Mads Møller Pedersen
CEO

Kim Bonde
CTO & Security Officer

Cybertruslen:

Vær et skridt foran de IT-kriminelle!

Cybertruslen mod Danmark er meget høj

"I CFCS kan vi se, at danske netværk kontinuerligt bliver scannet for sårbarheder, hvor hackerne kan komme ind. Det betyder kort sagt, at alle danske virksomheder er udsatte. Og det er snarere et spørgsmål om hvornår end om hvorvidt, man bliver ramt."

- Thomas Flarup, tidl. chef for Center for Cybersikkerhed

Ulven kommer?

Hver eneste danske virksomhed ramt af 2521 cyberangreb om ugen

Antallet af afpresningsangreb i Norden er stigende: 24 procent af angrebene er rettet mod danske mål

Ny rapport: Ofre for digital afpresning er steget med 77 %

Kraftigere cyber-angreb rammer danske virksomheder

Cybertruslen mod Danmark er alvorlig og ændrer sig hurtigt

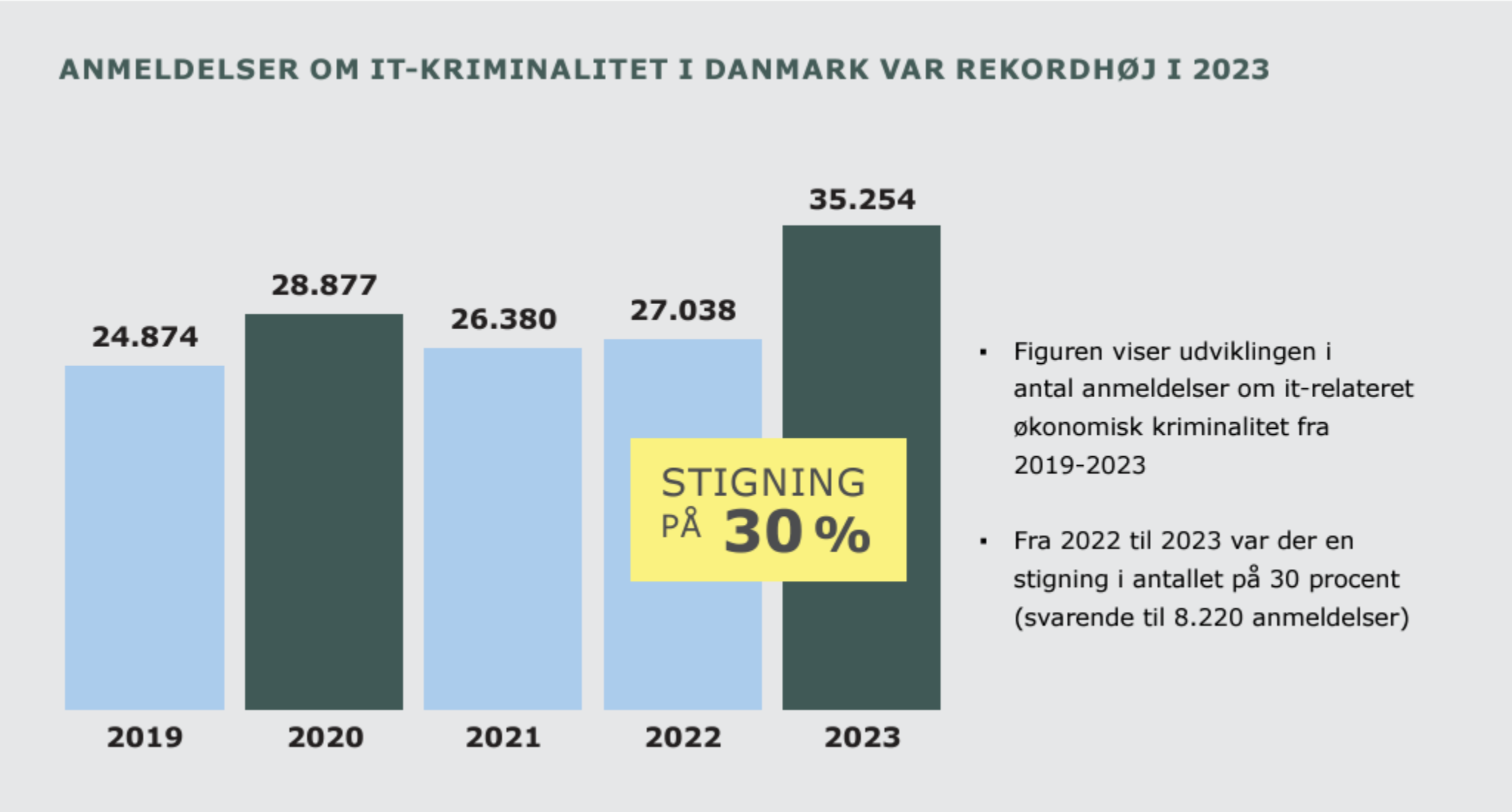
Cyberkriminalitet rammer alle virksomheder

Hackerangreb vælter ind over danske virksomheder

Det koster en million at blive ramt af hackerangreb

Virksomhedens største udgift er det driftstab, der kan være i forbindelse med et angreb.

Men det er desværre rigtig nok

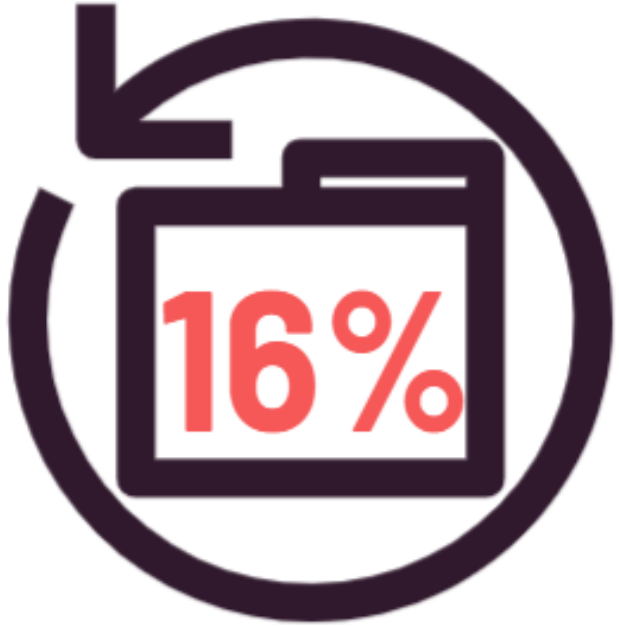


Statistikken taler for sig selv

- 96% udsat for phising-angreb
- 75% udsat for ransomware-angreb
- 50% af ransomware-angreb lykkes
- 40% kan ikke genskabe alle data
- 25% er allerede ramt uden at vide det

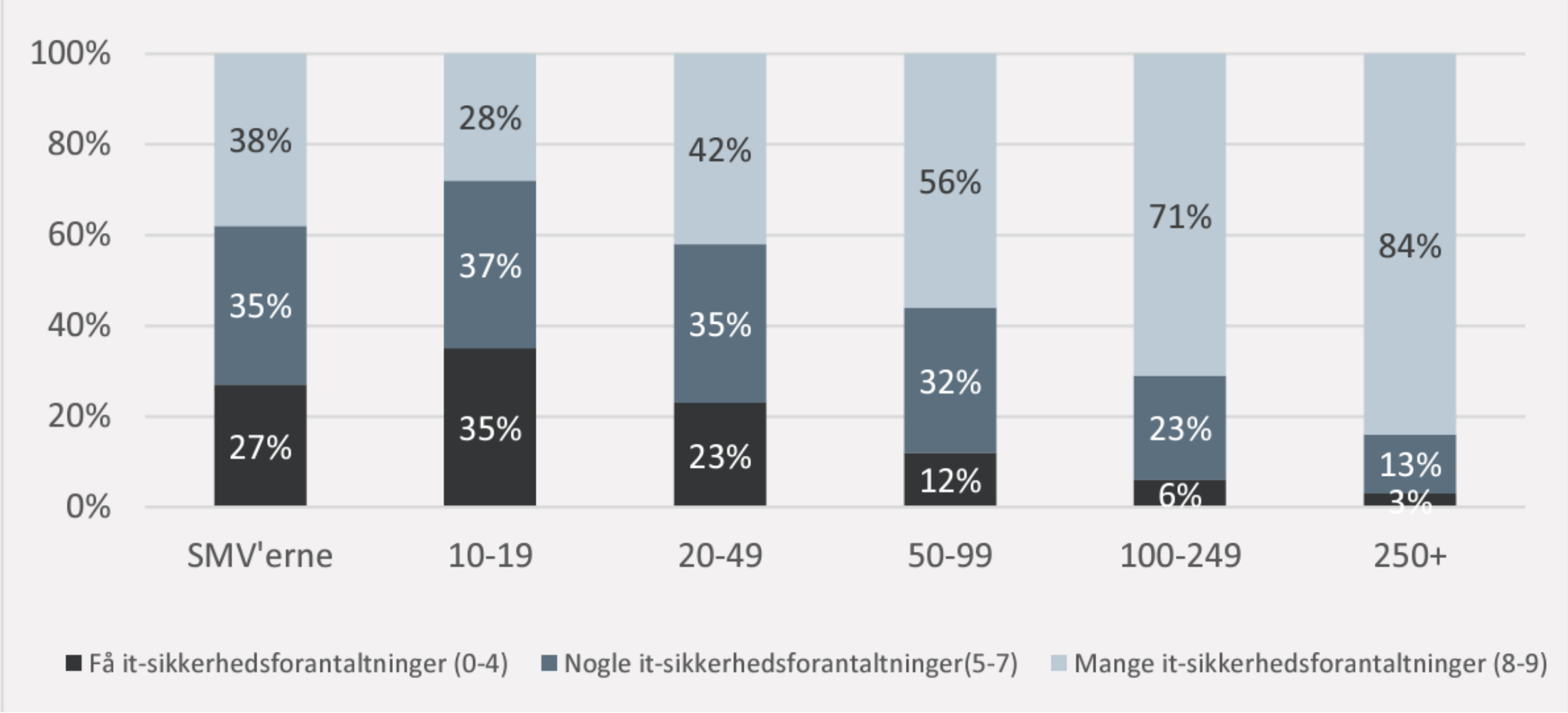
SMV'er halter bagud på IT-sikkerhed

Har et utilstrækkeligt digitalt sikkerhedsniveau

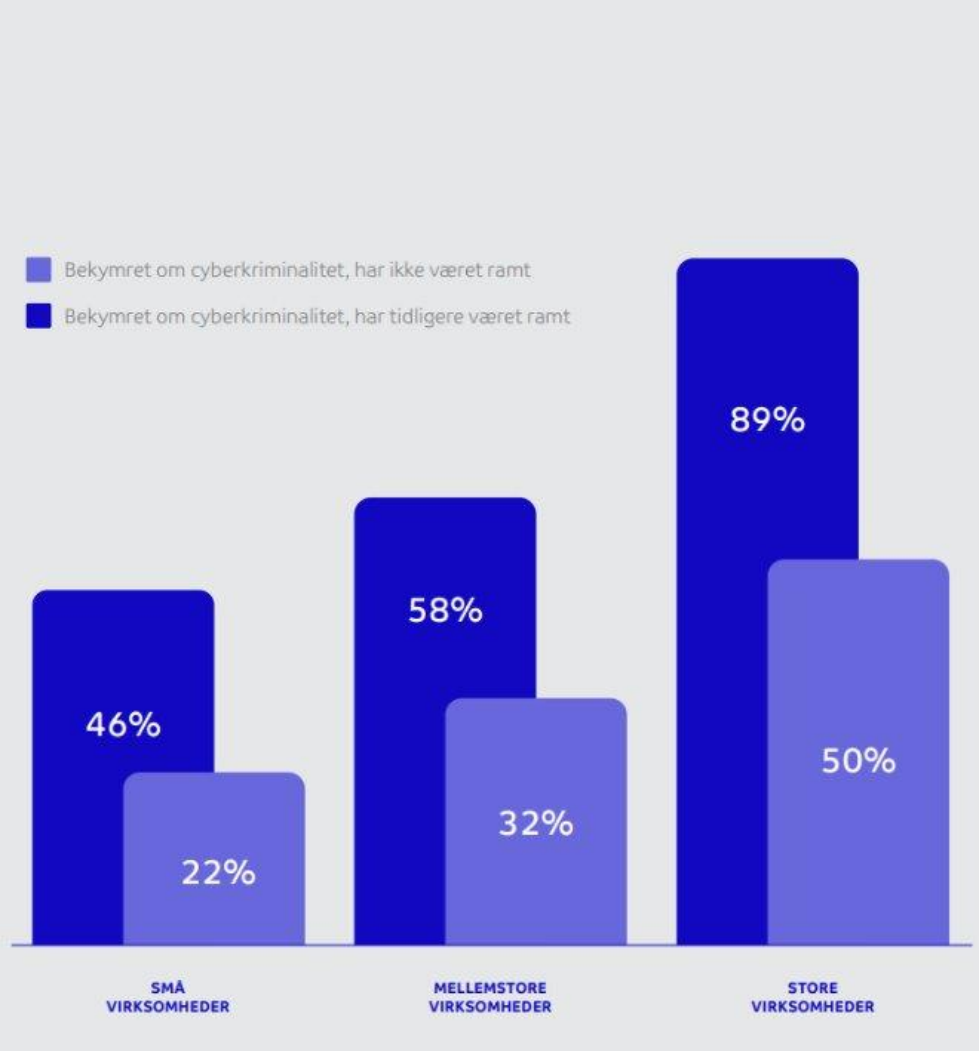


Har ikke basale sikkerhedsforanstaltninger

Manglende sikkerhedsløsninger i SMV'er



Cyberangreb rammer kun naboen!



Hvor mange af jer har været ramt?

Har I implementeret sikkerhedstiltag?

Er det noget, I taler om?

Ikke kun trusselsbilledet

Men også:

- Regulatoriske krav
- Branchekrav
- Lovgivning
- Krav fra kunder, leverandører, samarbejdspartnere
- Geopolitiske tilstande
- Økonomiske forhold
- NIS2

NIS2-direktivet rammer også jer!

Nye krav til organisationernes cyber- og informationssikkerhed, samt krav om tilsyn og rapportering

- Risikoanalyser og sikkerhedspolitik for informationssystemer
- Hændelseshåndtering og rapportering
- Krisehåndtering
- Værdikædesikkerhed for leverandører (bl.a. datalagring, processs- og sikkerhedsservices)
- Kryptering
- Politikker og procedure for vurdering af effektiviteten af sikkerhedstiltag
- Sikkerhed og regler for adgangskontrol

Ledelsen har ansvaret og kan sanktioneres direkte!

NIS2–direktivet

Formål med NIS2:
Sikre infrastruktur og samfundskritiske tjenester mod cybertrusler via et højt, ensartet niveau af cyber- og informationssikkerhed på tværs af EU.

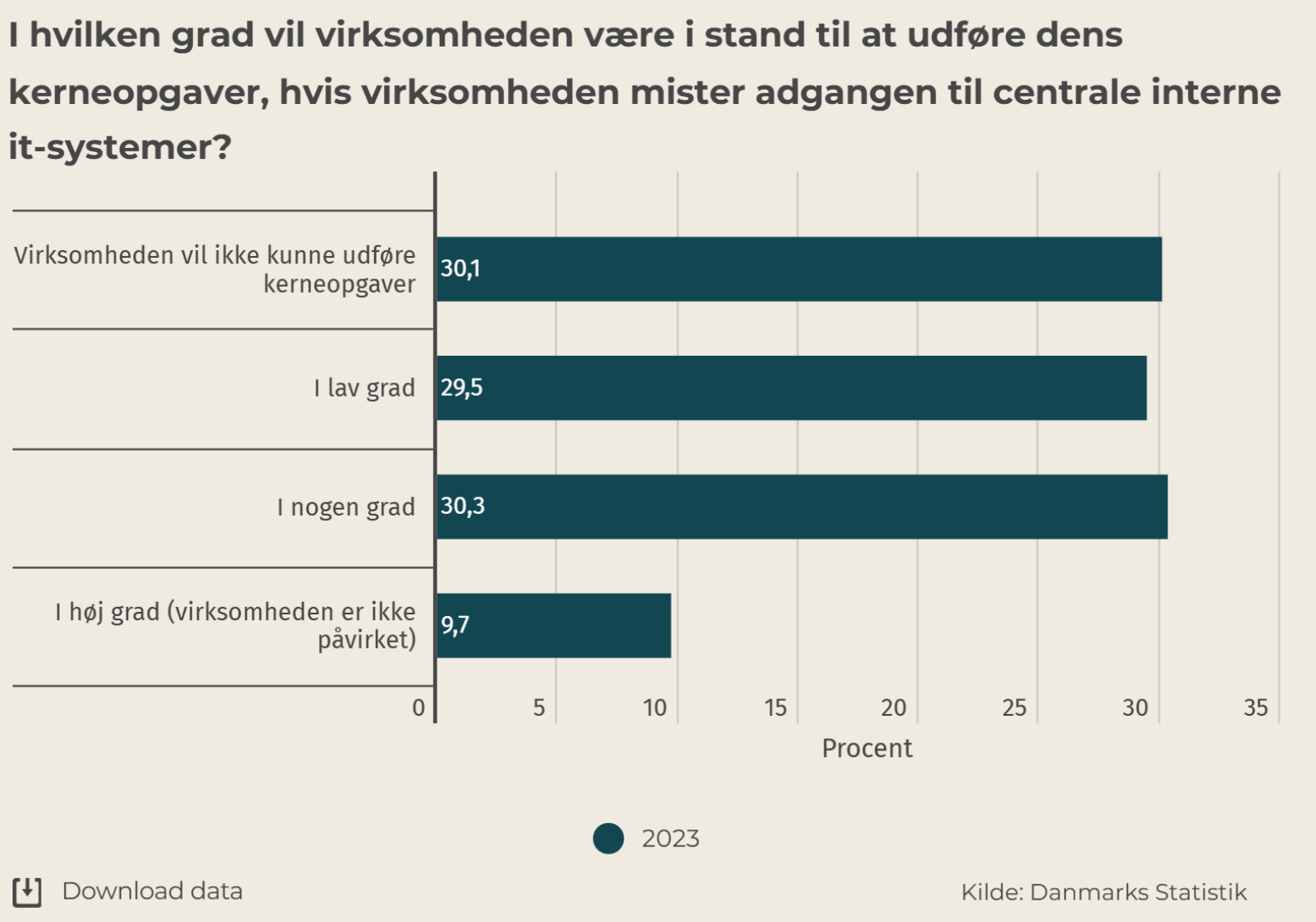
NIS2 omfatter:
Organisationer i sektorer, der håndterer samfundskritisk infrastruktur; energi, transport, sundhed, drikkevand, spildevand, affaldshåndtering og offentlig administration.

DERMED UDSIGT TIL STØRRE IT-SIKKERHEDSKRAV HOS MANGE DANSKE VIRKSOMHEDER

NIS2-bøder

”Er virksomheder ikke klar med deres sikkerhedsforanstaltninger i god tid, kan det få økonomiske konsekvenser i form af bøder på op 75 mio. kr. eller 2 pct. af virksomhedens omsætning. Bøden bliver det højeste af de to beløb”.

6 ud af 10 virksomheder bliver lammet



Konsekvenser af hackerangreb

- Mistet adgang til virksomhedens ordrebog og kundedatabase
- Ufrivillig deling af personfølsomme data
- Driftstab
- Tab af forretningskritiske dokumenter
- Risiko for afpresning
- Mistet tillid

"Jeg interesserer mig jo bare for chili"

Ud over tabt indtjening og en masse arbejdstimer har hackerangrebet også mindet ham om, hvor vigtigt "det der med sikkerhed" er.

For i hans lille virksomhed med seks til syv ansatte er der hverken en it- eller juraafdeling, og webshoppen er en ydelse, han køber hos en udbyder.

"Betal fem millioner dollars"

Stor bilforhandler oplevede hackerangreb: - Alt var sort og nogle maskiner også smadret

I marts 2023 oplevede Ole Hansen noget, som han ikke ønsker for sin værste konkurrent.

»Man går jo i chok. Jeg tror, det føles lidt på samme måde, som hvis nogen har sneget sig ind ad bagdøren i dit hus og stjålet dine ting. Man føler sig dybt uretfærdigt behandlet og først og fremmest magtesløs – for vi kunne jo intet gøre i begyndelsen. Alt i dag er bundet op på it, når systemerne svigter, har man pludselig ingenting. Kundeoplysninger, mails, arbejdskort, fakturaer ... Det hele var væk«, siger han.

Facebook konto blev hacket

Inden for første time efter firma FB konto blev hacket

- Password nulstillet og MFA slået til
- Køb af reklamer på kreditkort

FB kontaktet og konto låst

Fuld kontrol over konto efter 2 dage

Råd: MFA alle steder, privat og professionelt
Overvej hvor betalingsoplysninger gemmes

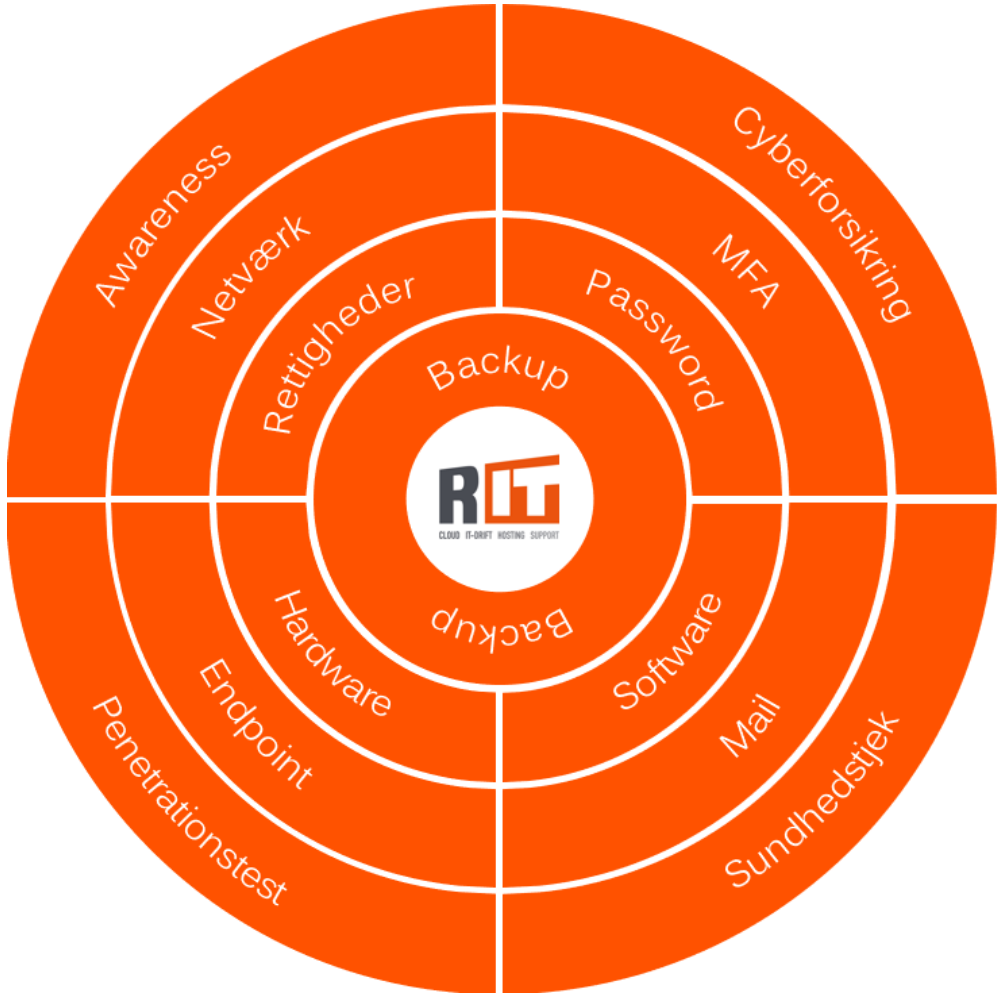
Hvor skal man sætte ind?

- 2-faktorsikkerhed (MFA)
- Endpoint Management (Monitorering og updates)
- Next-generation antivirus (EPDR)
- 24/7 sikkerhedsovervågning (SOC)

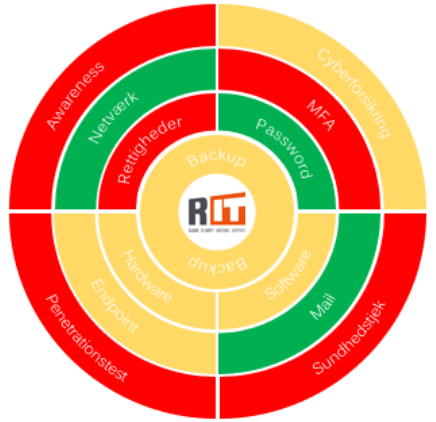
Hvor skal man sætte ind?

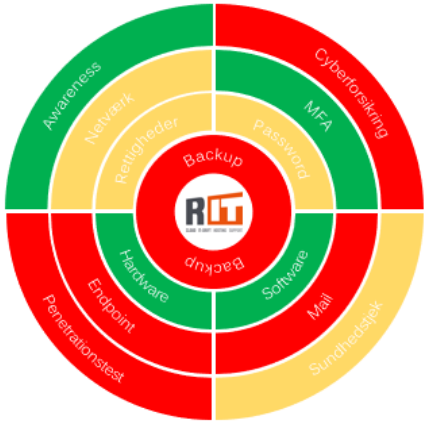
- Next-generation firewall (UTM)
- Segmentering og rettigheder
- Kryptering af mails, forbindelser og filer
- Sikkerhedsanalyse min. 1 gang årligt
- IT-sikkerhedspolitik og beredskabsplan

Hvor skal man sætte ind?



Eksempler:





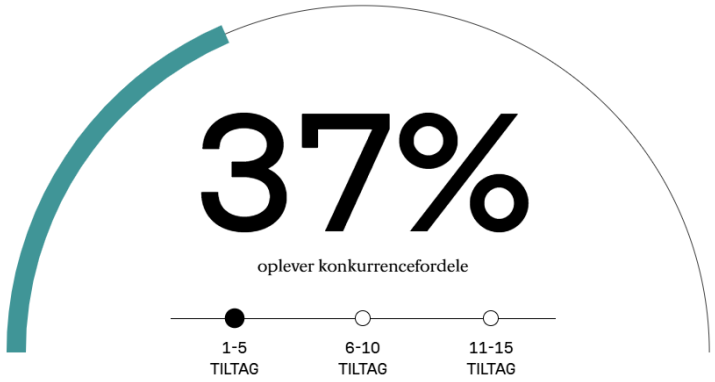
Oplevede fordele

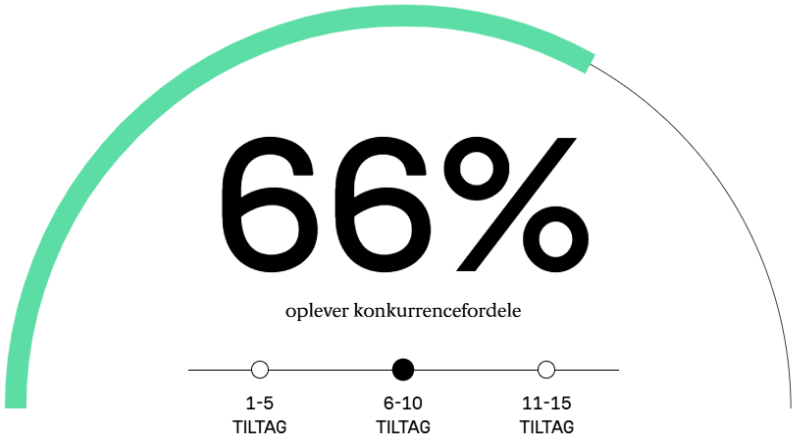
- Imødekomme kunde-, leverandør- og markedskrav
- Øget tillid fra kunder, samarbejdspartnere, ledelse
- Tiltrække nye kunder og medarbejdere
- Øget salg

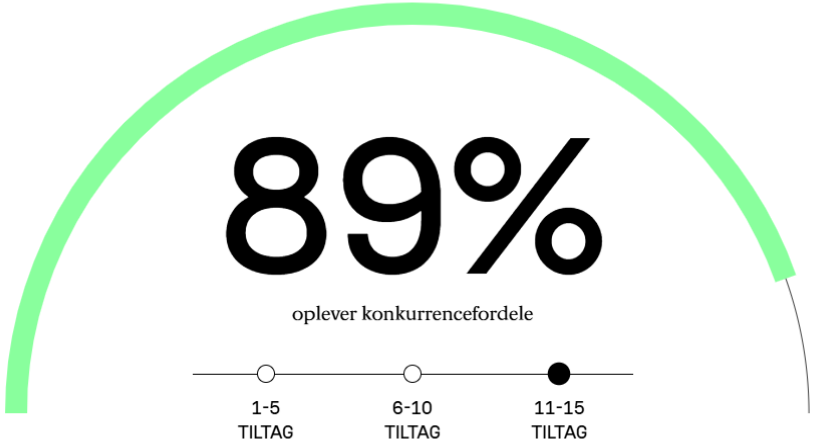
Oplevede fordele

- Effektivitet og nytænkning
- Implementering af ny teknologi
- Nye markedsmuligheder
- Bedre bundlinje

Udgift eller konkurrencefordel?







IT-sikkerhed er en strategisk beslutning og er forankret hos ledelsen!

9 råd
til at undgå cybersvindel

Bør jeg modtage denne?
Svar ikke på mails, sms eller opkald, når afsender og indhold virker mistænkeligt.

Tjek altid linket før du klikker
Hold musen hen over mistænkelige links og tjek URL'ens oprigtighed.

Afgiv aldrig fortrolige oplysninger
Afgiv aldrig adgangskoder, kreditkort- og personnummer via mail, telefon eller sms.

Du skal aldrig ændre oplysninger
Accepter aldrig anmodninger om at ændre person- eller kontooplysninger.

Lyder det for godt til at være sandt?
Vær altid skeptisk overfor tilbud, gaver og andre gratis belønninger.

Tjek afsenders mailadresse
Falske mailadresser ligner officielle. Blot et enkelt bogstav kan være forkert.

Tænk over aktualiteten
Svindelmails og opkald er hyppige ved juletid. Men også når I fx søger medarbejdere.

Installer aldrig programmer
Lad dig aldrig presse til at downloade programmer, selvom det lyder troværdigt.

Informer IT og advar kolleger
Informer altid jeres IT-ansvarlige og kolleger ved enhver mistanke.

Find flere gode tips & tricks
rlt.dk/nyheder

CLOUD IT-DRIFT HOSTING SUPPORT

Rådgivning i dag og telefonisk på mandag kl. 9-15 på: 20 89 24 63

RIT SECURITY

Mads Møller Pedersen
CEO
Mail: mmp@rit.dk
Tlf.: 40 88 22 30

Kim Bonde
CTO & Security Officer
Mail: kb@rit.dk
Tlf.: 20 89 24 63