Cybercrime Survey 2020

Virksomhedernes cybersikkerhedsstrategi skal nytænkes

pwc

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...

Højeste antal sikkerheds-hændelser i fire år

58%

angiver, at de har været udsat for én eller flere sikkerhedshændelser inden for de seneste 12 måneder.

Antallet af phishingangreb har aldrig været højere

79%

af dem, der har været udsat for en sikkerhedshændelse, siger, at de var udsat for phishingangreb.

Ét ud af tre phishing-angreb har været relateret til COVID-19-pandemien

35%

fortæller, at phishing-angrebene i nogen eller høj grad var relateret til COVID-19-pandemien.

Indhold

Virksomhedernes cybersikkerhedsstrategi skal nytænkes 3

PAVA – et forståeligt sikkerhedskoncept 4

Højeste antal sikkerhedshændelser i fire år 5

Høj grad af tillid til den finansielle sektors håndtering af data- og cybersikkerhed 6

Topledelsen mener, at de har bedre styr på cybersikkerheden 8

Behov for en øget indsats for at mindske persondatabrud 10

Ét ud af tre phishingangreb har været relateret til COVID-19-pandemien 12

Papirskjoldet er på plads 13

Awareness-træning er stadig i fokus i mange virksomheder 14

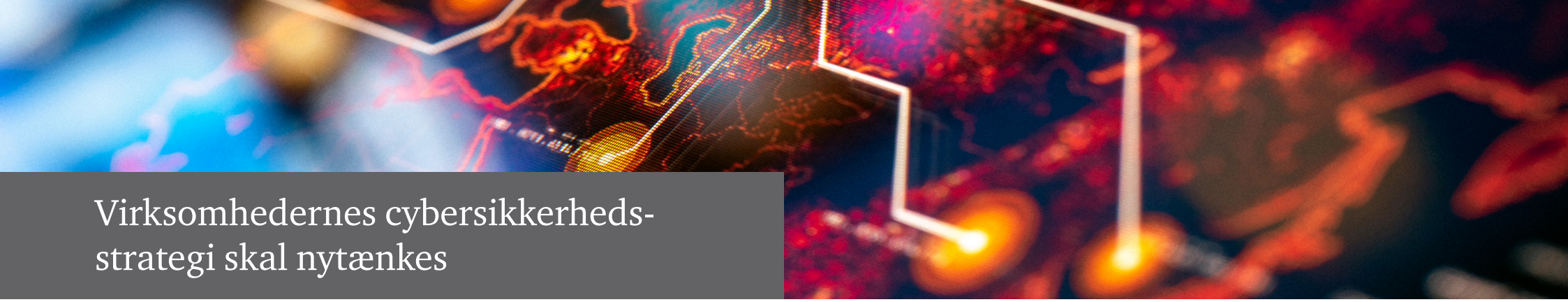
Antallet af phishingangreb har aldrig været højere 15

Virksomhederne højest prioriterede investeringer 18

Om undersøgelsen 20

Tjekliste 21

Kontakt 22



Virksomhedernes cybersikkerheds-strategi skal nytænkes

Cybercrime Survey 2020 viser, at der i år har været rekordmange phishingangreb. Heldigvis har mange virksomheder de seneste år forbedret deres cyber- og informationssikkerhed – og timingen for disse forbedringer kunne ikke have været bedre. COVID-19-pandemien har nemlig gjort det nødvendigt for mange virksomheder at lade medarbejderne arbejde fleksibelt eller hjemmefra, hvilket skaber udfordringer på grund af den øgede mængde digitale kommunikation. Under COVID-19 accelererer virksomhederne også digitalt på andre områder med en overraskende høj fart og rykker flere digitaliseringsår frem på ganske få måneder. Men cyberkriminelle udnytter kriser som COVID-19 – hvilket undersøgelsen bekræfter, ved at ét ud af tre phishingangreb i 2020 har været relateret hertil.

Cybercrime Survey 2020 viser desuden, at 58 % (51 % i 2019) af de danske virksomheder har været ramt af en sikkerhedshændelse. Vi oplever, at virksomhederne har været ramt af ransomware-hændelser, som har haft en signifikant økonomisk konsekvens. Medierne har fx belyst hændelser, hvor virksomheder har oplyst om økonomiske tab på 500-700 mio kr.[1] som følge af ransomware.

Virksomhedens CISO skal være tæt på ledelsen

Cybersikkerhed er mere end nogensinde før blevet et vigtigt tema for topledere. Der er behov for nye metoder, hvorpå cybersikkerhed kan integreres på tværs af forretningens områder som del af en robust cybersikkerhedsmodel, der skal sikre virksomhedens "kronjuveler". Det er derfor vigtigt, at virksomhedens Chief Information Security Officer (CISO) er tæt på ledelsen, så der kan kommunikeres et klart trusselsbillede og løbende skabes enighed om virksomhedens risikoprofil. Indsigten i det aktuelle trusselsbillede samt det rigtige niveau for risikovillighed og generel cybersikkerhedsledelse skal drøftes i virksomhedens ledelse. Til gengæld skal virksomhederne passe på med at gå for detaljeret til værks i risikostyringen. Det er vores erfaring, at de få virksomheder, som er påbegyndt rejsen, er druknet i et kæmpe detaljeringsarbejde. Her kan man med fordel skabe et hurtigt overblik ved at se på de store trusler først.

Cyberinvesteringer vs. value at risk

Undersøgelsen indikerer også, at topledelsen har fået bedre styr på sikkerheden. Der er dog stadig tydelige udfordringer mellem topledelsen og sikkerhedsfagfolkene, hvilket er nemmest illustreret ved budgetteringsøvelsen. Hvis en virksomhed har 100 kr. eller 100 % til it- og sikkerhedsbudgettet, så vil en almindelig fordeling se således ud:

1. It-drift 98 %
2. Sikkerhed 1 %
3. Produktion/Fabrikker 1 %.

Denne fordeling gør det svært at indføre store forandringer, da CISO'en først og fremmest skal trænge igennem mange ledelseslag, men også skal forsøge at forsvare, at flere økonomiske midler bliver afsat til sikkerhed. Det gab, der findes mellem det nuværende (og oftest manglende) sikkerhedsbudget og de reelle forandringer, der skal til, kan være svært at balancere. En virksomhed, der har haft en sikkerhedshændelse, er klar over de store omkostninger. Dette skulle vi dog alle helst undgå at opleve, og derfor kan "beregningsøvelsen" om, hvilken værdi/omkostning der er på spil, være relevant at inddrage i denne dialog.

Det er langt nemmere at have en effektiv dialog, hvis emnet omhandler risici, hvor investeringer kan reducere risikoen for et angreb og/eller minimere tabet ved en hændelse. Derfor er der brug for, at topledelsen og bestyrelsen stiller krav om bedre cyberrisikostyring, men også får koblet den eventuelt eksisterende Enterprise Risk Management-funktion tættere på sikkerhed, så virksomheden får et transparent perspektiv. Når dette er gjort, skal man blive bedre til at måle effekten af sine investeringer. Det er vores erfaring, at der stadig er for mange tilfældige investeringer, hvor man ikke altid får fulgt op på værdien. Stærk rapportering, risikobaseret styring og fælles beslutninger binder det hele sammen og skaber de bedste rammer for et vellykket cyberprogram.

Mads Nørgaard Madsen
Partner
Security & Technology

1) www.dr.dk/nyheder/penge/hackerangreb-koster-dansk-virksomhed-over-en-halv-milliard

PAVA – et forståeligt sikkerhedskoncept

Undersøgelsesresultatet er struktureret ud fra PwC's PAVA-koncept. Et koncept, vi mener, kan medvirke til at skabe en fælles forståelse mellem topledelsen og de fagfolk, der arbejder med sikkerhed. PAVA-konceptet er et generisk kommunikations-, vurderings- og rapporteringskoncept, som virksomheder kan bruge til bl.a. at vurdere og rapportere deres parathed og robusthed over for forskellige typer af cyberrisici og -trusler.

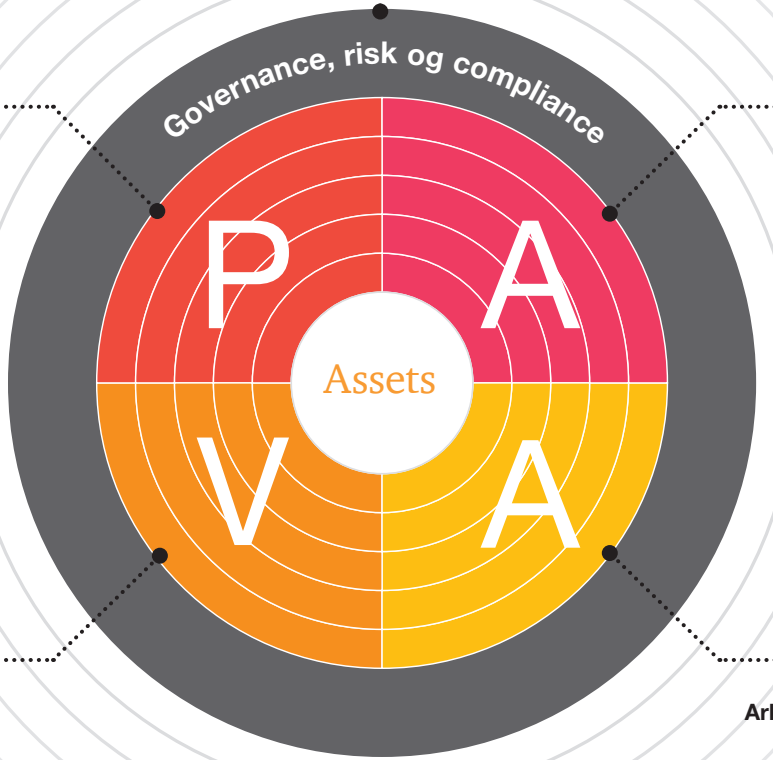
Konceptet kan anvendes på tværs af de mange forskellige sikkerhedsstandarder og frameworks og kan derfor rumme denne kompleksitet, samtidig med at der kan skabes klare fokusområder til sammenligning med andre virksomheder. På den måde giver PAVA et fælles grundlag for konkrete og prioriterede løsninger inden for specifikke sikkerhedsområder i virksomheden til brug i en bredere kontekst og til løbende effektmåling. PAVA dækker over fem hovedområder – fra governance, risk og compliance til proces, adfærd, validering og arkitektur.

Afhængig af den enkelte virksomheds modenheds- og sikkerhedsniveau er der behov for en indsats inden for alle områder, hvis man skal opnå en langsigtet og robust cyber- og informationssikkerhed. Denne struktur følger også de fleste virksomheders måde at fordele ansvar og roller for sikkerhedsarbejdet på, ligesom det er muligt at fokusere på enkelte områder efter behov uden at miste overblikket.

Procesområdet
dækker de processer og forretningsgange samt den dokumentation, som virksomheden har etableret, herunder hvordan processer er designet og kommunikeret, og om de er effektivt implementeret.

Governance, risk og compliance-området
er de styringsrammer, som virksomheden har eller bør etablere for at sikre en risikostyret prioritering af sikkerhedstiltagene samt for at overholde de gældende love, regler og krav.

Adfærdsområdet
omfatter niveauet af medarbejdernes bevidstheds- og kompetenceniveau i forhold til virksomhedens sikkerheds- og compliance-krav.



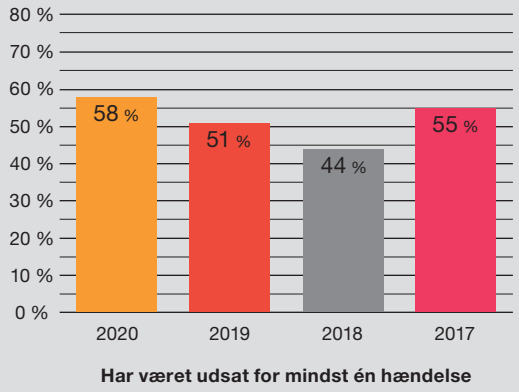
Valideringsområdet
beskriver aktiviteter til at opdage og verificere svagheder og sårbarheder i forhold til virksomhedens sikkerheds- og compliance-niveau.

Arkitekturområdet dækker design, konfiguration og implementering af tekniske og fysiske løsninger i forhold til virksomhedens sikkerheds- og compliance-niveau.

Højeste antal sikkerheds-hændelser i fire år

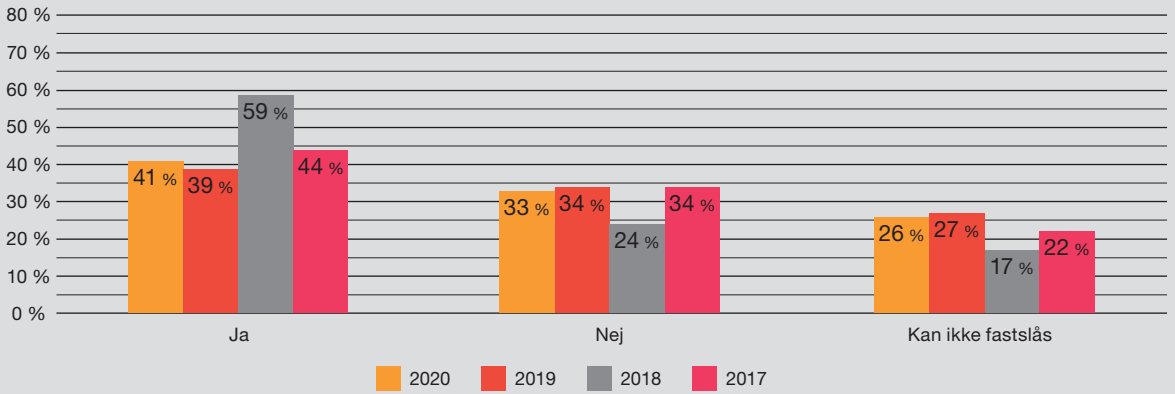
I Cybercrime Survey 2020 har 58 % angivet, at deres virksomhed har været udsat for minimum én hændelse inden for den seneste regnskabsperiode. Det er en stigning på 7 %-point sammenlignet med 2019 og hele 14 %-point i forhold til 2018. Hændelserne er nogenlunde lige så målrettede som i 2019, idet 41 % svarer, at de har oplevet én eller flere sikkerhedshændelser, der var målrettet deres virksomhed (39 % i 2019). Det stigende antal hændelser hænger godt sammen med, at respondenterne fortsat udviser betydelig bekymring for cybertruslen. 54 % angiver, at de er mere bekymrede for cybertrusler i dag, end de var for 12 måneder siden, hvilket dog er lidt færre end i 2019 (58 %).

Q Hvor mange gange har din virksomhed været udsat for en sikkerhedshændelse inden for det seneste regnskabsår?

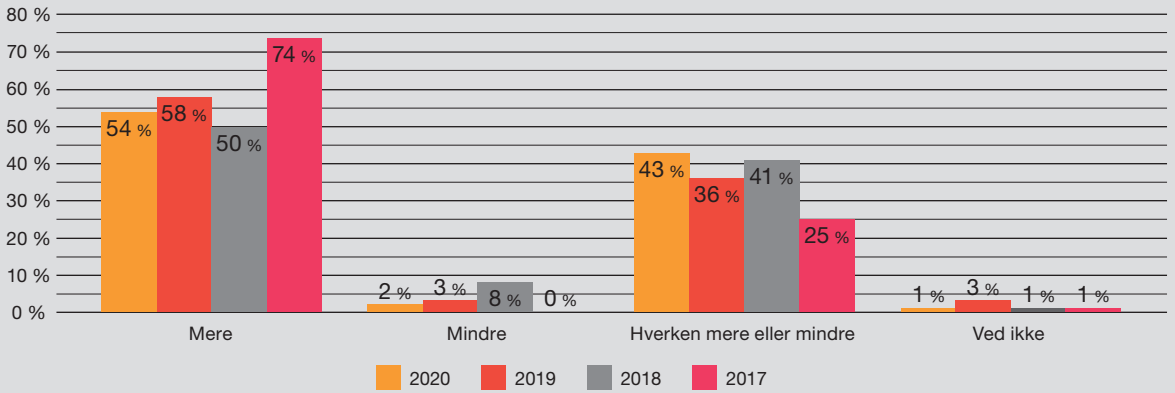


Har været udsat for mindst én hændelse

Q Har I i din virksomhed oplevet én eller flere sikkerhedshændelser, der var målrettet din virksomhed?



Q Bekymrer du dig mere eller mindre om de cybertrusler, I i din virksomhed oplever i dag, end du gjorde for 12 mdr. siden?



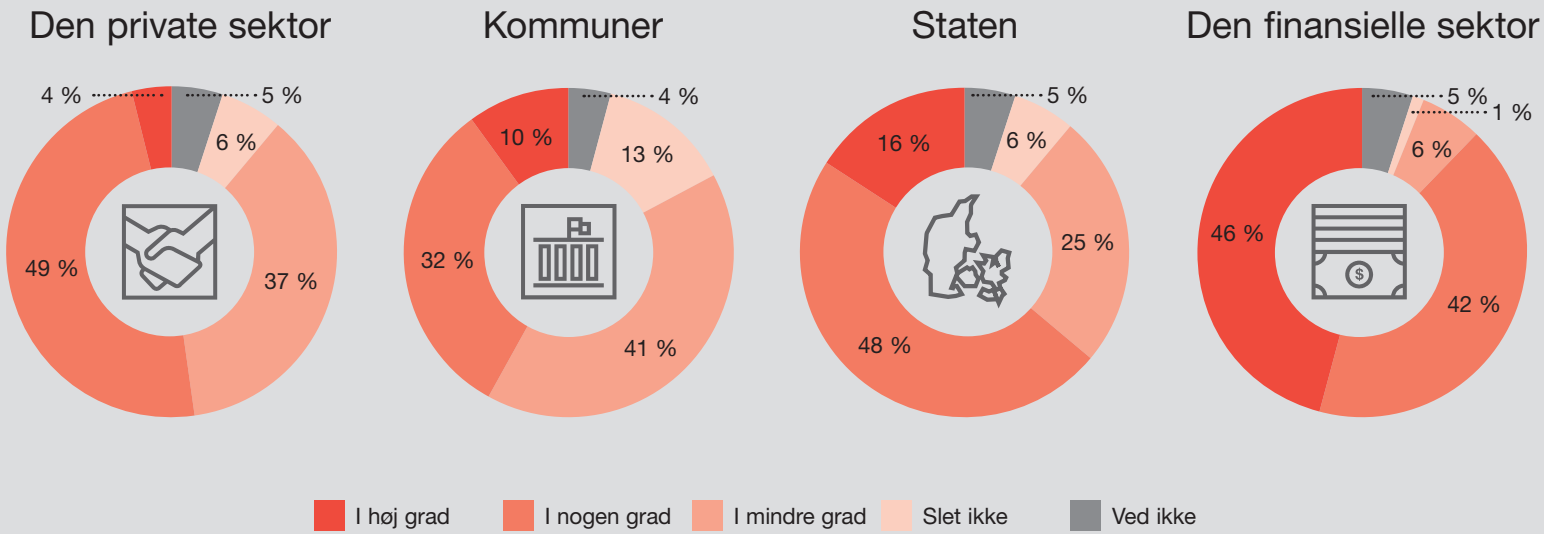
Høj grad af tillid til den finansielle sektors håndtering af data- og cybersikkerhed

De seneste års større brud på sikker og korrekt datahåndtering i såvel private som offentlige virksomheder sætter tilliden til virksomhedernes evne til at håndtere kunders og borgeres data under pres.

PwC's Cybercrime Survey viser, at tilliden til GDPR-compliance i den finansielle sektor er steget sammenlignet med 2019. I år angiver 88 %, at de i nogen eller høj grad har tillid til GDPR-compliance-niveauet i den finansielle sektor (77 % i 2019). Tilliden til GDPR-compliance i kommunerne er til sammenligning markant lavere. Her er billedet i forhold til sidste år uændret, idet 42 % svarer, at de i nogen eller i høj grad har tillid til GDPR-compliance i kommunerne (43 % i 2019). 54 % angiver, at de i mindre grad eller slet ikke har tillid til kommunernes GDPR-compliance (53 % i 2019).

Der ses en positiv udvikling i tilliden til den private sektors GDPR-compliance. Lidt over halvdelen (53 %) svarer i år, at de i nogen eller i høj grad har tillid til den private sektor. Dette tal var 40 % i 2019. Ligeledes ses en øget tillid til statens GDPR-håndtering, hvor 64 % angiver, at de i nogen eller høj grad har tillid til staten. Det er en stigning på 8 %-point sammenlignet med 2019.

Q I hvilken grad har du tillid til GDPR-compliance-niveauet i...

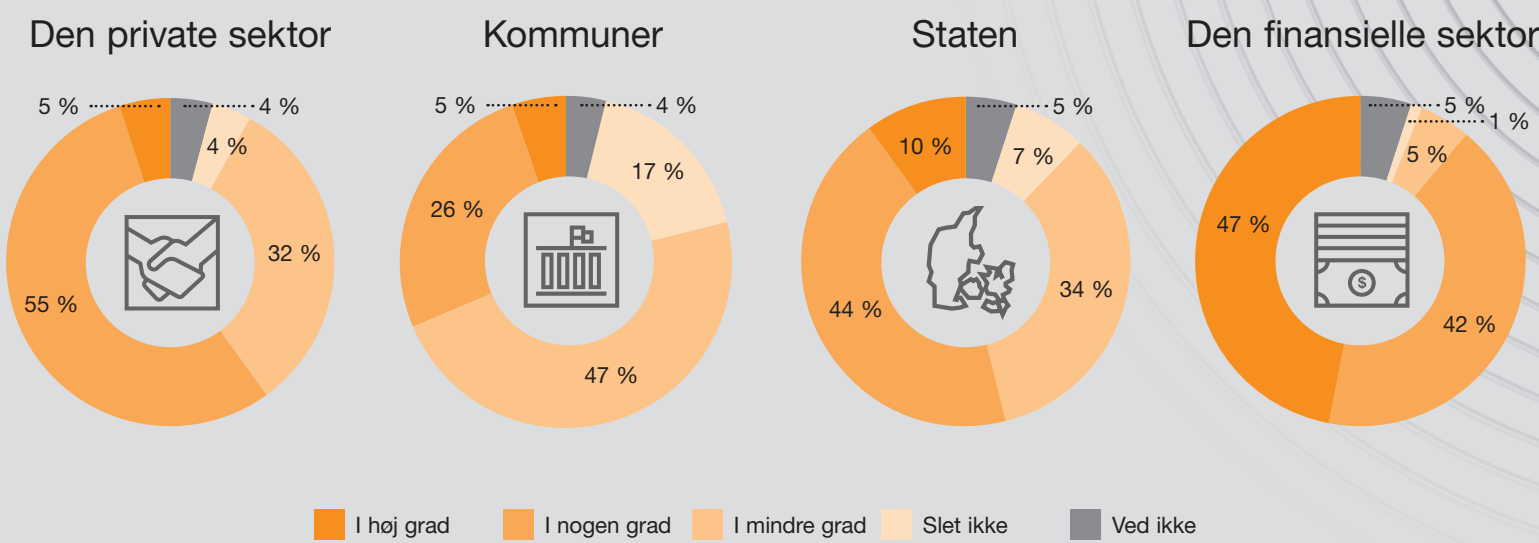


Når det gælder tilliden til cybersikkerhed, så er der i 2020 størst tillid til den finansielle sektor, hvilket også gjorde sig gældende i 2019. Hele 89 % angiver i år, at de i nogen eller i høj grad har tillid til cybersikkerheden i den finansielle sektor (86 % i 2019). Også på dette område er tilliden til kommunerne lavere. 74 % tilkendegiver således, at de i mindre grad eller slet ikke har tillid til cybersikkerheden i denne sektor. Tallet var 67 % i 2019, hvilket altså viser en negativ udvikling i tilliden til den offentlige sektor på 7 %-point.

Der ses desuden en øget tillid til cybersikkerheden i den private sektor i forhold til 2019. 60 % har i nogen eller i høj grad tillid til cybersikkerheden i den private sektor, hvilket er en stigning på 6 %-point sammenlignet med 2019. Tilliden til statens cybersikkerhed er på niveau med sidste år.

PwC anbefaler, at virksomhederne arbejder med tilliden til sikker og korrekt håndtering af borgeres og kunders data. Dette arbejde bør både være internt med fokus på at forhindre hændelser og eksternt med aktiviteter, som viser omverdenen, at datahåndtering er noget, man prioriterer og tager seriøst.

Q I hvilken grad har du tillid til cybersikkerheden i...



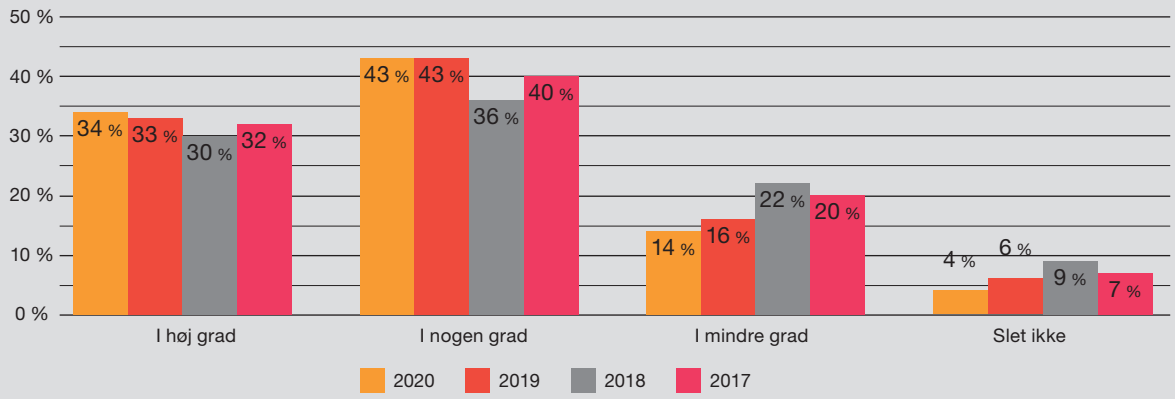
Topledelsen mener, at de har bedre styr på cybersikkerheden

Skal virksomheder lykkes med arbejdet inden for cyber- og informationssikkerhed, er det afgørende med ledelsesmæssig opbakning og forståelse, således at ressourcer og indsatser prioriteres på de rette områder.

I Cybercrime Survey 2020 tilkendegiver 77 %, at ledelsen i nogen eller i høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed.

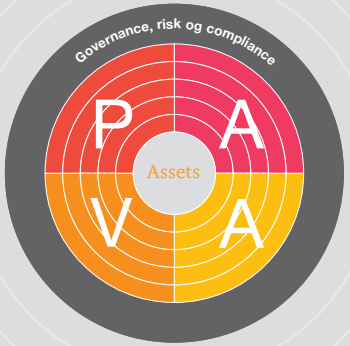
Det er på niveau med sidste år (76 % i 2019). Der ses dog samtidig en tydelig forskel på, hvordan CXO'er[2] og fagfolk[3] forholder sig til spørgsmålet. Således mener 86 % af CXO'erne, at ledelsen i nogen eller høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed, hvilket blot gør sig gældende for 72 % af fagfolkene.

Q I hvilken grad har direktionen/ledelsen i din virksomhed, efter din opfattelse, fokus på at opnå den rette balance mellem de cybertrusler, I står over for, og investeringer i cybersikkerhed?



2) Inkluderer stillingsbetegnelserne CEO, CFO, CIO, CCO, CTO mv.
3) Inkluderer stillingsbetegnelserne CISO, sikkerhedsmedarbejdere, sikkerhedsspecialister og øvrige medarbejdere.

Governance, risk og compliance



Game of Threats™

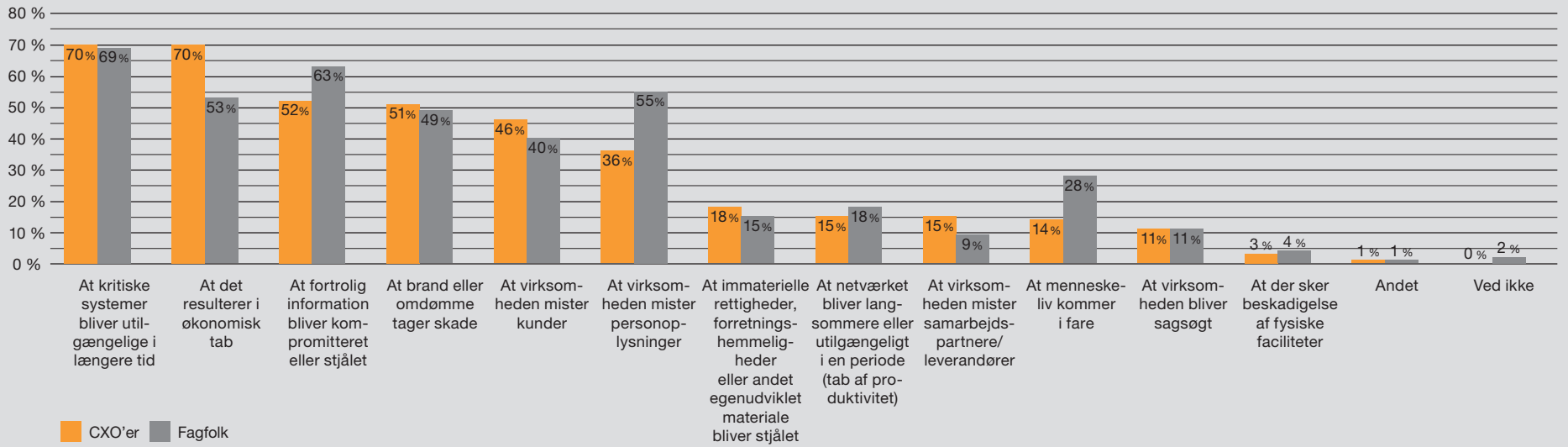
PwC's Game of Threats er specielt designet til at give ledelseslaget interaktiv undervisning i de risici, som er forbundet med cyberkriminalitet, og i vigtigheden i at investere i cyber- og informationssikkerhed. Læs mere på www.pwc.dk/cyberaware

Bestyrelse

Cybercrime Survey 2020 viser, at 81 % af de bestyrelsesmedlemmer, der har besvaret surveyen, angiver, at der ikke er etableret et cybertrænings- og uddannelsesprogram for bestyrelsen. Ligeledes svarer 67 % af bestyrelsesmedlemmerne, at de ikke modtager relevant rapportering med bl.a. cyberrisikovurdering, resultater fra sikkerhedstest, sikkerhedshændelser og resultater af audit forud for hvert bestyrelsesmøde.

Q

Hvad er din virksomheds største bekymring i relation til konsekvenserne af en sikkerhedshændelse?

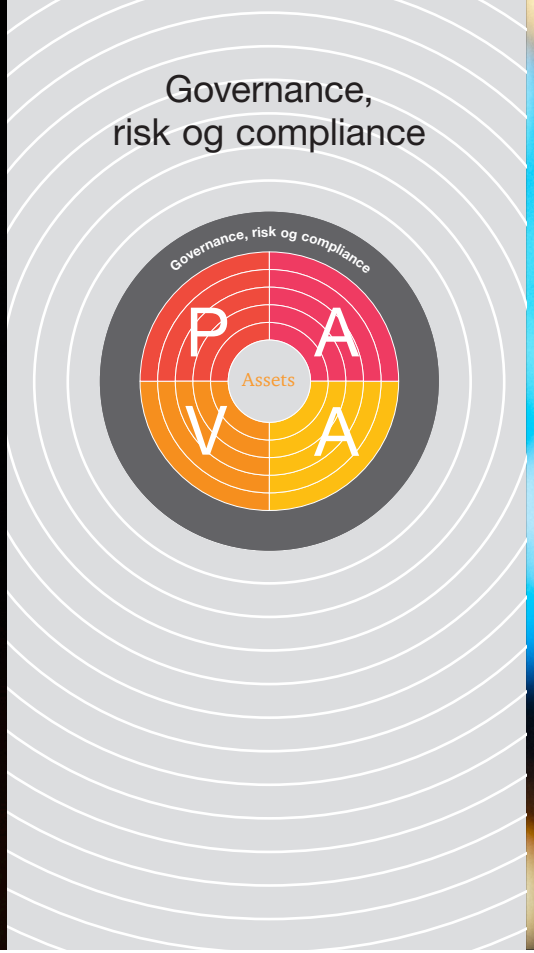


CXO'ernes og fagfolkenes primære bekymring i relation til sikkerhedshændelser er, at kritiske systemer bliver utilgængelige i længere tid. Det gør sig gældende for 70 % af CXO'erne og 69 % af fagfolkene.

CXO'erne er betydeligt mere bekymrede for, at en sikkerhedshændelse resulterer i økonomisk tab, mens fagfolkene i højere grad er bekymrede for, at fortrolig information bliver kompromitteret eller stjålet, samt at virksomheden mister personoplysninger.

For at sikre en fælles opfattelse hos topledelsen og fagfolkene anbefaler PwC, at virksomhedens topledelse fastsætter og kommunikerer deres risikoappetit ved at gennemføre en risikovurdering med udgangspunkt i potentiel forretningskonsekvens, således at fagfolkene kan støtte op om og være med til at prioritere effektive sikkerhedstiltag.

Behov for en øget indsats for at mindske persondatabrud

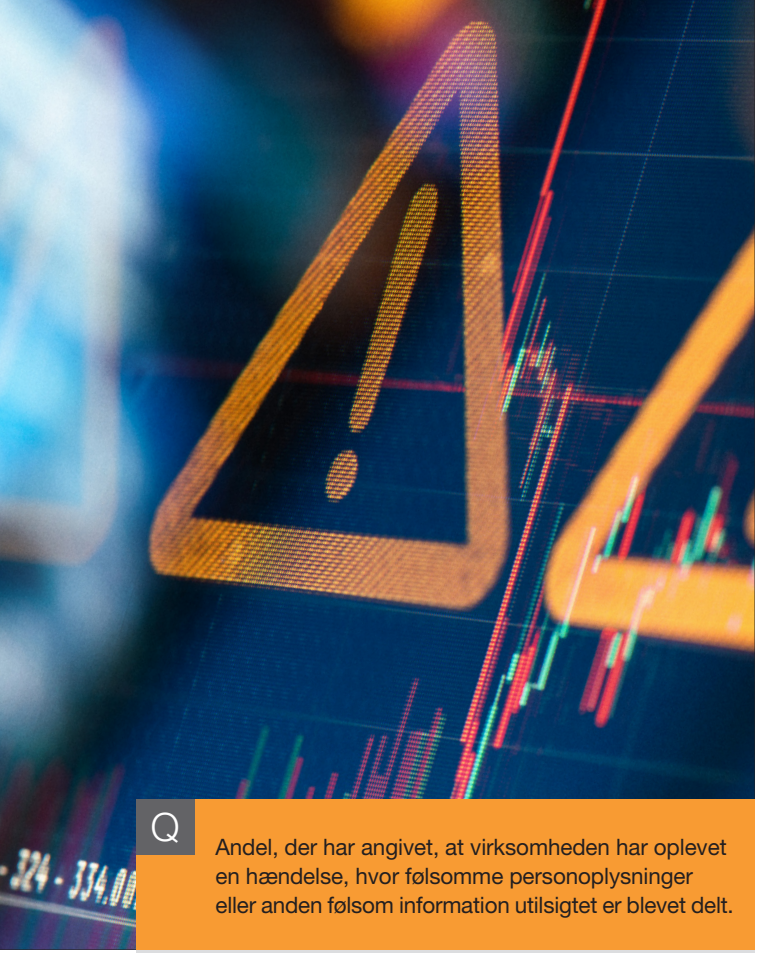


I Cybercrime Survey 2020 peger færre end tidligere på lovkrav/regulativer, herunder fx GDPR, som en trussel for virksomheden. Således svarer 15 % i 2020, at lovkrav/regulativer udgør den største trussel i relation til cyber- og informationssikkerhed. I 2019 var tallet 28 %, mens det i 2018 lå på hele 41 %.[4]

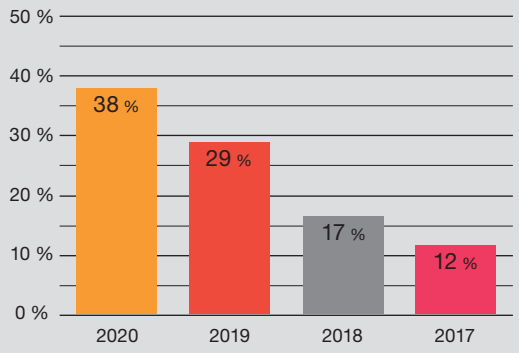
Dette skal ses i lyset af, at der i år er en betydelig stigning i antallet af hændelser, hvor følsomme personoplysninger eller anden følsom information utilsigtet er blevet delt (2020: 38 %, 2019: 29 %, 2018: 17 %, 2017: 12 %).[5]

Samtidig viser undersøgelsen, at virksomhederne befinder sig på samme niveau som sidste år i forhold til at beskytte de personoplysninger, som findes i virksomheden. I år svarer 88 % således, at virksomhedens personoplysninger i nogen eller i høj grad er tilstrækkeligt beskyttet i henhold til persondataforordningen (GDPR) (mod 89 % i 2019).

4) Se tabel over de største trusler for virksomhederne i relation til cyber- og informationssikkerhed på side 17.
5) Se tabel over, hvilke hændelser virksomhederne har oplevet de seneste 12 måneder, på side 16.

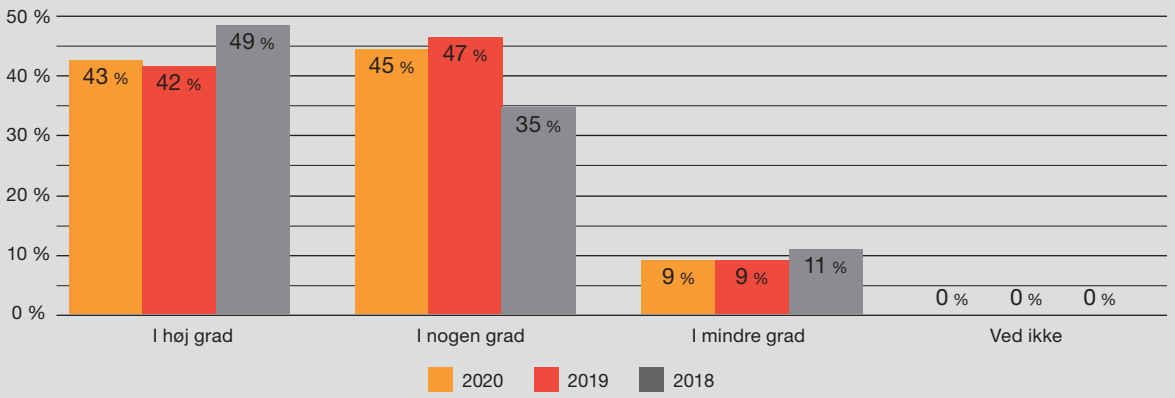


Q Andel, der har angivet, at virksomheden har oplevet en hændelse, hvor følsomme personoplysninger eller anden følsom information utilsigtet er blevet delt.



PwC erfarer, at langt de fleste virksomheder har designet og implementeret et GDPR-projekt, hvor der er kortlagt processer med personoplysninger, og de lovpligtige dokumenter er udarbejdet. Det er dog de færreste virksomheder, der har foretaget en afslutning af projektet og er overgået til en egentlig driftsfase. GDPR er ikke en engangsøvelse eller et juridisk papirskjold. PwC anbefaler derfor, at GDPR indarbejdes som en del af de faste forretningsprocesser, så det bliver en naturlig del af den daglige drift.

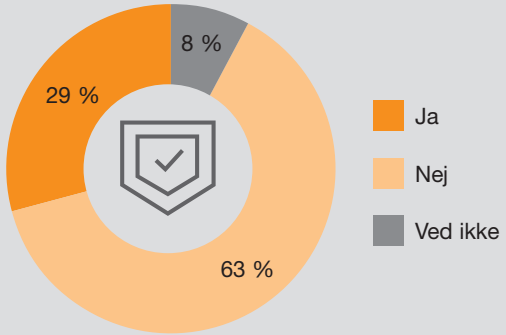
Q I hvilken grad er din virksomheds personoplysninger tilstrækkeligt beskyttet i henhold til persondataforordningen (GDPR)?



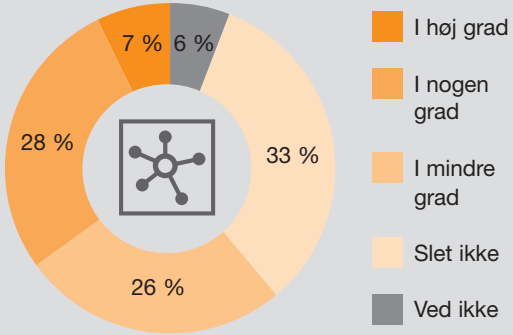
Ét ud af tre phishingangreb har været relateret til COVID-19

COVID-19 har sat sit præg på mange agendaer i 2020. Det gælder ikke mindst cyberagendaen, hvor COVID-19 har skabt grobund for nye muligheder og indgangsvinkler for cyberkriminelle, herunder muligheden for at udnytte sårbarheder i relation til hjemmearbejde. I den forbindelse svarer 29 %, at deres virksomhed har etableret et særligt cyberberedskab for at håndtere COVID-19-situationen. Således har ca. 2 ud af 3 (63 %) ikke etableret et særligt beredskab trods den øgede trussel. Cybercrime Survey 2020 har desuden kortlagt, hvordan virksomhederne konkret har været påvirket af COVID-19 – set fra et cyberperspektiv. Én ud af tre virksomheder (35 %), som har været udsat for et phishingangreb, svarer, at angrebet i nogen eller i høj grad har været relateret til COVID-19. Her kan der fx være tale om, at cyberkriminelle har benyttet COVID-19-relaterede budskaber i selve phishingmailen.

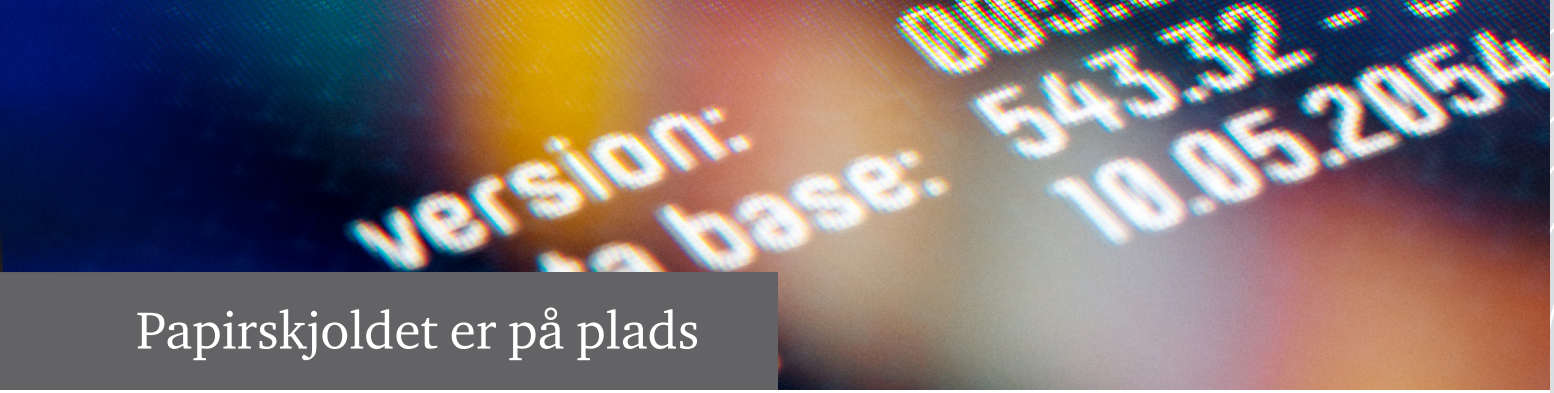
Q Har I etableret et særligt cyberberedskab i forbindelse med jeres virksomheds håndtering af COVID-19-situationen?



Q I hvilken grad har de phishingangreb, som I har oplevet, været relaterede til COVID-19? Fx at cyberkriminelle har benyttet COVID-19-relaterede budskaber i selve phishingmailen.



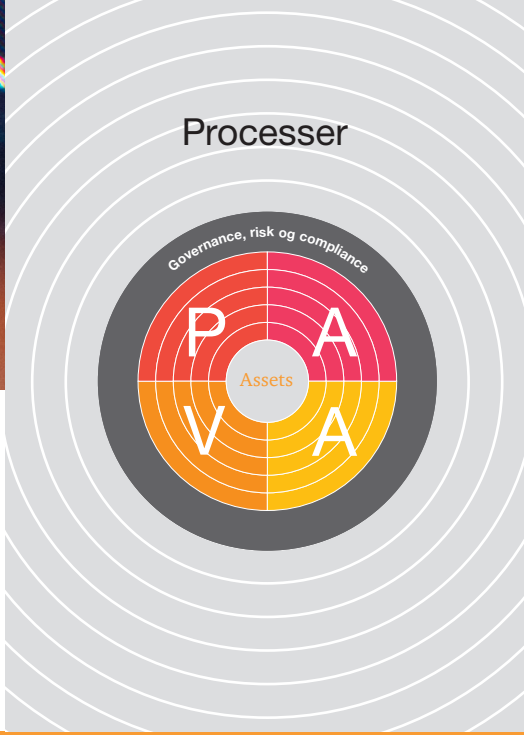
PwC anbefaler, at virksomhederne ikke nedprioriterer cybersikkerhedsaktiviteterne, selvom der er mange andre nye opgaver at varetage under en pandemi. Det vigtigste er at sikre, at it-sikkerhedsorganisationen ikke er underbemandet, og at man tager det nye trusselsbillede til efterretning. Det kan eksempelvis betyde, at man skal styrke overvågningen og evnen til at reagere på hændelser, eller at man udfører COVID-19-relaterede phishingtest for at øge medarbejdernes bevidsthed om truslen. Desuden bør der gøres en indsats for at skabe awareness hos medarbejderne om risikoen ved hjemmekontor og fjernarbejde.



Papirskjoldet er på plads

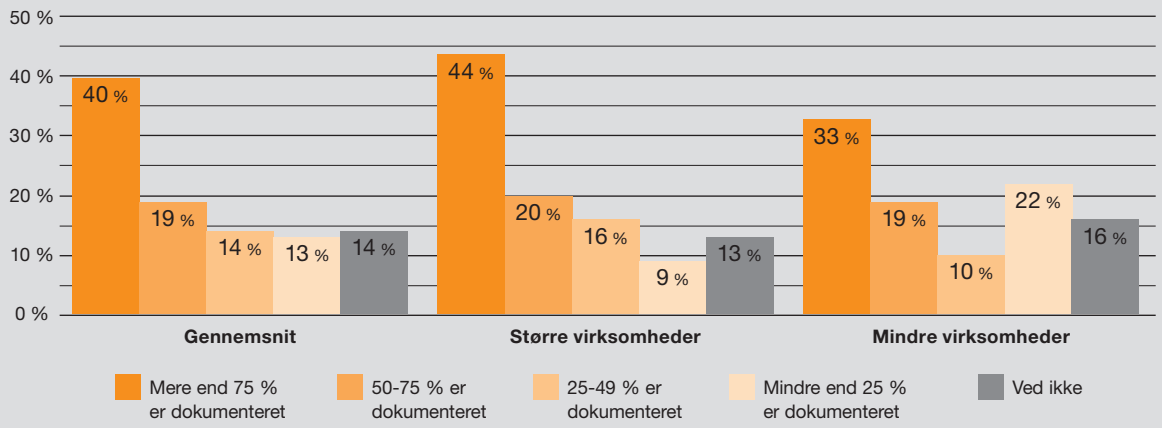
Der er fortsat behov for, at virksomhederne skifter fokus fra styring og compliance til teknisk forebyggelse og opdagelse for reelt at kunne øge cybersikkerheden. Vi ser i den forbindelse en tendens til, at virksomhederne har fået bedre styr på dokumentationen. På spørgsmålet om, i hvilket omfang sikkerheds- og lovgivningskrav er dokumenterede i virksomhedens interne retningslinjer, procedurer og/eller vejledninger, svarer 40 %, at mere end 75 % er dokumenteret.

Samtidig angiver 13 %, at mindre end 25 % er dokumenteret. Undersøgelsen viser også, at det primært er de større virksomheder, der arbejder med veldokumenterede processer. På det samme spørgsmål svarer 44 % af de større virksomheder, at mere end 75 % er dokumenteret, og kun 9 % svarer, at mindre end 25 % er dokumenteret, så der er fortsat plads til forbedring.



Q

I hvilket omfang er sikkerheds- og lovgivningskrav dokumenterede i jeres virksomheds interne retningslinjer, procedurer og/eller vejledninger?



PwC erfarer, at virksomheder i stigende grad ønsker at verificere, om deres politikker og retningslinjer er tilstrækkeligt forankret og efterlevet i organisationen – og ikke blot er publiceret med en forventning om, at alle medarbejdere så efterlever dem. PwC anbefaler, at virksomhederne øger indsatsen inden for design og implementering af tekniske sikkerhedstiltag samt verificering af, om disse er tilstrækkelige og effektive til at beskytte forretningen.

Awareness-træning er stadig i fokus i mange virksomheder

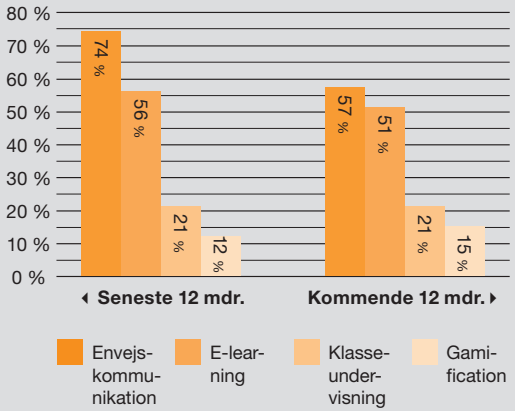
I takt med at truslen fortsat øges, er behovet for awareness-træning inden for cyber- og informationssikkerhed blevet større. Awareness-træning skal bidrage til at gøre medarbejderne opmærksomme på digitale trusler og risici, som kan have mindre eller større konsekvenser for virksomheden, kunder eller borgere.

I Cybercrime Survey 2020 svarer 74 %, at de i de seneste 12 måneder har gjort brug af envejskommunikation for at skabe awareness om cyber- og informationssikkerhed, hvilket er en stigning på 5 %-point sammenlignet med 2019. Envejskommunikation kan eksempelvis være i form af intranetnyheder og plakater. Lidt over halvdelen svarer, at de i de seneste 12 måneder har gjort brug af e-learning, hvilket ligeledes er en stigning på 4 %-point fra forrige år. Der ses en tendens til, at flere virksomheder supplerer envejskommunikation med e-learning, hvilket ligeledes gjorde sig gældende i 2019.

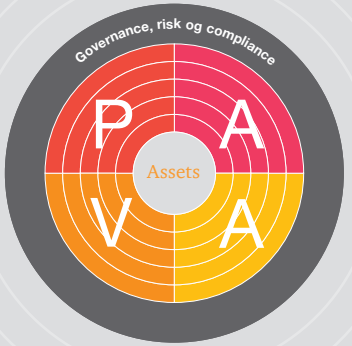
Vi ser, at færre planlægger envejskommunikation og e-learning de kommende 12 måneder sammenlignet med de seneste 12 måneder. Det er dog værd at bemærke, at flere virksomheder samtidig angiver, at awareness-træning i 2020 er deres højest prioriterede investering inden for it-sikkerhed.[6]

Q

Hvilke af følgende tiltag gør din virksomhed brug af i forbindelse med GDPR-, cyber- og informationssikkerheds-awareness?



Adfærd



E-learnings fra PwC

PwC har udviklet en række e-learnings om EU's persondataforordning og cybersikkerhed, som på en effektiv og lettilgængelig måde kan træne medarbejdere. Læs mere på www.pwc.dk/cyberaware

PwC anbefaler, at virksomhederne øger medarbejdernes bevidsthed om og evne til at opdage cyberangreb og agere i henhold til virksomhedens retningslinjer og dermed undgå at være "det svageste led" i virksomhedens forsvarskæde mod cyberkriminelle. Medarbejderne bør aktiveres med awareness-aktiviteter, som fx e-learning/micro-learning/blended learning, der i højere grad involverer modtageren og medvirker til en bedre forståelse og forankring af de vigtige budskaber.

6) Se grafen over virksomhedernes højest prioriterede investeringer inden for it-sikkerhed de næste 12 måneder på side 18.

Antallet af phishingangreb har aldrig været højere

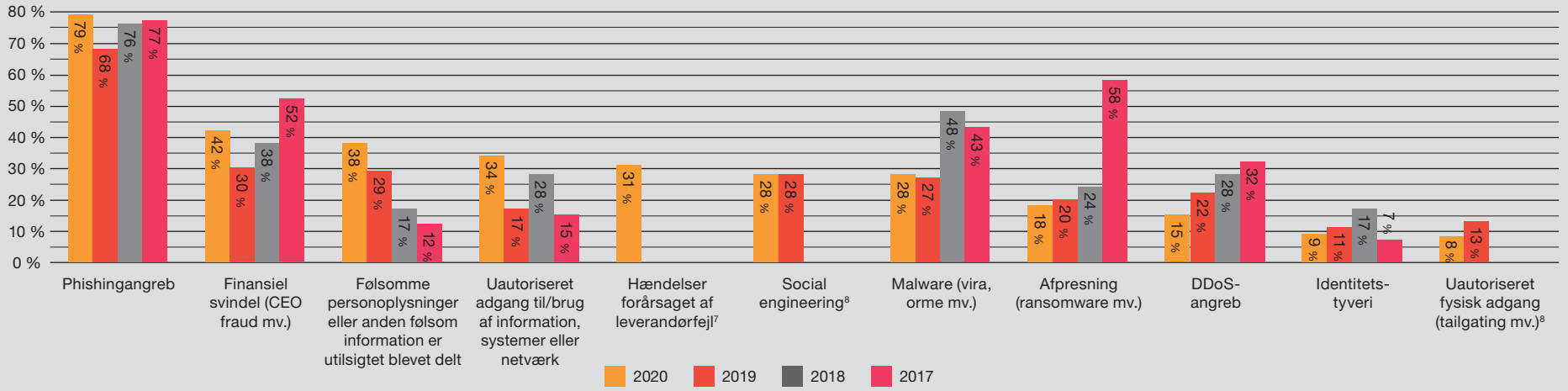
Cybercrime Survey 2020 viser, at phishingangreb til stadighed er den hyppigst oplevede angrebstype. Hele 79 % af dem, der har været udsat for cyberangreb, vurderer, at deres virksomhed har været udsat for phishingangreb de seneste 12 måneder. Det er en stigning på hele 11 %-point fra sidste år, og således er antallet af phishingangreb på det hidtil højeste niveau.

Der ses ligeledes en markant stigning i antallet af hændelser relateret til finansiel svindel, utilsigtet deling af følsomme personoplysninger/informationer og uautoriseret adgang til/brug af information, systemer eller netværk. I dette års Cybercrime Survey er hændelser relateret til leverandørfejl en ny svarmulighed. 31 % angiver, at de har oplevet denne type hændelse.

PwC oplever, at phishingangreb bliver mere og mere avancerede og netop forsøger at udnytte det svage led, der fx kan være en travl medarbejder. Awareness-aktiviteter, der fokuserer på denne trussel, inklusive simulerede phishingkampagner, kan medvirke til at reducere risikoen. Men virksomheden bør se bredere på de tekniske kontroller, der kan reducere konsekvensen ved et angreb. Det gælder bl.a. en forøget indsats for at beskytte den enkelte enhed ("endpoint") såvel som en højere grad af netværkssegmentering, der kan modvirke, at fx malware spreder sig fra én pc til hele virksomheden uden særlige forhindringer.

Q

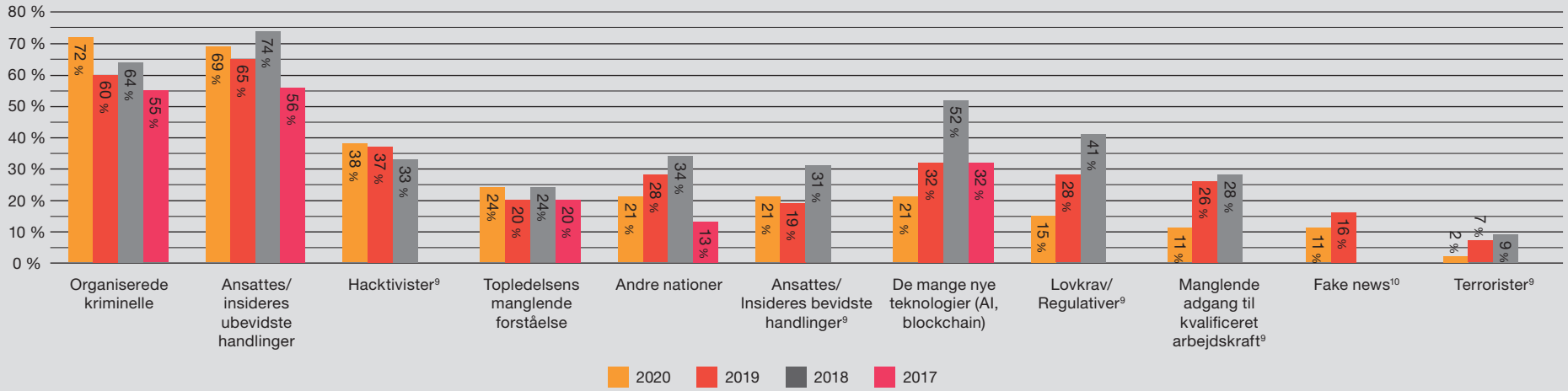
Hvilke hændelser har din virksomhed oplevet i de seneste 12 måneder som resultat af cyberkriminalitet eller informationssikkerhedshændelser?



7) Hændelser forårsaget af leverandørfejl er en svarmulighed tilføjet i 2020, hvorfor det ikke er muligt at påvise en udvikling fra 2019, 2018 og 2017.
8) Social engineering og uautoriseret fysisk adgang er svarmuligheder tilføjet i 2019, hvorfor det ikke er muligt at påvise en udvikling fra 2018 og 2017.

Q

Hvad udgør de største trusler for din virksomhed i relation til cyber-/informationssikkerhed?

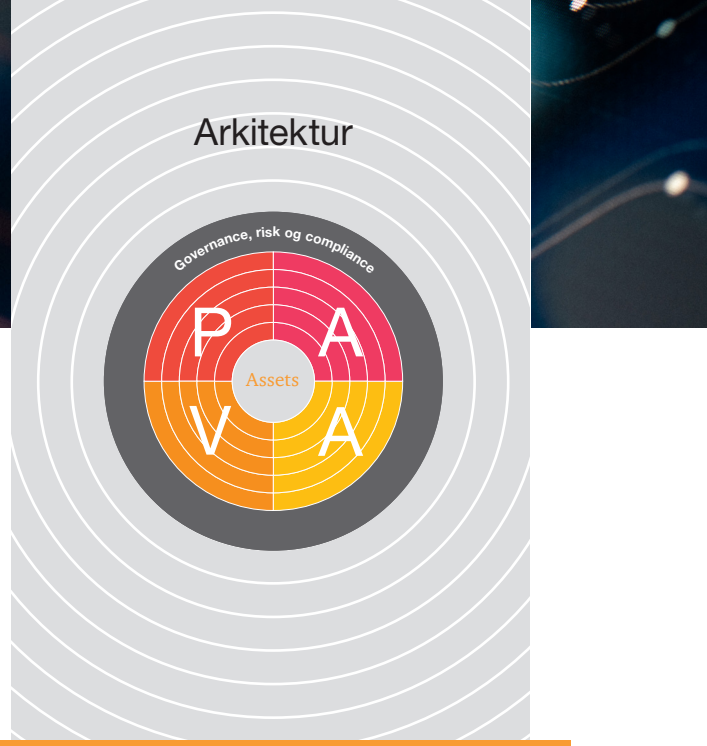


Undersøgelsen viser desuden, at organiserede kriminelle i år udgør den største trussel for virksomhederne i relation til cyber- og informationssikkerhed. Hele 72 % peger i 2020 på denne trussel, hvilket er en stigning på 12 %-point i forhold til sidste år. Efter organiserede kriminelle kommer sidste års højdespringer: Ansattes/insideres ubevidste handlinger (69 %). At ansattes/insideres ubevidste handlinger fortsat ligger højt på listen over trusler, kan afspejle det høje antal phishingangreb i år, da succesen ved denne type angreb afhænger af ansattes/insideres ubevidste handlinger.

Det er PwC's erfaring, at organiserede kriminelle i stigende grad forsøger at udnytte det menneskelige led, når de skal kompromittere virksomheder, hvilket ses i den stigende benyttelse af phishing-angreb. Som nævnt på foregående side, bør virksomheden målrette beskyttelsen mod denne trussel gennem en bred indsats, der omfatter awareness om truslen, endpoint-beskyttelse, beskyttelse af privilegerede adgange og netværksbeskyttelse. En enkelt med-arbejders ubevidste handling kan have alvorlige konsekvenser, hvis malware får mulighed for at sprede sig.

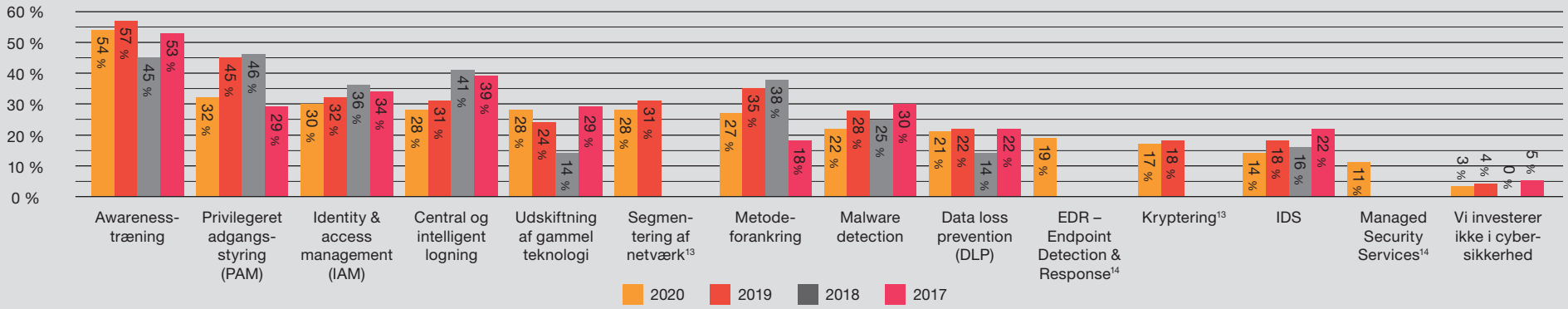
9) Hacktivister, ansatte/insiders bevidste handler, lovkrav/regulativer, manglende adgang til kvalificeret arbejdskraft og terrorister er svarmuligheder tilføjet i 2018, hvorfor det ikke er muligt at påvise en udvikling fra 2017.
10) Fake news er en svarmulighed tilføjet i 2019, hvorfor det ikke er muligt at påvise en udvikling fra 2018 og 2017.

Virksomhedernes højest prioriterede investeringer



Ser man på virksomhedernes investeringer, så viser undersøgelsen, at de tre højest prioriterede investeringer inden for cyber- og informationssikkerhed de næste 12 måneder er awareness-træning (54%), privilegeret adgangsstyring[11] (32%) og identity & access management[12] (30%). Det bemærkes, at disse top-3 investeringer alle er faldet siden 2019. Phishingangreb udgør en stor del af de sikkerhedshændelser, der rammer virksomhederne, hvilket kan hænge sammen med, at over halvdelen (54 %) angiver, at awareness-træning i 2020 er den højest prioriterede investering inden for it-sikkerhed. Awareness-træning er afgørende for at forebygge, at eksempelvis medarbejdere reagerer uhensigtsmæssigt på fx en inficeret e-mail i forbindelse med et phishingforsøg. Endvidere kan privilegeret adgangsstyring og identity & access management forhindre hackerne i at afvikle deres hackerprogrammer.

Q Hvad er din virksomheds højest prioriterede investeringer inden for cyber- og informationssikkerhed de næste 12 måneder?



11) Privilegeret adgangsstyring (PAM) handler om at få styr på de privilegerede rettigheder i en virksomheds infrastruktur.
12) Identity & access management (IAM) handler om at strukturere og automatisere alle identiteter i ens virksomhed, herunder rettidigt at sikre korrekt rettighedstildeling og -fratagelse.
13) Segmentering af netværk og kryptering er svarmuligheder tilføjet i 2019, hvorfor det ikke er muligt at påvise en udvikling fra 2018 og 2017.
14) EDR – Endpoint Detection & Response og Managed Security Services er svarmuligheder tilføjet i 2020, hvorfor det ikke er muligt at påvise en udvikling fra 2019, 2018 og 2017.

PwC anbefaler, at man sikrer sig effektivt og tilstrækkeligt imod organiserede kriminelle og hacktivister ved både at investere i en sund sikkerhedskultur (awareness) og med en bred indsats på understøttende sikkerhedsteknologier, med prioritet til proaktive beskyttelsesforanstaltninger for virksomhedens forretningskritiske applikationer, såsom sikring af privilegerede adgange, endpoint-beskyttelse og netværkssikring.

Om undersøgelsen

326 danske virksomhedsledere, it-chefer og sikkerheds-specialister har deltaget i PwC's Cybercrime Survey 2020. Undersøgelsen er igen i år gennemført med opbakning fra Center for Cybersikkerhed, DI Digital, Finans Danmark, Dansk Erhverv, IT-Branchen, Dansk It, KITA, Rådet for Digital Sikkerhed, ISACA og Bestyrelsesforeningen. Analysen bygger på onlinebesvarelser.

Respondenterne er blevet stillet en række spørgsmål, som relaterer til cyberområdet, fx om de er blevet ramt af et cyberangreb, om de er bekymrede for truslen fra cyberkriminalitet, hvad der er deres højest prioriterede investeringer, og i hvor høj grad virksomhedernes personoplysninger er tilstrækkeligt beskyttet i henhold til GDPR.

Målingens spørgsmål og svarmuligheder er udarbejdet af PwC, og onlinespørgeskemaet er udsendt i samarbejde med førnævnte organisationer.

Fakta: Undersøgelsens respondenter fordelt på sektorer

Den private sektor

67 %

Større virksomheder

Defineret ved ≥200 medarbejdere

Mindre virksomheder

Defineret ved ≤199 medarbejdere

Den offentlige sektor

22 %

Den finansielle sektor

11 %

Tjekliste

I PwC vil vi gerne hjælpe virksomhederne med at sikre sig bedst muligt mod cybertruslen – både før, under og efter et angreb. Da løsningerne kan være mange og ofte komplekse, har PwC udarbejdet nedenstående liste, der kan hjælpe virksomhederne med at tage stilling til nogle af de vigtigste indsatsområder inden for cyber- og informationssikkerhed.

Governance, risk og compliance

- [ ] Har i etableret et formelt sikkerhedsudvalg med repræsentanter fra virksomhedens topledelse?
- [ ] Arbejder I struktureret med risikovurdering ud fra sikkerhedstrusler og sårbarheder?
- [ ] Rapporteres virksomhedens sikkerhedsstatus løbende til virksomhedens direktion/bestyrelse?
- [ ] Omfatter arbejdet med sikkerhed både informationssikkerhed (ISO 27001) og cybersikkerhed? Læs mere på pwc.dk/iso27001
- [ ] Har I implementeret databeskyttelsesforordningen?
- [ ] Er der etableret en driftsorganisation for fortsat sikring af compliance med databeskyttelsesforordningen?

Processer

- [ ] Har I foretaget en måling af jeres robusthed mod cybertrusler (cyber assessment)?
- [ ] Har I dokumenteret og kommunikeret processer for alle områder af sikkerhed?

Adfærd

- [ ] Er der etableret et program for uddannelse og oplysning af medarbejderne om sikkerhed? Læs mere på www.pwc.dk/cyberaware

Validering

- [ ] Gennemfører I løbende test til identifikation af sårbarheder i jeres infrastruktur og systemer?
- [ ] Har I en defineret og afprøvet incident response-proces? Læs mere på www.pwc.dk/response
- [ ] Har I testet beredskabsplanen for cyberhændelser? Læs mere på pwc.dk/beredskab

Arkitektur

- [ ] Har I en plan for implementering af sikkerhedsteknologi?
- [ ] Har I en proces og plan for efterlevelse af privacy by design, herunder implementering af en sikkerhedsarkitektur? Læs mere på pwc.dk/pam og pwc.dk/iam

Kontakt

Vi vil meget gerne i dialog med dig om resultaterne fra årets Cybercrime Survey. Kontakt en af PwC's eksperter for en uforpligtende snak om dine konkrete udfordringer og behov. Du kan også læse mere om vores ydelser inden for cyber- og informationssikkerhed på www.pwc.dk/cyber

Om PwC

I PwC arbejder vi for at styrke tilliden i samfundet og være med til at løse væsentlige problemstillinger. Det gør vi med udgangspunkt i vores viden inden for revision, skat og rådgivning. Vores kunder kommer fra alle dele af erhvervslivet og den offentlige sektor, og vi er ca. 2.500 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi over 280.000 PwC'ere i 155 lande, og i Danmark er vi markedsledende. Mød os over hele landet. Vi er der, hvor du er.

Succes skaber vi sammen ...

PwC's eksperter inden for cyber- og informationssikkerhed

Mads Nørgaard Madsen
Partner
Security & Technology
2811 1592
mads.norgaard.madsen@pwc.com

Jørgen Sørensen
Partner
Security & Technology
2494 5254
jorgen.jgs.sorensen@pwc.com

Christian Kjær
Partner
Security & Technology
3945 3282
christian.kjaer@pwc.com

Cyber Incident Response-team

PwC hjælper kunder med at forebygge og håndtere cybersikkerhedshændelser.

Vi har etableret en central cyberhotline for kunder, så du har mulighed for at få akut hjælp. PwC's team af eksperter hjælper med at skabe overblik over indsatsområder i forhold til den konkrete trussel, og vores cyber-forensics-specialister identificerer angrebets art og de udnyttede sårbarheder. Derefter implementerer vi forbedringer af sikkerheden og udarbejder en rapport til brug for blandt andet ledelsen, forsikringen, Datatilsynet og politiet.

PwC's cyberhotline

70 222 444

Du kan også læse mere på www.pwc.dk/response

pwc

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...