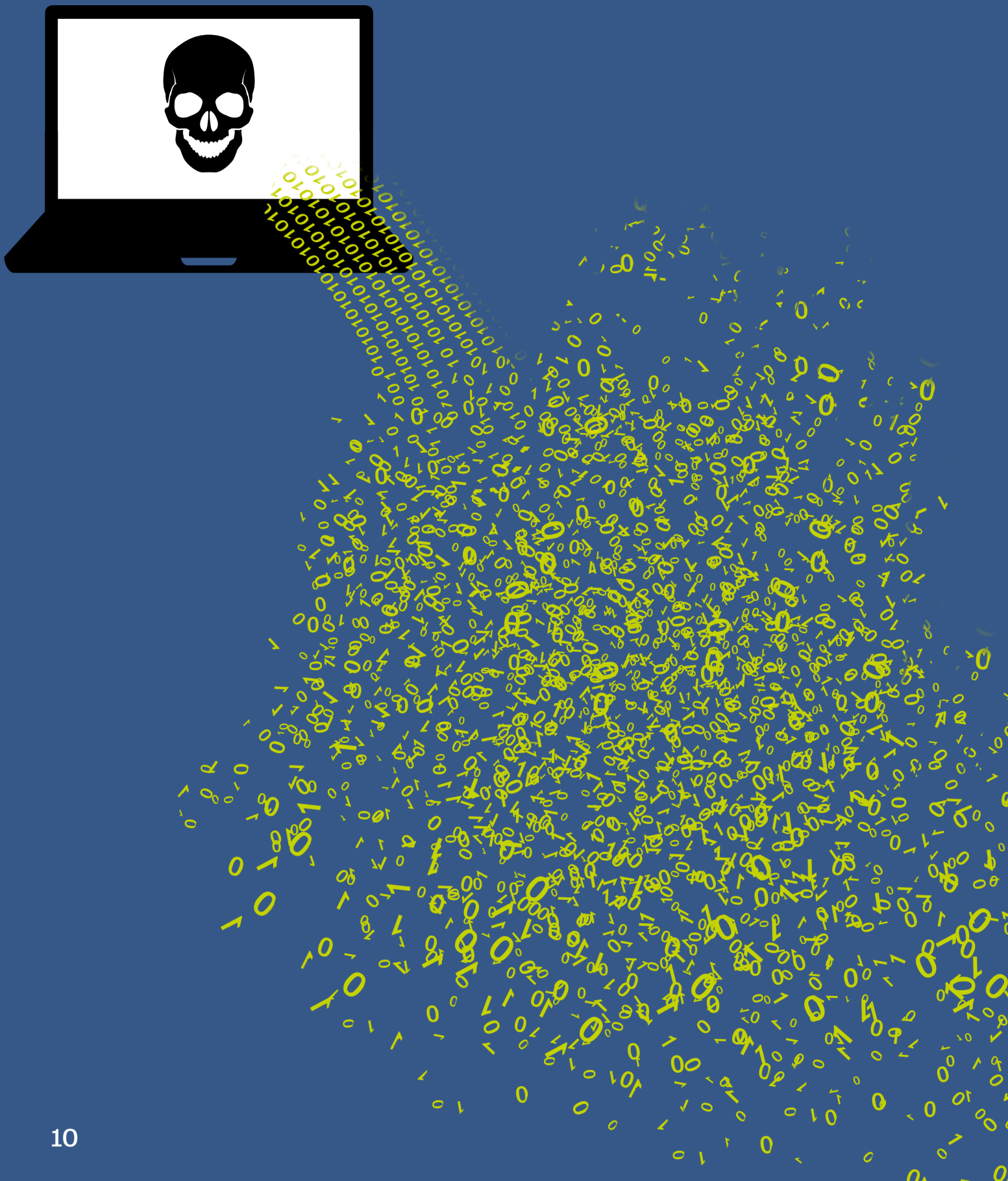
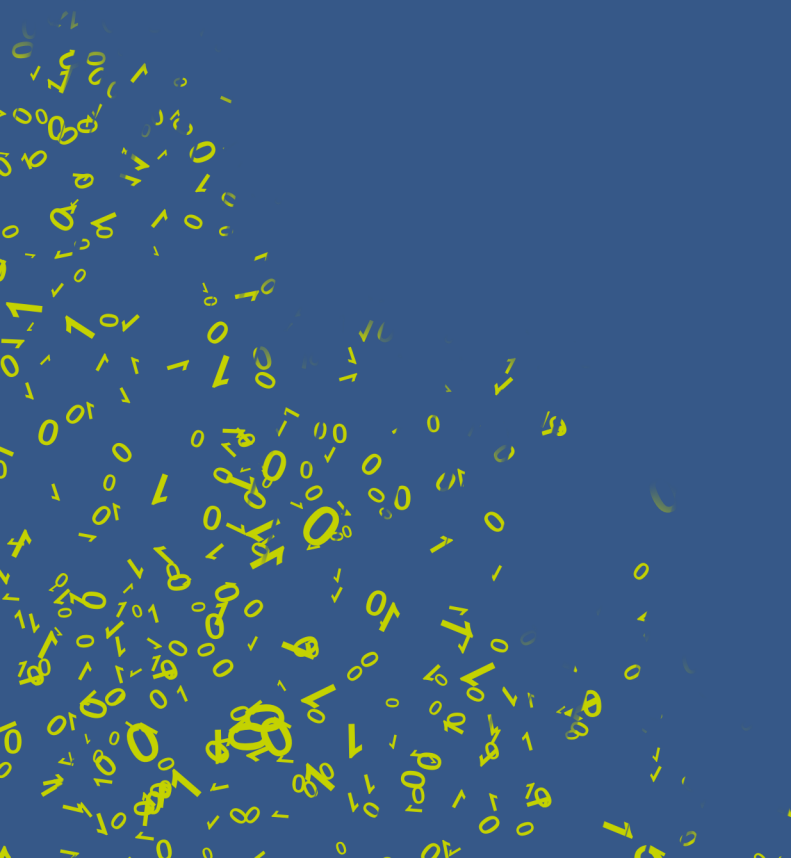
It-kriminalitet

Tekst: **MICHAEL DEGN**



Små virksomheder har store huller i it-sikkerheden

De mindste danske virksomheder har de største huller i it-sikkerheden, viser nye undersøgelser. Det er et problem, fordi hackere typisk skyder med spredehagl og rammer både store og små.



Hackeren sidder i mørklagte lokaler, begravet over tastaturet, mens han udpeger sit næste offer i cyberspace og går målrettet til værks. Noget tyder på, at det er det billede, som toner frem på nethinden hos lederne i små- og mellemstore virksomheder, når de hører ordene "hacker" eller "it-kriminelle".

– En udbredt forståelse blandt virksomhederne er, at de it-kriminelle går målrettet efter "noget, der er værd at stjæle", lyder det i en ny rapport, som Det Kriminalpræventive Råd (DKR) netop har offentliggjort.

Sandheden er bare en anden. Langt de fleste angreb er nemlig mere eller mindre tilfældige. Taktikken er ofte at skyde med spredehagl og så håbe på, at der er gevinst, forklarer it-ekspert.

– Det tager kun seks minutter at scanne alle computere på internettet. Enhver computer på internettet bliver derfor scannet med jævne mellemrum af hackere, der søger en computer at angribe, så den lille virksomhed kan sagtens blive ramt. Se på det ud fra et cost-benefit-perspektiv. Det er gratis for hackerne at angribe et system, så selvom en hacker måske ikke får meget ud af at hacke et system, så er det en god investering, siger Willard Rafnsson, adjunkt på IT-Universitet i København.

Det kan godt være, at hackeren ikke kan bruge dit kundekartotek til noget særligt, men måske er det meningen at bruge din server til at få flere muskler til at sende endnu flere angreb ud i cyberspace. En anden meget brugt metode er at låse hele systemet og kræve løsepenge for at give adgang til filerne igen. Er der bare en lille brøkdel, der gør det, så virker forretningsmodellen for hackerne, da det som sagt nærmest er gratis for dem at gøre det. Samtidig er det vigtigt at forstå, at det ikke nødvendigvis kræver en doktorgrad i datalogi at slå sig ned som hacker. Der er en bred vifte af computerprogrammer, der lynhurtigt sætter uerfarne brugere i stand til at finde smuthullerne i sikkerheden.

– Jeg har studerende, der lærer at bruge de her værktøjer på et par uger. Ikke for at kunne hacke men for at kunne beskytte virksomhederne og vise hvor sårbarhederne er i systemerne, siger Willard Rafnsson.

Hver fjerde uden basal it-sikkerhed

Blandt de små- og mellemstore virksomheder (SMV'er) har 40 procent et lavt niveau for it-sikkerhed, da de kun bruger mellem nul og fire ud af i alt ni anbefalede sikkerhedsråd. Erhvervsstyrelsen konkluderer endda i sin seneste undersøgelse fra august i år, at 26 procent af SMV'erne ikke engang gør brug af de to helt centrale sikkerhedsforanstaltninger. Det drejer sig om opdatering af styresystemer og backup af data. For de helt små virksomheder på mellem fem og ni ansatte gælder dette for hver tredje af virksomhederne.

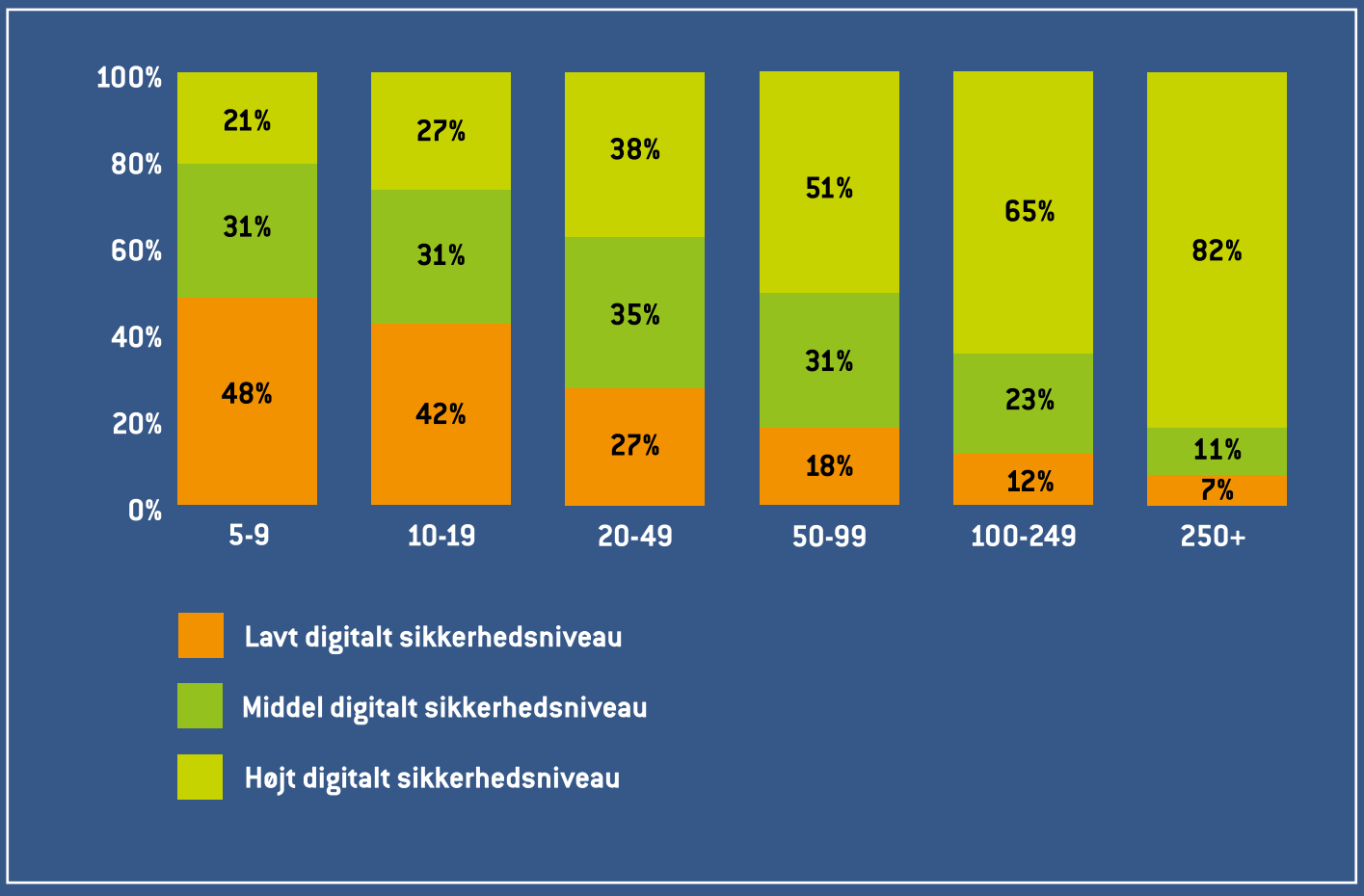
– Tragedien er, at sikkerhed koster penge, og det er ikke nemt at sælge, da det ikke giver nye funktioner. Derfor bør man argumentere med, at it-sikkerhed er en forsikring mod mulige skader, siger Willard Rafnsson.

Ni it-sikkerhedsråd

1. Systematisk opdatering af software
2. Backup af data
3. Adgangskontrol til netværk
4. Stærke adgangskoder
5. Lagring af logfiler
6. Brug af VPN
7. Kryptering af data
8. Risikoanalyse
9. Tests af it-sikkerhed

Kilde: Erhvervsstyrelsen, Digital Sikkerhed i Danske SMV'er, august 2020.

Digital sikkerhed fordelt på størrelse (antal ansatte)



Kilde: Digital Sikkerhed i Danske SMV'er, udgivet af Erhvervsstyrelsen.

Det kræver viden om de sikkerhedsrisici, der lurer i cyberspace, før man som virksomhedsejer kan vurdere, om man har sikret sig på den bedste måde. Af samme grund står IT-Universitet bag en række gratis online-webinarer, hvor små- og mellemstore virksomheder kan få råd og vejledning til at forebygge og håndtere cyberkriminalitet, uden at det kommer til at vælte årsregnskabet omkuld.

Byggebranchen helt i bund

Byggebranchen er især udfordret på it-sikkerheden. Ifølge undersøgelsen har kun 11 procent af virksomhederne i bygge- og anlægsbranchen et højt sikkerhedsniveau, mens det gælder for 27 procent af industrivirksomhederne. Man skal dog helt over i kommunikationsbranchen, før flertallet af SMV'erne har et højt sikkerhedsniveau. Ifølge it-eksperten kan der være flere årsager, men en af forklaringerne er, at håndværkerbranchen har omfavnet alle de nye muligheder i hverdagen gennem de seneste 20 år, uden at opmærksomhed på sikkerheden er fulgt med den udvikling.

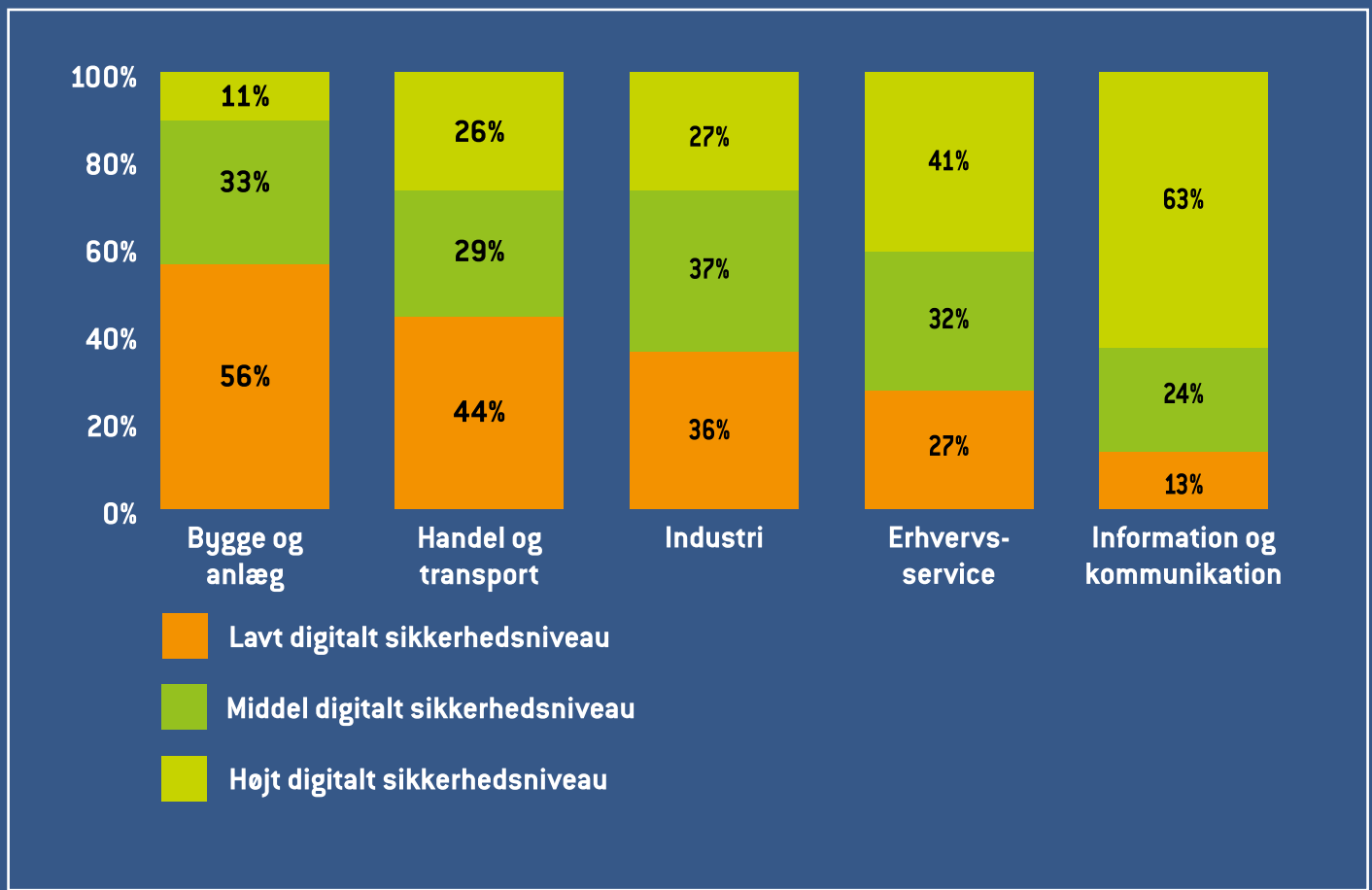
Om undersøgelserne:

Erhvervsstyrelsens undersøgelse er lavet på baggrund af besvarelser fra 5.292 virksomheder med minimum fem årsværk. De tilhører de private, ikke-finansielle byerhverv.

Det Kriminalpræventive Råds undersøgelse er en såkaldt kvalitativ undersøgelse, hvor man har interviewet i alt 36 af de helt små virksomheder (under 10 ansatte) om deres syn på it-sikkerhed.

Betegnelsen "SMV" er defineret ved at være virksomheder med 5-249 medarbejdere.

Digital sikkerhed fordelt på branche



Kilde: Digital Sikkerhed i Danske SMV'er, udgivet af Erhvervsstyrelsen.

– Før i tiden var it ikke så udbredt i el- og vvs-branchen, men it er krøbet gradvist ind hos dem, så det nu bliver brugt overalt til effektivisering. Det handler om alt fra servere til IoT-enheder, og derudover bruger medarbejderne smartphones i dagligdagen. It-løsningerne er blevet billigere, og der er mulighed for at bruge dem alle steder, men opmærksomhed på it-sikkerheden er ikke fulgt med den udvikling, siger Willard Rafnsson.

Minister: Det er en stor trussel

Erhvervsstyrelsen henviser i sin rapport til, at SMV'erne ikke føler sig i risikozonen for at blive ramt, da de ikke mener, at deres virksomhed rummer oplysninger, der har værdi for de it-kriminelle. Det skal man dog passe på med at tro, mener it-eksperten fra ITU. Installatørerne kan for eksempel ligge inde med kundernes forbrugsdata og andre oplysninger.

– Det er følsomme oplysninger for kunden, som derfor vil forvente, at de data er beskyttet, og for virksomhederne er det også værdifulde oplysninger, siger Willard Rafnsson.

Budskabet går igen på Christiansborgs gange, hvor forsvarsminister Trine Bramsen med bekymring ser på antallet af cyberangreb, der ifølge hende er steget kraftigt det seneste år.

– Det er alvorligt, og derfor bliver vi alle nødt til at være meget bevidste om, at det foregår og er en stor trussel. Vi ser også en bekymrende tendens til, at hackerne ikke kun låser oplysninger og kræver løsepenge. De begynder også at true med at offentliggøre intimiderende eller vigtige oplysninger for virksomhederne, medmindre de får løsepenge, udtalte Trine Bramsen i midten af oktober til TV2.

I løbet af coronakrisens første uger forklarede samme forsvarsminister, flankeret af Center for Cybersikkerhed, at hackerne ville forsøge at udnytte krisen til at skaffe sig adgang til både virksomheder og myndigheders it-systemer. Pludselig skulle en stor del af Danmark arbejde hjemmefra, hvilket gav risiko for sprækker i it-sikkerheden.

Opgør med forældet tankegang

Første skridt er derfor at få gjort op med forestillingen om "at der ikke er noget at hente hos mig" eller "at de kun går efter de store fisk". Sådan lyder det blandt andet i den nye undersøgelse fra Det Kriminalpræventive Råd (DKR). Her tager man udgangspunkt i de mindste virksomheder og ser på løsninger til at højne it-sikkerheden. Hvis det skal lykkes, er det nødvendigt at få virksomhederne til at indse risikoen, tage ansvaret på sig og stille krav til deres virksomheds it-sikkerhed. Det er ikke ensbetydende med, at alle installatører skal videreuddanne sig til it-eksperter, men ledelsen skal tage ansvaret på sig og stille krav til leverandøren. Det sker kun, hvis de får den rigtige vejledning. Her oplever en del SMV'er, at det er en jungle at finde rundt i produkter og leverandører på markedet. De savner en troværdig kilde at gå til, når de skal danne sig et overblik, og her kan oplysningskampagner og brancheorganisationer spille en rolle.

– De fleste virksomheder i denne undersøgelse orienterer sig typisk igennem brancheorganisationer om fagrelevante emner (25 ud af 33 adspurgte). Virksomhederne fortæller i forlængelse heraf, at det også er hos brancheorganisationer, at de helst vil have viden om it-sikkerhed. Gennem brancheforeninger skabes en indgang hos en aktør, som virksomhederne har tillid til, og som kender det specifikke fagområde, lyder det blandt andet i undersøgelsen fra DKR.

It-eksperten på ITU mener også, at mere viden er vejen frem, hvis man skal højne it-sikkerheden. Derudover skal procedurerne være nemme at følge i hverdagen.

– Uddan medarbejderne, så de er opmærksomme på angreb. Samtidig er det vigtigt, at sikkerhedsfunktionerne ikke bliver for vanskelige at bruge. Ellers risikerer man, at nogle lader være med at bruge dem, siger Willard Rafnsson. ●

It-kriminalitet: Ordforklaring

HACKING er uautoriseret adgang til en computer af it-kriminelle, som udnytter svagheder i sikkerheden på en computer.

PHISHINGMAILS kaldes i Danmark også trickmails. Det sker typisk ved, at du får tilsendt en e-mail (phishing), hvor afsenderen forsøger at få dig til at udlevere dine personlige oplysninger, som fx betalingskortoplysninger, NemID-oplysninger eller andre oplysninger, via e-mail, en falsk hjemmeside eller andet.

FALSKE FAKTURAER er ofte kendetegnet ved, at forurettede modtager fakturaer på varer eller ydelser, de ikke har modtaget. I disse sager er der - foruden bedrageri - ofte tale om dokumentfalsk i form af falske eller forfalskede fakturaer.

RANSOMWARE er kendetegnet ved, at dine data på computeren bliver krypteret af it-kriminelle, som kræver en løsesum for, at du kan få dine data igen. Det kan for eksempel være inficeret software, som er speciallavet til at blokere for adgangen til filerne på en computer.

CEO FRAUD kaldes i Danmark også for direktørsvindel. Ved CEO fraud anvendes ofte spoofing, så gerningspersonen kan sende en e-mail, der ser ud til at komme fra en virksomhedsdirektør eller en foreningsformand. Under dække af at være direktøren beder gerningspersonen over e-mail en økonomimedarbejder om at overføre et troværdigt beløb. I andre tilfælde benytter gerningspersoner sig af typosquatting, hvor gerningspersonen før angrebet registrerer et domænenavn (en e-mailadresse), der ligger så tæt op ad direktørens, at medarbejderen ikke bemærker, at den genkendelige e-mailadresse afviger med én enkelt karakter.