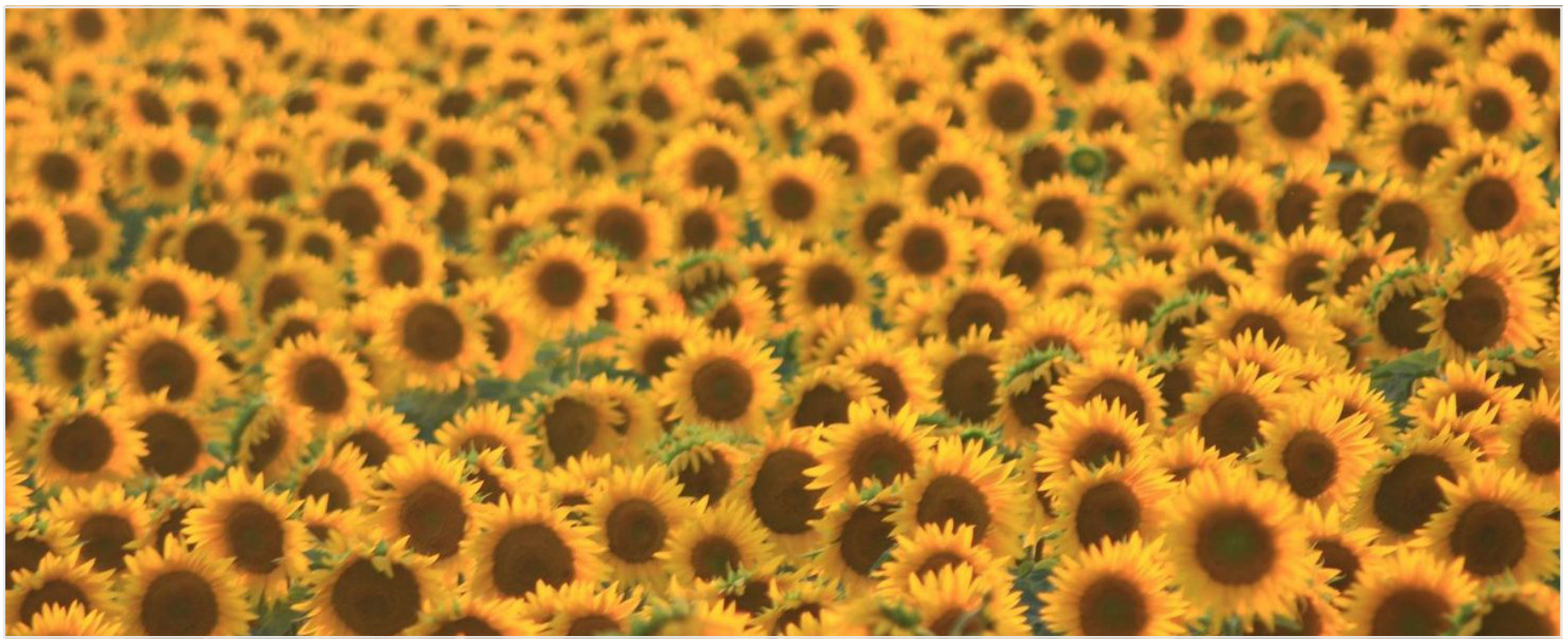
Juli 2019 | IT-trusler og cyber-sikkerhed



IT-SIKKERHED: DANSKE SMV'ER HALTER EFTER PÅ OMRÅDET, MEN HAR DET IKKE PÅ DAGSORDENEN

I en analyse af IT-sikkerhed og datahåndtering i danske SMV'er foretaget af Monitor Deloitte på vegne af Erhvervsministeriet tilbage i april 2018 blev det slået fast, at IT-sikkerheden i danske virksomheder på trods af en høj digitaliseringsgrad ikke har fulgt med trusselsbilledet. Helt konkret havde 39% af SMV'erne et utilstrækkeligt IT-sikkerhedsniveau set i forhold til deres risikoprofil, og det skyldtes dels et manglende engagement i IT-sikkerhed fra ledelsens side, dels en manglende imødekommenhed overfor forandringer fra medarbejdernes side. Monitor Deloittes rapport viste ligeledes, at 14% havde oplevet et IT-sikkerhedsbrud, og heraf havde 43% oplevet det inden for det seneste år. I en undersøgelse med et ligeværdigt datasæt foretaget af Danske Bank i april 2019, ser det ikke ud til, at meget har ændret sig siden i fjor – tværtimod antyder den nye undersøgelse, at tiltagene for at imødekomme den bekymrende kløft mellem gardering og sikkerhed på IT-området har været sparsommelige, og at der samtidig har været en nævneværdig stigning i antallet af angreb: 27 % af danske SMV'er meddeler her at have været udsat for et cyberangreb. Særligt hårdt ramt er de mellemstore virksomheder med mindst 50 ansatte, hvor hele 43 % angiver, at de har været ramt af et IT-angreb – men selv virksomheder med helt ned til to ansatte bidrager i hobetal til den kedelige statistik.

De største trusler mod IT-sikkerheden

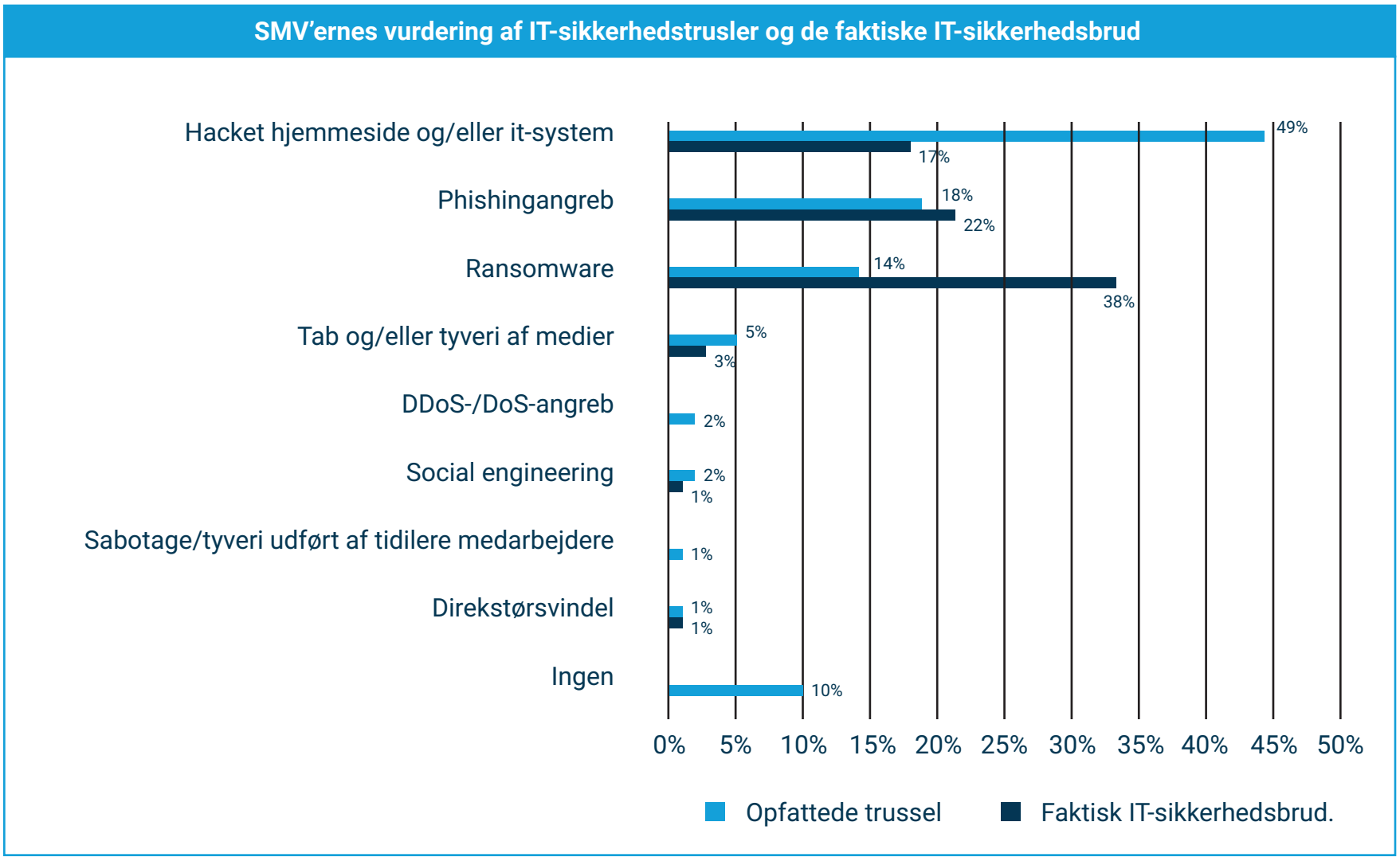
Der findes en række områder, hvor trusselsniveauet må vurderes at være højt nok til, at det bør være indtænkt i enhver virksomheds sikkerhedspolitik. Deloitte har i sin undersøgelse opgjort de mest relevante sikkerhedstrusler inden for IT, hvor de samtidig har sammenlignet med SMV'ernes egen vurdering af truslerne: **(se figur 1)**

Som det fremgår af Deloittes undersøgelse, er der væsentlige afvigelser mellem opfattet trusselsniveau og faktisk sikkerhedsbrud, hvor især faren ved en hacket hjemmeside er overvurderet, og faren ved Ransomware og phishing er undervurderet. PwC offentliggjorte samtidig som Deloitte deres "Cybercrime Survey 2018", og her blev truslerne procentmæssigt fordelt en smule anderledes blandt deres respondenter, men også her fremhæves Ransomware og især phishing som værende ekstraordinært vigtige at have for øje.

Ransomware er cyberkriminalitet, hvor svindleren udvikler et ondsindet krypteringsprogram, der kan tage dine filer/data som gidsel. Programmet er typisk skjult i et link i en e-mail eller på en hjemmeside, som ved et klik låser alle dine filer med en krypteringsnøgle. Du opkræves herefter betaling for at få fat i nøglen, som er din eneste chance for at få dine data igen.

Phishing er når du franarres følsomme oplysninger ved at en afsender giver sig ud for at være en troværdig kilde, til hvem du skal bekræfte et kodeord, kreditkortnummer, navne el.lign.

Danske Bank vælger dog at fremhæve to punkter, som de ud fra deres undersøgelser mener, er to former for cyber-svindel i 2019, du i særdeleshed bør indtænke i dine arbejdsgange.



Kilde: Wilke for Monitor Deloitte i rapport om IT-sikkerhed og datahåndtering

Figur 1

1) CEO fraud

CEO fraud handler basalt set om, at en svindler, typisk via e-mail, foregiver at være ejeren af virksomheden til en af medarbejderne, hvor vedkommende efterspørger en overførsel til en ny konto i forbindelse med et hemmeligt projekt e.l. Svindlerne i denne kategori er ofte mere sofistikerede og forberedte end afsenderne af de åbenlyst mistænkelige og stavefejlsfyldte e-mails, man kender fra spamfilteret. De bruger gerne meget tid på at skaffe oplysninger om virksomheden og ejeren, og i nogle af de mere professionelle tilfælde har svindlerne hacket sig ind på direktørens mailkonto, så de kan lære at efterligne direktørens sprogbrug kombineret med, at de opnår en indsigt i aktuelle begivenheder i din virksomhed, som de kan bruge til at virke mere overbevisende. Herefter kan mailen bliver efterfulgt af en opringning fra en troværdig person, der beder om en fremskyndelse af overførslen, og den loyale medarbejder i en blanding af stolthed over betroelsen og af frygt for at stille spørgsmålstegn parerer ordrer og foretager overførslen. Så snart pengene har forladt kontoen, er det i disse tilfælde typisk for sent, da de hurtigt sender dem videre til andre oversøiske konti.

2) Ændring af leverandøroplysninger

Næsten ligeså udbredt som den såkaldte "CEO-fraud" er hvor svindleren udgiver sig for at være en af din virksomheds faste leverandører. Med forskellige metoder får de et indgående kendskab til relationen mellem virksomheden og leverandøren, og i nogle tilfælde ved de tilmed, hvornår faste betalinger falder. Det giver svindlerne gode kort på hånden i forhold til at kunne opbygge troværdighed og i forhold til svindelnummerets timing. Det kan virke ganske harmløst at ændre et kontonummer og en forfaldsdato, når det kommer fra hvad der fremstår som en pålidelig kilde, og det er desværre først noget, der bliver opdaget, når den rigtige leverandør ringer og spørger ind til, hvor pengene bliver af.

Jo flere medarbejdere du har, des vigtigere er det at være opmærksom på digitale faresignaler og få kommunikeret dem utvetydigt ud - men uanset antallet af ansatte bør du have klare og nedskrevne processer på området til dine nuværende og fremtidige medarbejdere for at undgå at blive fanget i en omkostningstung og potentielt altødelæggende situation for din virksomhed.

Hvad kan du gøre for at sikre dig mod svindel på egen hånd?

› Kommuniker relevante risici for svindel klart ud til alle medarbejdere. Hvad, der virker som åbenlyse risici for dig som ejer, er måske ikke åbenlyse for dine medarbejdere.
› Indarbejd en proces, hvor medarbejdere altid kan og ved, at de skal bekræfte afsenderens identitet ved særlige ordrer.
› Bekræft altid alle e-mail-forespurgte ændringer fra samarbejdspartnere og leverandører med et opkald.
› Brug "four-eyes principle" ved transaktioner, der involverer større beløb. Eller to-faktor-kontrol med en form for login el.lign.
› Overvej hvilke oplysninger, der er nødvendige at dele om dine medarbejdere på hjemmesiden. Kan du f.eks. undvære at offentligt dele deres e-mailadresse?
› Overvej om det er nødvendigt at offentliggøre, hvilke leverandører du driver forretning med.
› Træn dine medarbejdere løbende i relevante områder som phishing m.m.
› Nedskriv en sikkerhedspolitik.
› Oplys eksplicit medarbejderne om, hvordan og hvem de skal kontakte ved tvivl eller mistanke om snyd.

Flere initiativer søsættes til at styrke IT-sikkerheden

Virksomhedsrådet for IT-sikkerhed

I marts 2016 nedsatte regeringen et virksomhedsråd for IT-sikkerhed, som har til formål at skabe dialog og erfaringsudveksling mellem private og offentlige aktører.

Virksomhedsrådet kommer med anbefalinger om, hvordan databeskyttelse og IT-sikkerheden kan styrkes i virksomheder med særligt fokus på SMV'er. Det har ført til flere konkrete og nyttige politiske retninger, blandt andet med "Strategi for Danmarks digitale vækst", der inkluderer 38 initiativer med et budget på knap 1 mia. kr. frem for 2025 og en "National strategi for cyber- og informationssikkerhed". Virksomhedsrådet har en bred vifte af kompetencer, da holdet er sammensat af en række prominente ledere inden for sikkerhedsafdelingerne fra store organisationer som blandt andet Novo Nordisk, PwC, Tryg, DI og DTU. I fornævnte rapporter har holdet bag virksomhedsrådet fremhævet tre overordnede indsatsområder, som de anbefaler, at der skal særligt politisk fokus på for at hæve IT-sikkerheden blandt SMV'er

1) Bedre viden om IT-sikkerhed og ansvarlig datahåndtering i små og mellemstore virksomheder
2) Kvalificeret udbud og efterspørgsel af den rigtige sikkerhed i løsningerne
3) Klare regler, hjælp til efterlevelse og effektiv håndhævelse

Det er med disse anbefalinger in mente, at de udtænker og udarbejder de relevante initiativer, som danner rammerne for den politiske udvikling på området. Læs mere om virksomhedsrådets anbefalinger her.

"Danmark skal have et mærke for IT-sikkerhed"

På lig linje med ordninger som "e-mærket" eller ISO-certificering foreslår Virksomhedsrådet for IT-sikkerhed, at der indføres en frivillig mærkningsordning for IT-sikkerhed, der skal gøre området til et større konkurrenceparameter i dansk erhverv, hvor intentionen her underforstået er at hæve det overordnede digitale sikkerhedsniveau. Tom Engly, Formand for Virksomhedsrådet for IT-sikkerhed udtaler:
"Vi har de seneste år set, hvordan cyberangreb kan have store økonomiske omkostninger for danske virksomheder. Desværre er særligt SMV'erne sårbare over for it-sikkerhedshændelser, fordi mange ikke har implementeret basale sikkerhedstiltag. Derfor anbefaler Virksomhedsrådet for IT-sikkerhed nu, at der etableres et frivilligt mærke for it-sikkerhed. Mærket skal nedsætte risikoen for it-sikkerhedshændelser og signalere til kunder, at der er styr på it-sikkerheden. Samtidigt skal det have et omkostningsniveau, så SMV'erne kan være med." (Sikkerdigital, 2019)
Mærket er tiltænkt som en bredt funderet ordning, der kører i samspil med andre tiltag på området. Det skal ikke erstatte eksisterende løsninger - det skal snarere bygge bro og udfylde det gab, der er imellem dem, så alle virksomheder uanset kompleksitet og modenhed kan være med.
(Se figur 2)

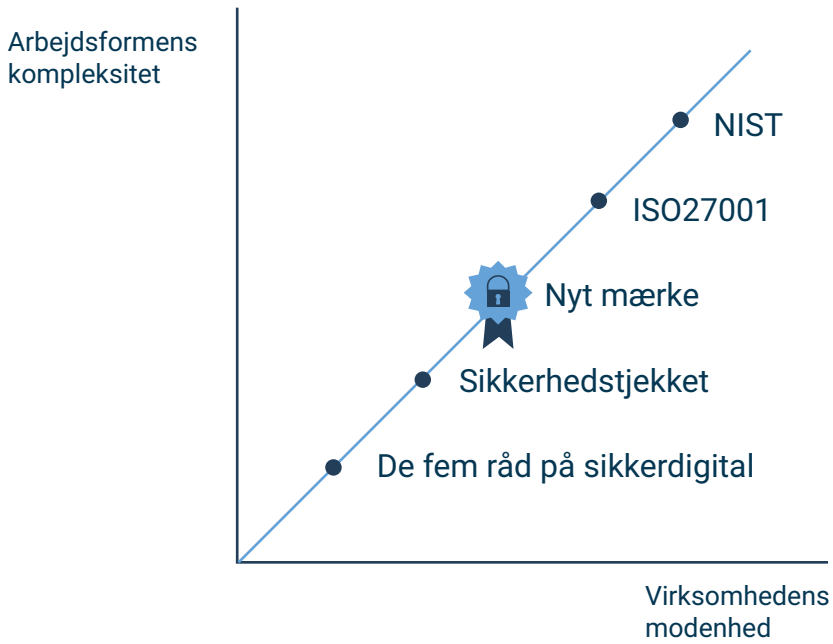
En sådan ordning er med fin succes blevet etableret hos vores britiske naboer allerede tilbage i 2017 under navnet "Cyber Essentials". Det er blandt andet de erfaringer, der har skabt grobund for ønsket om at implementere et IT-sikkerhedsmærke herhjemme. Selvom initiativet endnu ikke er søsat, kan du stadig med fordel opdatere din virksomheds sikkerhedspolitik med en eller flere af følgende tiltag

› De fem råd på sikkerdigital
› Sikkerhedstjekket
› ISO27001
› NIST

Bliv klogere på IT-sikkerhed

I forbindelse med fokusset på IT-sikkerhed og databeskyttelse har Erhvervsstyrelsen i samarbejde med Teknologisk Institut og PwC kortlagt markedet for IT-sikkerhedsydelser i Danmark, hvor der især lægges vægt på tab af data, beskyttelse mod elektroniske indbrud, rådgivning og forsikringsydelser. Rapporten giver et udførligt billede af branchen, hvor du både kan blive klogere på, hvordan markedet fungerer og på hvilke udbydere, der gør sig størst bemærket inden for hver sikkerhedsydelse. Du kan læse hele rapporten her.

Kompleksitet it-sikkerhedsarbejdsfromer ift. virksomheds modenhed



Figur 2

Kilde: EM, Anbefaling om et mærke for it-sikkerhed, 2019