at sætte cybersikkerhed på dagsordenen kan du styrke virksomhedens sikkerhed gennem en række små, men effektive tiltag. Hver enkelt handling bidrager til at øge beskyttelsen og reducere konsekvenserne af et angreb.

Sørg for at tale om IT-sikkerhed både internt og med dine IT-leverandører, så du får et klart overblik over dine sårbarheder og de kritiske data, du skal beskytte.

Der er en række tiltag, som du kan arbejde videre med som for eksempel: etablering og implementering af en IT-sikkerhedspolitik, træning af alle medarbejdere og måske en cybersikkerhedsforsikring. Tjek, at den dækker din forretnings behov og i hvilket omfang.

Det er forskelligt fra virksomhed til virksomhed, hvor man får mest effekt af de investerede kroner i IT-sikkerhed. Derfor handler det om at prioritere indsatserne rigtigt i forhold til jeres risiko.

Din køreplan til at komme i gang på en praktisk måde

IT-sikkerhed kan føles som en uoverskuelig opgave. Derfor kan det være en god ide at prioritere dine indsatser. Hellere starte småt og bygge videre derfra. Men hvor skal du begynde? Du får her en 7-trins køreplan, der kan hjælpe dig med at komme rigtigt i gang.

7-Trins køreplan

1. Oplæring
Træn dine medarbejdere i at genkende phishing-mails. Mange angreb starter med en falsk mail, der ser ægte ud. Giv konkrete eksempler og lær dem, hvad de skal kigge efter – fra mistænkelige links til mærkelige afsendere.

2. Praksis for password
Sørg for, at alle medarbejdere i virksomheden bruger stærke og unikke passwords. Det kan være en ide at bruge en password-manager. Dette skal suppleres med to-faktor-godkendelse.

3. Beskyt jeres computere
Anvend kun godkendte softwareprogrammer og sørg for, at jeres software altid er opdateret. Sikr dig, at medarbejderne ikke har administrator rettigheder og kan downloade alle typer af software.

4. Husk at arbejdstelefon og tablets også er en indgang
Arbejdstelefoner og tablets udgør også en risiko på samme måde som computere. Sørg for, at de er beskyttet med en adgangskode, og undgå at installere apps fra ukendte kilder.

5. Arbejd sikkert uden for virksomheden
Sørg for, at medarbejdere, der arbejder hjemmefra eller på farten, er trænede i at arbejde på sikre forbindelser.

6. Rapportér
Gør det let og tydeligt for medarbejdere, hvem de skal rapportere til, når de opdager mistænkelig aktivitet. Jo hurtigere I opdager en hændelse, desto lettere er det at afværge skaden.

7. Beredskabsplan
Udarbejd en klar plan for, hvad du og dine medarbejdere skal gøre, når I bliver ramt af et cyberangreb. Planen skal klart definere, hvem der gør hvad, og hvordan I begrænser skaderne.

Det er vigtigt løbende at teste planen af, så du ved, om den holder i praksis. Det er desuden vigtigt at identificere hvilket nødtelefonnummer, der skal stå på planen – angreb sker typisk udenfor almindelig arbejdstid – og i forbindelse med ferie/helligdage.

Planen skal findes på papir. I værste fald har I ikke adgang til jeres systemer under et angreb.

Få 1:1 sparring om cybersikkerhed

Cybersikkerhed behøver ikke at være en kamp, du står alene med. Med den rette vejledning og hjælp kan du effektivt styrke cybersikkerheden i din virksomhed og den værdikæde, du er en del af. Det arbejde hjælper vores erfarne forretningsudviklere dig gerne med – gratis og uvildigt.

Få for eksempel hjælp til:

- At identificere vigtige indsatsområder og lavthængende frugter, der kan styrke dit værn mod cyberangreb.
- Hvor du skal starte, og hvordan du kommer videre.
- Hvad NIS2 er, og hvem der er omfattet af lovgivningen.
- Hvad du kan gøre, hvis du er del af en værdikæde, og vil undgå at være det svageste led.

Læs mere om hvordan vi kan hjælpe her.

Skal vi tage en snak om cybersikkerhed?

Niklas Hall
Senior forretningsudvikler
M: 61 88 46 18
E: nhl@ehhs.dk

Cybersikkerhed handler ikke om at gøre alt selv – men om at finde de rette samarbejdspartnere og få hjælp fra dem, der ved, hvordan.

E-bogen er produceret af projektet 'Styrket Cybersikkerhed for SMV'er', der hjælper små og mellemstore virksomheder med at forbedre cybersikkerheden, både internt og i samarbejde med værdikædepartnere. Projektet drives af Erhvervshusene og er støtte af Industriens Fond.

Læs mere om Styrket Cybersikkerhed for SMV'er her.

Erhvervshusene

INDUSTRIENS FOND