MINDCORE

7 OVERSETE FJENDER

DE FLESTE VIRKSOMHEDER OVERSER
DISSE 7 CYBERSÅRBARHEDER

CYBERSIKKERHED HANDLER IKKE KUN OM DRAMATISKE ANGREB

"Danmark står overfor det mest alvorlige risiko- og trusselsbillede siden anden verdenskrig" – sådan indleder Styrelsen for Samfundssikkerhed sin trusselsvurdering for 2025. (Kilde)

Av min arm for en åbning. **Måske tænker du sådan her lige nu:**

"Vorherre bevares, endnu en omgang dommedagsretorik, der ikke rigtigt hjælper mig" – fordi du de sidste 5 år har fået tudet ørerne fulde om, at cyberangreb er det værste, der kan ske for din virksomhed.

Og ja, truslen er alvorlig. Men cybersikkerhed bliver forbundet med dramatiske hackerhistorier, awarenesstræning og millioninvesteringer – og ikke de små lavpraktiske tiltag, der gør en stor forskel.

Du kan sammenligne det med sikkerhed i dit hjem:

Forestil dig, at du investerer i en god og fornuftig løsning, så du og familien kan føle jer trygge – måske med smart lås, alarm og overvågning via en app. Du føler dig tryg, også når du ikke er hjemme.

Men... Det smarte system forslår som en skrædder i helvede, hvis junior glemmer at lukke køkkenvinduet, og du kører med hele familien på en 7-dages ferie hos svigerfamilien. Det er de små ting, der gør forskellen.

Også i din virksomhed. Det er summen af de små huller i sikkerheden, der bliver til risiko og sårbarhed overfor cyberangreb.

Og derfor har vi lavet en oversigt over typiske svagheder i sikkerheden, og hvordan du kommer i gang med at løse dem.

Jesper Petersen
Practice Lead for
Sikkerhed og Microsoft 365

1. sårbarhed: ringe brugerstyring

Det sker typisk, når aktive brugerkonti bliver glemt (f.eks. når Lennart får nyt job), ikke bliver gennemgået eller når to kollegaer laver Netflix-finten og deler login til en konto.

Hvad er konsekvensen?

Glemte konti er som en kattelem for cyberkriminelle, og de glemte konti fører ofte til databrud og bøder for non-compliance.

Og så har vi ikke engang talt om hvad, det koster at få sit navn på forsiden af Berlingske med teksten "databrud."

Kort sagt: det bliver dyrt, både for omdømmet og forretningen.

Sådan løser du det

Det er ikke så eksotisk, men den eneste vej er at auditere og disable ubrugte konti, sørge for stærk identifikation (multifaktorgodkendelse) og aldrig, aldrig lade kollegaer dele konti.

KOMMUNE SVINDLET FOR MERE END 1,3 MIO.

I december 2023 blev Guldborgsund Kommune svindlet for mere end 1,3 mio. kroner, da kriminelle hackere kompromitterede en medarbejders mailkonto. Herefter sendte de fakturaer til betaling hos kommunens økonomiafdeling, ved hjælp af denne mail-konto.

Tabet ved svindel kan ikke kun opgøres i kroner og ører

Én ting er de økonomiske konsekvenser ved digital svindel og cyberkriminalitet, en anden er sociale og psykologiske...

At blive offer for et cyberangreb kan gå ud over selvværdet, for ingen har lyst til at være “den der blev snydt.”

(Kilde: Styrelsen for Samfundssikkerhed, Cybertruslen mod Danmark 2025)

2. sårbarhed: tilfældig software

Du har sikkert hørt din kollega sige noget a la "jeg har lige hentet den her smarte Pomodoro-app."

Det virker uskyldigt, men når kollegaer installerer uautoriseret software eller bruger shadow IT (f.eks. Dropbox eller WeTransfer) åbner det en uovervåget dør for cyberangreb.

Hvad er konsekvensen?

Den smarte Pomodoro-app kan gemme på malware, eller blive udnyttet til ransomware.

Og du kan nok forestille dig, hvad det koster, når en butikskæde bliver ramt, kortbetaling går ned, og omsætningen står stille i over 24 timer.

Hvad kan du gøre?

Her skal du være skrap og konsekvent:

Lad kun autoriserede personer installere software og lav evt. en liste over godkendt software. Og så handler det om at genbesøge og lave intern audit – igen og igen.

HOSPITAL PÅVIRKET AF RANSOMWARE-ANGREB

I 2024 blev det danske hostingselskab, IT-hotellet, udsat for et ransomware-angreb, der krypterede IT-hotellets systemer og data – og dermed blev gjort utilgængelige.

Her blev bl.a. Odense Universitets-hospital påvirket, da de mistede adgangen til et centralt overvågningssystem, som de bl.a. anvendte til at justere varmen på hospitalet.

Det skal siges, at hændelsen ikke havde konsekvenser for patienter på hospitalet, men hændelsen understreger de alvorlige konsekvenser, et ransomware-angreb kan have.

(Kilde: Styrelsen for Samfundssikkerhed, Cybertruslen mod Danmark 2025)

3. sårbarhed: styring af tilladelser

Det her er en klassiker rundt omkring i de danske virksomheder:

Hanne skifter afdeling fra HR til Marketing, og i en travl hverdag glemmer man at opdatere hendes adgangsrettigheder. **Det betyder**, at hun stadig har fuld adgang til mapper med fortrolige data, såsom lønoplysninger.

Hvad er konsekvensen?

Det er nemt at miste overblikket, og du ved reelt set ikke, hvor mange skjulte brugere, der gemmer sig. Derudover har brugere adgang til data og systemer, de ikke burde, og det øger risikoen for databrud.

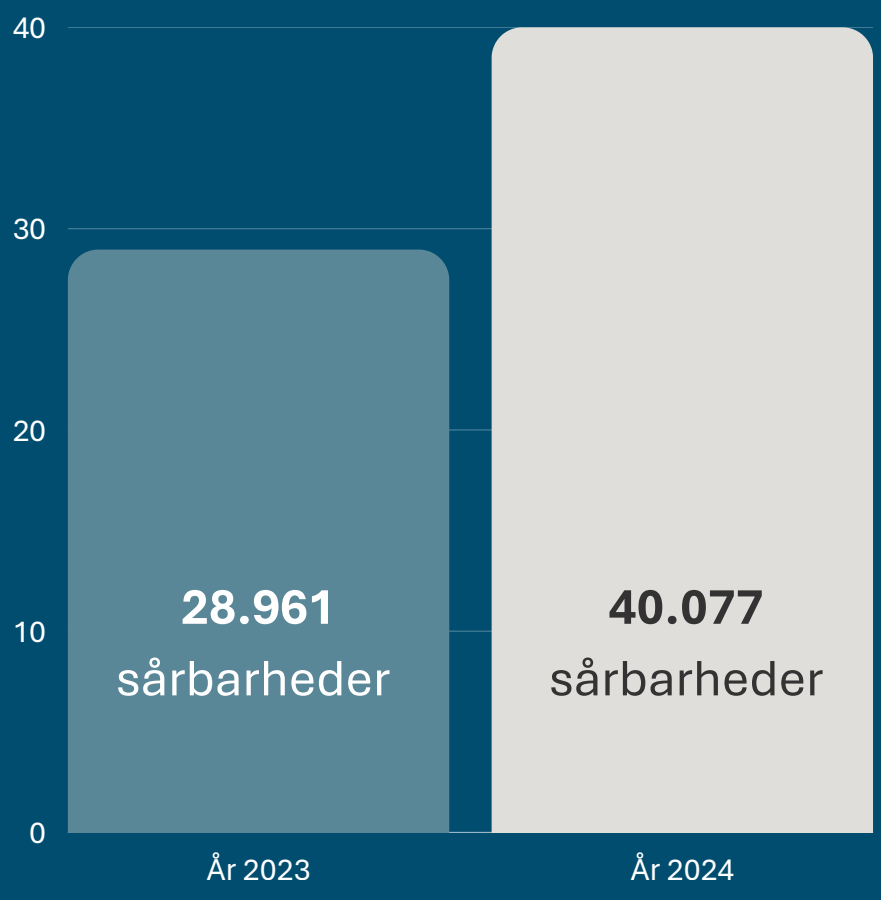
Hvad kan du gøre?

Brug rollebaserede adgange i stedet for de individuelle adgange, der er knyttet op på en enkelt person.

På den måde giver du medarbejdere adgang ud fra deres funktion (f.eks. HR, IT eller Marketing) i stedet for personen. Sørg også for at lave løbende gennemgang af alle rettigheder hos rollerne, så Hanne fra HR ikke hænger i systemet flere år efter, hun har forladt afdelingen.

HØJESTE ANTAL SÅRBARHEDER – NOGENSINDE

Udnyttelse af sårbarheder er en udbredt angrebsteknik, hvor cyberkriminelle udnytter en eller flere tekniske fejl i software eller hardware. Den amerikanske nonprofitorganisation MITRE vedligeholder en offentligt tilgængelig database over sårbarheder (CVE'er), og opdateres i takt med, at nye sårbarheder opdages. I 2024 blev 40.077 sårbarheder tilføjet til databasen – det højeste nogensinde. Til sammenligning var antallet i 2023 i alt 28.961. **Det svarer til en stigning på ca. 38 pct.**



(Kilde: Styrelsen for Samfundssikkerhed, Cybertruslen mod Danmark 2025)

4. sårbarhed: intet overblik over enheder

Prøv at gå en runde på kontoret og se, hvad der gemmer sig i skufferne og jalousiskabene.
I mange virksomheder vil du finde gamle laptops og anden hardware, der er strandet efter Lennart, Hanne og Gitte, har fået nyt.

Hvad er konsekvensen?

Tænder du f.eks. Hannes gamle PC, der ikke er sikkerhedsopdateret i flere år, gør du det nemt for *bad actors* at få adgang f.eks. via jeres netværk. Gammelt hardware kan altså være en åben dør for cyberkriminelle, og hvis døren først er opdaget, kan det gå meget hurtigt.

Hvad kan du gøre?

Med moderne håndtering af jeres enheder – f.eks. Microsoft Intune – har du altid styr på, om en enhed er compliant, overholder jeres sikkerhedstjek, og om den må få adgang til virksomhedens netværk og data.

Det vil sige, at kun enheder, der er compliant, får adgang.

350.000 KUNDER RAMT AF SUPPLY CHAIN-ANGREB

I 2023 blev ip-telefoni-udbyderen, 3CX, ramt af et supply chain-angreb, hvor nordkoreanske cyberkriminelle havde kompromitteret en leverandør til 3CX og fået adgang til 3CX's netværk. De udnyttede adgangen til at indarbejde en bagdør i en kommende opdatering til deres ip-telefoni software. Og på den måde fik hackerne potentielt adgang til kundernes enheder, da 3CX udrullede opdateringen af softwaren. På daværende tidspunkt var mere end 350.000 organisationer, heriblandt danske organisationer, kunder hos 3CX.

Ifølge Gartner vil 60% af supply chain-orgisationer bruge cyber-sikkerhedsrisici som et afgørende kriterium, når de vurderer samarbejder, og transaktioner med tredjepartsleverandører.

(Kilde: Gartner 2025)

5. sårbarhed: leverandører

Angrebsteknikken kaldes supply chain-angreb, hvor cyberkriminelle typisk først rammer leverandøren, og herefter udnytter tillid og adgang mellem kunde og leverandør.

Det betyder, at når I bruger forskellige leverandører til alt fra cloudsystemer til CRM-systemer, kan cyberkriminelle få adgang til visse data, f.eks. personale-, bank- eller kundeoplysninger.

Hvad er konsekvensen?
Det kan ramme jer, hvis leverandører ikke har fuldstændig kontrol over deres sikkerhed. Har de ikke styr på compliance og egne processer, risikerer virksomheden et datalæk - med jeres data. Her taler vi altså GDPR- og NIS2-bøder og risiko for møgsager i pressen.

Hvad kan du gøre?

I skal forholde jer kritisk til (nye) leverandører:

✓ Lav grundig screening af leverandører
✓ Hav klare databehandleraftaler
✓ Få risikovurdering på plads

PRISEN FOR ET DATABRUD

30,2 mio.

Ifølge IBM var den globale omkostning ved et databrud i 2024 $4,4 mio. dollars, svarende til 30,2 mio. danske kroner.

279 dage

Når stjålne eller kompromitterede data var gemt på tværs af flere miljøer (fx både i skyen og lokalt), tog det 279 dage at opdage og få stoppet bruddet i 2025.

Kun 49% investerer i sikkerhed efter et databrud

I 2025 så vi et markant fald i, hvor mange organisationer der vil skrue op for sikkerheden efter et databrud. I 2024 sagde 63%, at de planlagde at investere mere i sikkerhed efter et brud. I 2025 er tallet faldet til 49%.

Og selv blandt dem, der faktisk vil investere, er det under halvdelen, der forventer at sætte ind med AI-baserede løsninger. Det kan fx være:

- værktøjer til at opdage og stoppe trusler hurtigere (threat detection & response)
- planlægning og øvelser for, hvad man gør, når et angreb rammer (incident response/IR)
- bedre beskyttelse af data (data security/data protection)

(Kilde: IBM, Cost of a Data Breach Report 2025)

6. sårbarhed: sårbar deployed code

De fleste du kender har nok klikket “udsæt opdatering til senere”, fordi de lige skulle skrive en vigtig mail eller scrolle færdigt.

Og så er der dem, der flittigt opdaterer, fordi de ved, hvor vigtige opdateringer er for sikkerheden. Men hvad hvis opdateringen har **ondsindet kode** med sig? Dét er sårbar *deployed code*, og det kan have store konsekvenser...

Hvad er konsekvensen?

Et eksempel er SolarWinds, der blev angrebet i 2020, hvor cyberkriminelle inficerede en opdatering af programmet Orion, der blev skubbet ud til Solarwinds' kunder. På den måde fik de mulighed for at få adgang til virksomhedernes IT systemer.

Sådan et angreb er i sig selv skadeligt for virksomheden og kunderne, men en anden ting er tilliden:
Hvis kunderne mister tilliden til sikkerhedsopdateringer, har vi et stort problem.

Hvad kan du gøre?

Grundighed, grundighed, grundighed. Du bør teste alle opdateringer, du sender ud, så du ved, hvad der sker hos brugerne – også opdateringer fra dine leverandører.

Men endnu vigtigere:
Det er ikke sikkert, at I kan fange et angreb som SolarWinds, før det er for sent.

Derfor er det vigtigt at have et solidt sikkerhedsberedskab.

FRA LAV TIL MIDDEL TRUSSEL

Sikkerhed er ikke for sjov. Truslen fra destruktive cyberangreb mod Danmark blev i juni 2024 hævet fra lav til middel.

Det betyder, at Styrelsen for Samfundssikkerhed (SAMSIK) vurderer, at det er sandsynligt, at **statslige russiske hackere** udfører cyberspionage mod dansk kritisk infrastruktur. Formålet er bl.a., at forberede sig på at kunne udføre destruktive cyberangreb i fremtiden. Derudover vurderer SAMSIK, at **truslen mod danske virksomheder og myndigheder er høj**. Sådan vurderer SAMSIK trusselsniveauet:

Ingen	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
Lav	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet. høj
Middel	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
Høj	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
Meget høj	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, eller en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

(Kilde: Styrelsen for Samfundssikkerhed, Trusselsvurdering: Cybertruslen mod Danmark 2025)

7. sårbarhed: dependencies

Når du skal udvikle noget, tager du ofte pakker eller biblioteker (altså dependencies) ind, så du slipper for at opfinde alt fra bunden.
F.eks. en pakke, der laver præcise udregninger, eller én, der optimerer en hjemmeside til både mobil og desktop.
Smart, men... Hvad hvis en pakke er inficeret med ondsindet kode?

Hvad er konsekvensen?

Et konkret eksempel er pakken ngx bootstrap, hvor man har opdaget en funktion, der fisker passwords ud af ens program og sender videre til dem, der introducerede det.
Puha. En sikkerhedsrisiko fra helvede

Hvad kan du gøre?

Kort sagt handler det om at minimere risici, overvåge og kontrollere.

Her er nogle idéer:

• Brug en dependency-scanner/SCA-værktøj, der scanner dine dependencies (pakker) og giver besked, når der opdages en sårbarhed.

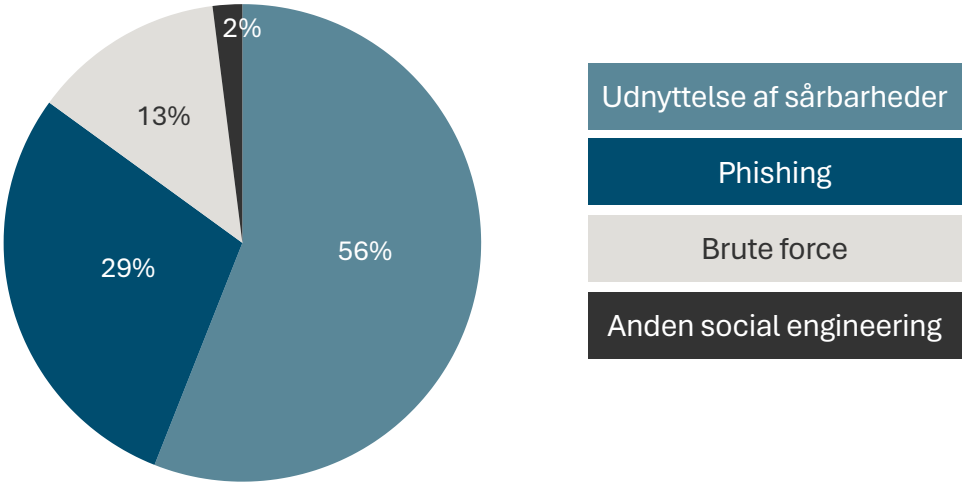
• Hold dependencies opdaterede med automatisering, der opdaterer pakker uden konflikter.

• Lav grundig screening af pakker: er de aktive? Er der kendte sårbarheder? Kommer der ofte sårbarheder?

HVORDAN ANGRIBER DE CYBERKRIMINELLE?

Ligesom teknologi udvikler sig hurtigere, end vi kan følge med, finder *bad actors* hele tiden på **nye måder at lave cyberangreb**.

Men de bruger ofte samme indledende øvelser til, at åbne bagdøren til organisationer og her er de fire mest udbredte ifølge Styrelsen for Samfundssikkerhed:



Diagrammet viser andelen af FE's registrede cyberangreb fordelt på angrebsteknikker. Grafikken er udarbejdet med afsæt i data fra FE's situationscenter fra de seneste to år. Bemærk, at fordelingen i grafikken af tekniske årsager kan afvige fra det reelle aktivitetsbillede.
(Kilde: Cybertruslen mod Danmark 2025, Styrelsen for Samfundssikkerhed)

DE MEST UDBREDTE ANGREBSFORMER

Udnyttelse af sårbarheder:

Når en angriber udnytter en kendt (eller ukendt) fejl i software/hardware til at få adgang, køre kode eller stjæle data.

Phishing:

Når nogen franarrer dig information ved at få dig til at klikke på noget i en sms eller en mail – eller ved et deepfake opkald på telefonen.

Brute force-angreb:

Når en angriber prøver ekstremt mange kodeord/kombinationer (ofte automatisk) indtil noget virker. F.eks. bombarderer angriberen en server med tusindvis af passwordforsøg i timen, indtil en svag adgangskode rammes (fx “Sommer2024!”).

Anden social engineering:

Her udnytter angriberen psykologi for at få adgang eller information ved manipulation, pres, udnyttelse af tillid og rutiner.

F.eks. hvis en person ringer til receptionen og siger: “Jeg er fra IT, vi har en akut fejl, kan du lige give mig navnet på jeres IT-ansvarlige og hans direkte nummer?”

Klip til næste opkald: “Hej, det er IT. Jeg skal lige have en engangskode for at fikse din konto.”

HVIS DU KUN TAGER ÉN TING MED, SÅ LAD DET VÆRE DET HER

Cybersikkerhed handler ikke kun om store dramatiske angreb. Det handler også om de små huller i sikkerheden.

Og her er det ikke kun de store millioninvesteringer i sikkerhedsløsninger, der beskytter jer.

En sidste ting...

Hvis du en dag får den mindste uro i maven over sikkerhed og risiko i din virksomhed, får du lige mine oplysninger.

Mine sikkerhedskolleger er dygtige, og giver gerne ekstra øjne på jeres sikkerheds set – uden at binde dig til en stor løsning.

Tusind tak for din tid.

Hilsen Jesper Petersen
Practice Lead for Sikkerhed og Microsoft 365

Email: jp@mindcore.dk
www.mindcore.dk