Cybercrime Survey 2019

325 virksomhedsledere, it-chefer og specialister fra danske virksomheder har deltaget i PwC's Cybercrime Survey 2019, hvor de har delt deres syn på positive udviklinger samt udfordringer for cyberkriminalitet i Danmark. De har således taget stilling til udviklingen i trusselsbilledet og har rapporteret, hvordan og i hvilket omfang de arbejder med udfordringerne.

51%

angiver, at de har været udsat for én eller flere sikkerhedshændelser inden for det seneste regnskabsår.

76%

svarer, at topledelsen i nogen eller i høj grad har fokus på balancen mellem cyber-trusler og investeringer i cybersikkerhed.

50%

mener, at GDPR har været en byrde for forretningen.

pwc

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...

Indhold

Cybersikkerhed kræver et skift i fokus og holdninger

Teknologi forandrer konstant vores hverdag. Den teknologiske it-udvikling sker i forskellige sprints og har skabt store ændringer i vores samfund, siden man indførte den første edb-maskine i 1960 til enkelte centrale opgaver. Senere bevægede man sig mod en bredere teknisk it-anvendelse, og udbredelsen tog for alvor fart med personlige computere og mobile enheder. I dag lever vi i et samfund, hvor næsten al teknologi er forbundet over internettet.

Hver gang der sker et "teknologiskifte", er der også behov for et ændret fokus på sikkerhed. Således har sikkerhed udviklet sig fra at være fysisk sikkerhed, i form af fx en aflåst dør til mainframen i kælderen, til it-sikkerhed med fokus på driftssikkerhed og adskillelse af kritiske server-applikationer over til en udbredt anvendelse af pc'er og mobiler i det daglige arbejde. I dag skal vi håndtere cybersikkerhed af høj kompleksitet, og risikoen for cybertrusler er større end nogensinde før.[1] De gamle sikkerhedsprincipper er derfor ikke længere tilstrækkelige.

Øget fokus fra topledelsen

PwC's Cybercrime Survey har de seneste fem år vist en udvikling inden for sikkerhedsområdet, der er blevet påvirket gennem øgede krav fra bl.a. GDPR, men også af alvorlige cybersikkerhedshændelser, der har fået store konsekvenser for danske og udenlandske virksomheder. Undersøgelsen viser i år, at 51 % har været ramt af en sikkerhedshændelse. Det er en stigning på 7 %-point siden sidste år (44 % i 2018). Forøgelsen i antallet af sikkerhedshændelser kan være medvirkende til, at topledelsen har fået et større fokus på cybersikkerhed. 76 % af respondenterne angiver således i 2019, at topledelsen i nogen eller i høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed. Undersøgelsen viser også, at det særligt er ledelsen, der bekymrer sig om cybertruslen, hvilket kan være med til at forklare, at der i dag investeres mere i cybersikkerhed. Undersøgelsen viser også, at de større virksomheder har et gennemsnitligt cybersikkerhedsbudget på 19 mio. kr., mens de mindre virksomheders tilsvarende budget er 700.000 kr.

Fra styring og compliance til forebyggelse og opdagelse

Men selvom topledelsen har fået et større fokus på cybersikkerhed, kan flere virksomheder med fordel sætte øget fokus på netop de forbedringstiltag, der reelt øger cybersikkerheden. Det er tiltag, der på længere sigt skaber styring og lever op til mange compliance-krav, samt giver et godt grundlag for en stabil sikkerhed. Udfordringen er dog, at virksomhederne er sårbare nu. Derfor er det vores anbefaling, at virksomhederne skal rette fokus mod de sikkerhedstiltag, der mindsker risikoen for cyberangreb på kort sigt. Det betyder, at der skal være skærpet fokus på implementering af tekniske sikkerhedsløsninger, der forebygger og opdager sikkerhedshændelser. Et fokus som også kommer til udtryk i den nationale strategi for cyber- og informationssikkerhed, hvor der lægges vægt på sikkerhedstiltag af mere teknisk karakter.

Fra "need to know" til "need to protect"

Cybersikkerhedens kompleksitet og natur kræver også et opgør med de gamle sikkerhedsprincipper. Mange virksomheder tillader i dag både kunder og leverandører adgang til deres systemer og fortrolige data. Det er derfor ikke tilstrækkeligt blot at fokusere på funktionsadskillelse og "need-to-know"; der er behov for fokus på "need-to-protect", hvilket kræver en større involvering af forretningen og ledelsen. Og her ligger et centralt holdningsskifte. Det kræver nye kompetencer hos sikkerhedsfolkene, der skal kunne oversætte de ofte meget tekniske og komplekse sikkerhedsmæssige udfordringer til et risikobillede, der kan anvendes som beslutningsgrundlag for forretningen og ledelsen. Lige nu er holdningsskiftet nødvendigt for at sikre den langsigtede investering i beskyttelse mod cybertruslerne ud fra en risikovurdering, der fokuserer på beskyttelse af virksomhedens absolut mest kritiske aktiver. Det er derfor tid til en mere forretningsfokuseret tilgang til sikkerhed, hvor fokus er på reel cybersikkerhed med forretnings- og ledelsesinvolvering.

Stor tak til de flere end 300 erhvervsledere og fagfolk, der har svaret på PwC's Cybercrime Survey 2019, og til undersøgelsens samarbejdspartnere, der har været med til at bakke op om tiltaget.

Mads Nørgaard Madsen
Partner
Security & Technology

[1] Trusselsvurderingsenheden ved Center for Cybersikkerhed, marts 2019. Cybertruslen mod Danmark.

PAVA – et forståeligt sikkerhedskoncept

Dette års undersøgelsesresultat 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.

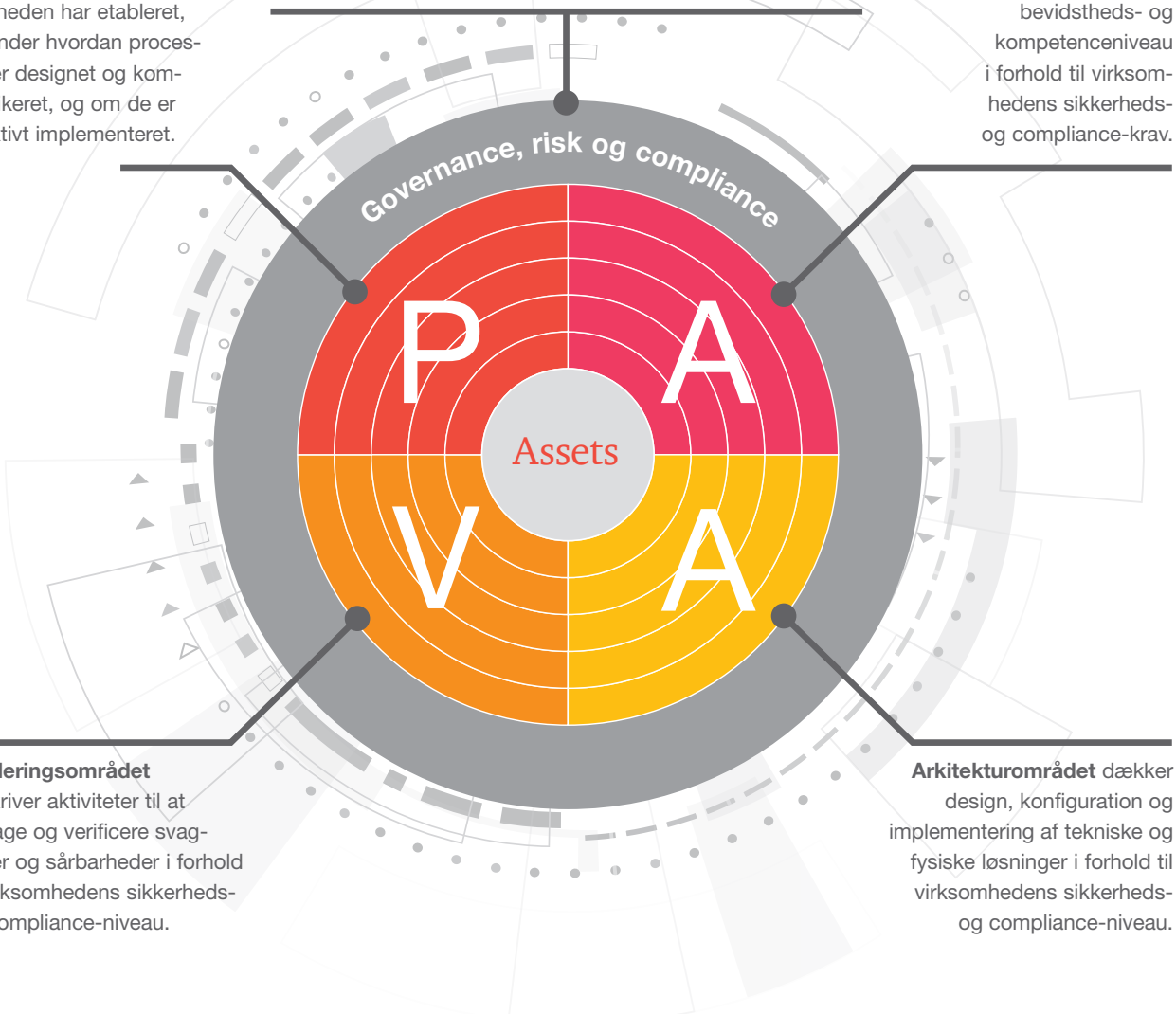
På den måde giver PAVA et fælles grundlag for konkrete og prioriterede løsninger inden for specifikke sikkerhedsområder i virksomheden til brug i en bredere kontekst og til løbende effektmåling.

PAVA dækker over fem hovedområder fra governance, risk og compliance til proces, adfærd, validering og arkitektur. Der er behov for en indsats inden for alle områder, afhængig af den enkelte virksomheds modenheds- og sikkerhedsniveau, 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, 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.



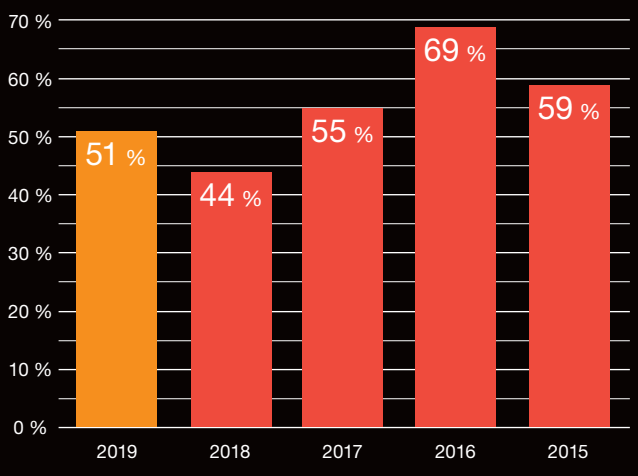
Valideringsområdet beskriver aktiviteter til at opdage og verificere svagheder og sårbarheder i forhold til virksomhedens sikkerheds- og compliance-niveau.

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

Hver anden virksomhed har været udsat for en sikkerhedshændelse

For femte år i træk undersøger PwC's Cybercrime Survey niveauet for cyber- og informationssikkerhed i erhvervslivet. PwC's Cybercrime Survey 2019 viser, at der er sket en stigning i antallet af respondenter, der angiver, at de har været udsat for en sikkerhedshændelse. 51 % af respondenterne angiver i 2019, at de har været udsat for én eller flere sikkerhedshændelser, hvilket er en stigning på 7 %-point siden 2018 (fra 44 % i 2018 til 51 % i 2019).

Femårig udvikling over andel respondenter, der har været udsat for minimum én sikkerhedshændelse[2]



[2] Respondenterne har besvaret følgende spørgsmål: Hvor mange gange har din virksomhed været udsat for en sikkerhedshændelse inden for det seneste regnskabsår?

Investeringer topper i større virksomheder

Større virksomheder

>200
medarbejdere

Gennemsnitligt aktuelt cyber-/informationssikkerhedsbudget

19 mio. kr.

Mindre virksomheder

<199
medarbejdere

Gennemsnitligt aktuelt cyber-/informationssikkerhedsbudget

700.000 kr.

Større virksomheder >200 medarbejdere

Det stigende antal hændelser kan være med til at forklare virksomhedernes budgetniveau. Undersøgelsen viser, at de respondenter, der kommer fra større virksomheder, har et gennemsnitligt aktuelt budget på 19 mio. kr.[3] Samtidig kan det ses, at de større virksomheder planlægger højere budgetter i år 2020 med et forventeligt gennemsnitligt budget på 20,5 mio. kr.

Det er ikke uden grund, at der især i de større virksomheder bliver investeret mange penge i cyber- og informationssikkerhed. 61 % af respondenterne fra de større virksomheder svarer nemlig, at de har været udsat for mindst én sikkerhedshændelse, mens tallet er 33 % i de mindre virksomheder. Tilsvarende er det også de større virksomheder, der bliver udsat for flest målrettede sikkerhedshændelser. Her svarer 45 %, at de har været udsat for én eller flere målrettede sikkerhedshændelser, mens tallet er 29 % for de mindre virksomheder.

Mindre virksomheder <199 medarbejdere

Til sammenligning har man i de mindre virksomheder et gennemsnitligt aktuelt budget på 700.000 kr.[3] og et forventeligt budget på 550.000 kr. i år 2020. I modsætning til de større virksomheder planlægger de mindre virksomheder dermed mindre budgetter inden for det næste år.

Derudover svarer 33 % i de mindre virksomheder, at de har været udsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår, mens 29 % angiver, at de har oplevet én eller flere sikkerhedshændelser, der var målrettet deres virksomhed.

"Det er PwC's erfaring, at stigningen i antallet af sikkerhedshændelser og de skærpede regler til cybersikkerhed samt GDPR har gjort ledelsen mere opmærksom på cyber- og informationssikkerhedsrisici, hvilket kan have ført til de dedikerede budgetter."

[3] De anførte beløb er afrundet og korrigeret for outliers. Beløbene er beregnet ud fra de respondenter, der har angivet, at de har et cyber-/informationssikkerhedsbudget.

Størst tillid til den finansielle sektors GDPR-compliance

En af de væsentligste forudsætninger for at opnå succes med digitalisering i såvel virksomheder som samfundet er, at kunder og borgere har tillid til, at deres data behandles sikkert og fortroligt. Dette er også den primære baggrund for databeskyttelsesforordningen (GDPR) og en af de grundlæggende målsætninger med den danske nationale cyberstrategi. Derfor har vi igen i år spurgt ind til respondenternes tillidsniveau til de forskellige sektorer i forhold til cybersikkerhed og GDPR-compliance.

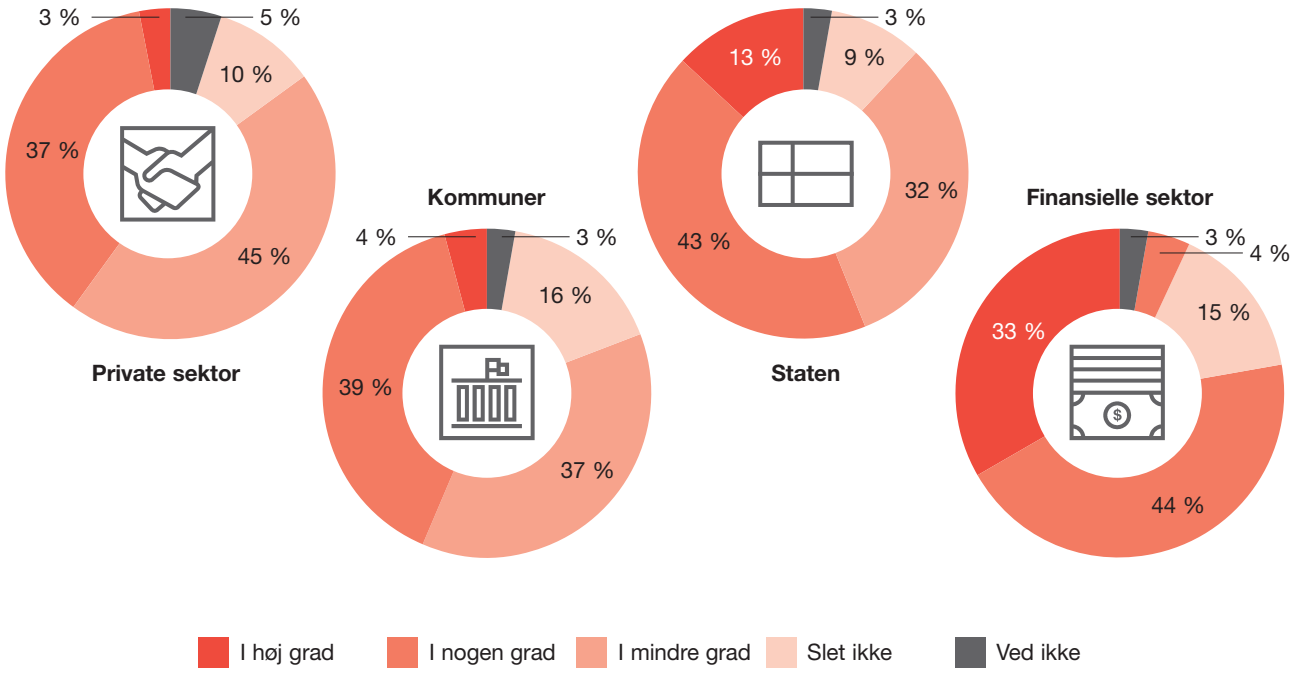
Ser man på tilliden til GDPR-compliance, så ligger den finansielle sektor ligesom sidste år øverst. 77 % svarer således i år, at de i nogen eller høj grad har tillid til compliance-niveauet i den finansielle sektor, mens 19 % udtrykker en mindre grad af tillid. I 2018 var tilliden til GDPR-compliance lavest i kommunerne, da 68 % angav, at de i mindre grad eller slet ikke havde tillid til GDPR-compliance i denne sektor. I år ses en positiv udvikling for kommunerne, da 43 % nu udtrykker nogen eller en høj grad af tillid mod blot 32 % i 2018. 53 % svarer, at de har mindre eller slet ingen tillid GDPR-compliance i kommunerne, altså en forbedring på 15 %-point.

I 2019 er tilliden til GDPR-compliance lavest i den private sektor, idet 55 % angiver, at de i mindre grad eller slet ikke har tillid til GDPR-compliance i den private sektor, og blot 3 % udtrykker en høj grad af tillid. Tilliden til GDPR-compliance i den private sektor er dog ikke blevet betydeligt lavere sammenlignet med sidste år (58 % i 2018); det er den forøgede tillid til GDPR-compliance i kommunerne, der har medført, at tillidsbilledet i år har ændret sig.

Også i forhold til cybersikkerhed skiller den finansielle sektor sig positivt ud i 2019, da 40 % svarer, at de har en høj grad af tillid til cybersikkerheden i den finansielle sektor. Kun 13 % angiver, at de i mindre grad eller slet ikke har tillid til cybersikkerheden i denne sektor.

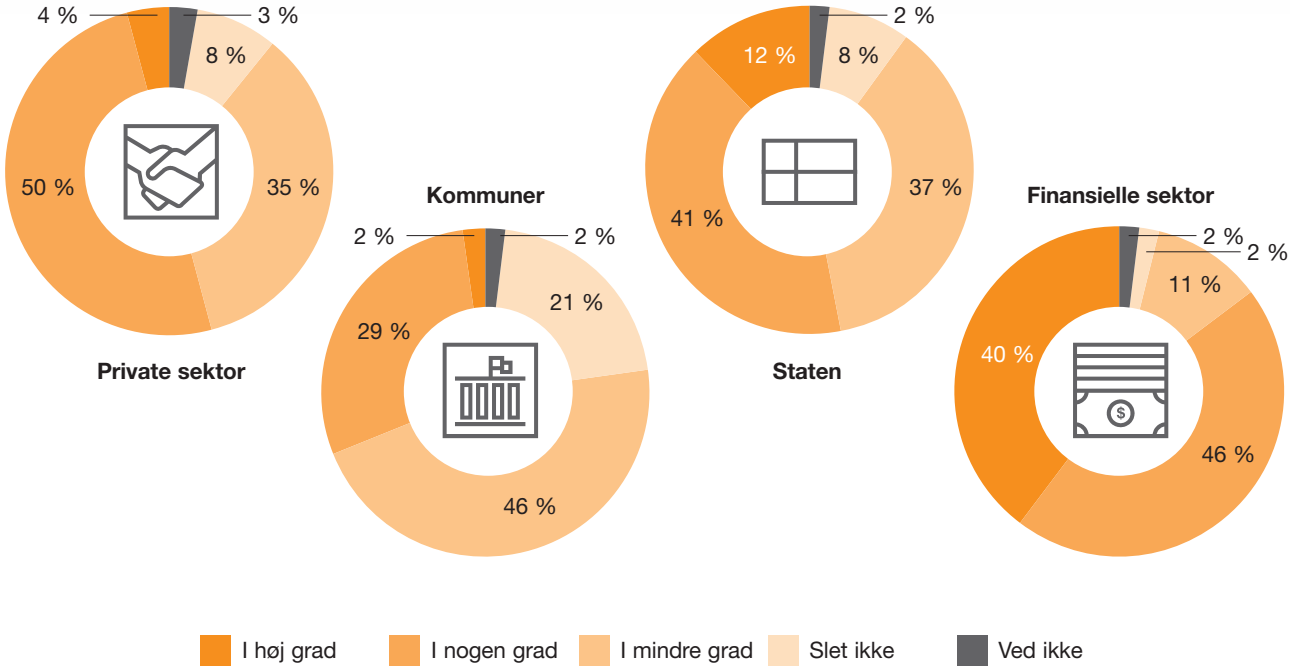
Anderledes ser det ud for kommunerne, idet 67 % tilkendegiver, at de i mindre grad eller slet ikke har tillid til cybersikkerheden i denne sektor. Dette tal var 70 % i 2018. På trods af at tallet i år er forbedret med 3 %-point, viser undersøgelsen, at tilliden til kommunernes cybersikkerhed fortsat er lavest.

I hvor høj grad har du tillid til GDPR-complianceniveauet i 2019 i ...



"Det er positivt at se udviklingen i tilliden til GDPR-implementeringen og særligt den øgede tillid til GDPR-compliance i kommunerne. Det er dog PwC's erfaring, at selvom der er skabt et compliance-grundlag i form af dokumentation, så mangler mange virksomheder og organisationer stadig at få indarbejdet GDPR i det daglige arbejde for på længere sigt at kunne fastholde et compliance-niveau. Der er derfor behov for at få implementeret tiltag, der fungerer i praksis – og ikke bare er skrevet juridisk korrekt."

I hvor høj grad har du tillid til cybersikkerheden i 2019 i ...



Topledelsen har fået større fokus på cybertruslen

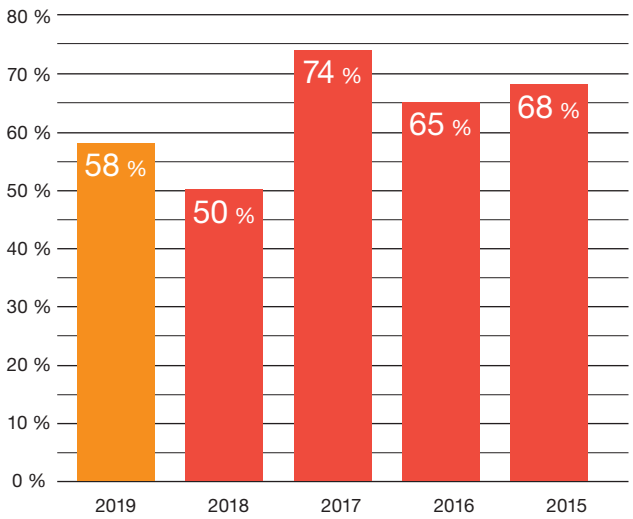
PwC's Cybercrime Survey 2019 viser en stigning i antallet af respondenter, der angiver, at topledelsen i nogen eller i høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed. Udviklingen er undersøgt på tværs af sektorer, og der ses en tendens til, at det særligt er i den private sektor, at topledelsen har fokus på cybertruslen.

I 2018 angav 66 % af respondenterne, at topledelsen i nogen eller i høj grad havde fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed. I 2019 er tallet steget til 76 %. Respondenternes bekymring om cybertrusler i virksomheden er dog fortsat høj og er steget siden sidste år. 58 % af respondenterne angiver, at de bekymrer sig mere om cybertruslen i dag, end de gjorde for 12 måneder siden (50 % i 2018).

Ser vi på undersøgelsens resultater fordelt mellem ledelse og fagfolk, ses der en tendens til, at det særligt er ledelsen, der bekymrer sig mere om cybertruslen. Blandt CxO'er[4] svarer 65 %, at de bekymrer sig mere om cybertruslen i dag end for 12 måneder siden. Blandt fagfolk[5] er tallet lavere, idet 49 % her svarer, at de er mere bekymrede i dag. At det især er ledelsen, der bekymrer sig mere om cybertruslen, kan hænge sammen med, at ledelsens fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed er steget, og kan samtidig være med til at forklare de dedikerede budgetter.

Bekymrer du dig mere om de cybertrusler, din virksomhed oplever i dag, end du gjorde for 12 måneder siden?

Respondenter, der svarer ja:



Cyber Arena

Et interaktivt simuleringsværktøj til træning af beredskabs- og incident-teams i håndteringen af realistiske cyberhændelser. Læs mere på www.pwc.dk/cyberarena

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, samt vigtigheden i at investere i cyber- og informationssikkerhed. Læs mere på www.pwc.dk/cyberaware

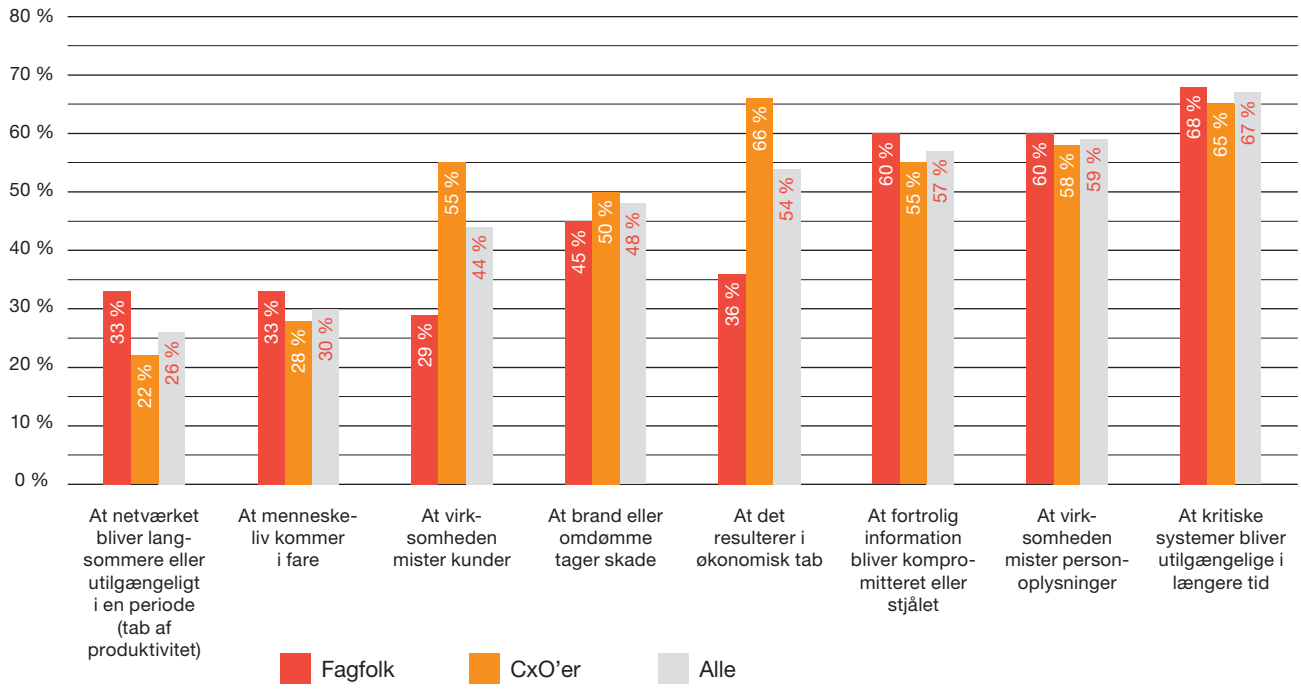
[4] Inkluderer stillingsbetegnelserne CEO, CFO, CIO, CCO, CTO, CISO mv.
[5] Inkluderer stillingsbetegnelserne sikkerhedsmedarbejdere, sikkerhedsspecialister og øvrige medarbejdere.

Ser man nærmere på henholdsvis CxO'ernes og fagfolkenes bekymringer i relation til konsekvensen af en cyberhændelse, bekymrer de to grupper sig nogenlunde lige meget om, at kritiske systemer bliver utilgængelige i længere tid (CxO 65 % og fagfolk 68 %), at virksomheden mister personoplysninger (CxO 58 % og fagfolk 60 %), og at fortrolig information bliver kompromitteret eller stjålet (CxO 55 % og fagfolk 60 %).

Den største forskel mellem de to grupper ses dog ved, at særligt CxO'erne bekymrer sig om cyberhændelser, der resulterer i økonomisk tab (CxO 66 % og fagfolk 36 %), og cyberhændelser, der resulterer i, at virksomheden mister kunder (CxO 55 % og fagfolk 29 %).

"Undersøgelsen understreger det grundlæggende behov, der er for afstemning af holdning og fokus mellem ledelsen og fagfolk. Det er nødvendigt, at ledelsen involveres i cybersikkerheden, da cybertrusler i dag kan få stor indvirkning på forretningen. Ledelsen har behov for at få kommunikeret problemerne på en forretningsforståelig og anvendelig måde. Fagfolkene har ligeledes brug for en klar retning og prioritering af de cybertiltag, som ledelsen vil finansiere for at imødegå de cyberrisici, som ledelsen prioriterer højest. Vi anbefaler derfor, at der udarbejdes en samlet cyberrisikovurdering som grundlag for fastlæggelse af en god kommunikationsform samt afstemte formater for rapportering og beslutningsoplæg."

Hvad er din virksomheds største bekymring i relation til konsekvensen af en cyberhændelse?

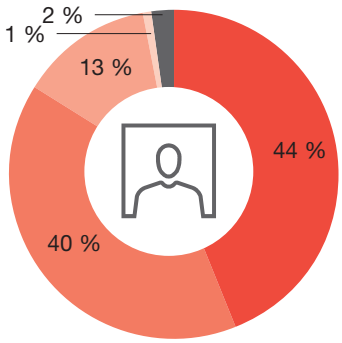


Der arbejdes målrettet med den nationale strategi for cyber- og informationssikkerhed

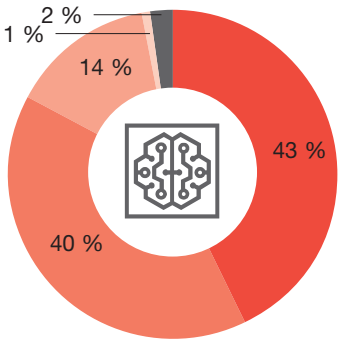
I starten af 2019 lancerede staten Danmarks nationale strategi for cyber- og informationssikkerhed.[6] Strategien har til formål at styrke cyber- og informationssikkerheden i de samfundskritiske sektorer – nemlig tele-, finans-, sundheds-, transport- og søfartssektoren. PwC's Cybercrime Survey 2019 viser, at knap halvdelen af undersøgelsens respondenter (47 %) er omfattet af strategien. Undersøgelsen viser også, at de respondenter, der angiver, at de er omfattet af strategien, generelt giver udtryk for, at der i virksomheden arbejdes målrettet med strategiens hovedområder.

Således angiver 84 %, at der i virksomheden i nogen eller i høj grad er klarhed over roller og ansvar på området for cyber- og informationssikkerhed. Tilsvarende svarer 83 % af respondenterne, at de i virksomheden i nogen eller i høj grad har adgang til den nødvendige viden for at håndtere de stigende udfordringer med cyber- og informationssikkerhed. Hele 93 % angiver desuden, at virksomhedens kritiske funktioner i nogen eller i høj grad er beskyttet mod cyberangreb eller andre større informationssikkerhedshændelser.

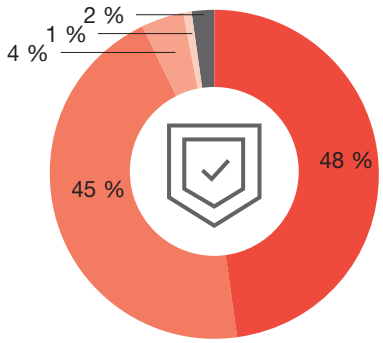
Hvor langt er din virksomhed kommet med nedenstående tre hovedområder i den nationale cyberstrategi?



I hvilken grad er der i virksomheden klarhed over roller og ansvar på cyber- og informationssikkerhedsområder?[7]



I hvilken grad har I adgang til den nødvendige viden for at håndtere de stigende cyber- og informationssikkerhedsudfordringer?[7]



I hvilken grad er virksomhedens kritiske funktioner beskyttet mod cyberangreb eller andre større informationssikkerhedshændelser?[7]

I høj grad | I nogen grad | I mindre grad | Slet ikke | Ved ikke

[6] Regeringen fremlagde i 2018 en ny strategi for cyber- og informationssikkerhed, der med 25 initiativer samt seks målrettede strategier for de mest samfundskritiske sektorer skal bidrage til at løfte det nationale niveau for cyber- og informationssikkerhed.
[7] På baggrund af strategiens 25 hovedinitiativer har vi udarbejdet tre hovedemner, der rammer initiativerne.

Læs strategien

Download via Finansministeriets hjemmeside www.fm.dk

At virksomhederne arbejder målrettet med strategien, afspejles også i respondenternes tilkendegivelser af, hvordan strategien har påvirket virksomheden. 46 % angiver, at de er blevet mere oplyste om mulige trusler, 38 % angiver, at strategien har styrket samarbejdet i sektoren, og 37 % har svaret, at strategien har resulteret i, at man har opnået et øget sikkerhedsniveau i virksomheden. Således afspejler svarene en positiv tendens, der viser, at virksomhederne har taget strategien alvorligt og har haft fordel af den målrettede indsats.

Hvordan har den nationale cyberstrategi påvirket din virksomhed?

46 % Vi er blevet mere oplyste om mulige trusler.

38 % Den har styrket vores samarbejde i sektoren.

37 % Den har resulteret i, at vi har øget sikkerhedsniveauet i vores virksomhed.

26 % Den har resulteret i nye teknologiinvesteringer.

23 % Den har ikke påvirket os på nogen måder.

18 % Den har resulteret i nye ansættelser.

"Svarene afspejler en positiv tendens, der viser, at virksomhederne har taget strategien alvorligt og har draget fordel af den målrettede indsats."

Hver anden ser GDPR som en byrde

Databeskyttelsesforordningen (GDPR) fik virkning den 25. maj 2018, og vi kan i 2019 se en tendens til, at virksomhederne for alvor er blevet opmærksomme på, at det er ressourcekrævende at efterleve de komplekse regler i forordningen.

PwC's Cybercrime Survey 2019 viser, at der er sket et fald på 7 %-point i antallet af respondenter, der angiver, at virksomhedens personoplysninger i høj grad er tilstrækkeligt beskyttet i henhold til GDPR (fra 49 % i 2018 til 42 % i 2019). Samtidig viser undersøgelsen en stigning på 10 %-point i antallet af respondenter, der angiver, at virksomhedens personoplysninger i nogen eller i mindre grad er tilstrækkeligt beskyttet i henhold til GDPR (fra 46 % i 2018 til 56 % i 2019).

Det kan indikere, at virksomhederne er blevet mere opmærksomme på deres egne muligheder for at beskytte personoplysninger tilstrækkeligt. I forlængelse heraf viser analysen, at 50 % af respondenterne mener, at GDPR har været en byrde for forretningen. Til sammenligning var dette tal 33 % i 2018, og der er således tale om et større spring på hele 17 %-point. Tilsvarende viser undersøgelsen, at flere respondenter angiver, at GDPR har krævet store omlægninger af forretningen (fra 9 % i 2018 til 17 % i 2019), nye ansættelser (fra 29 % i 2018 til 36 % i 2019) og nye teknologiinvesteringer (fra 35 % i 2018 til 40 % i 2019).

42 %

angiver, at deres data i **høj grad er beskyttet** i henhold til GDPR

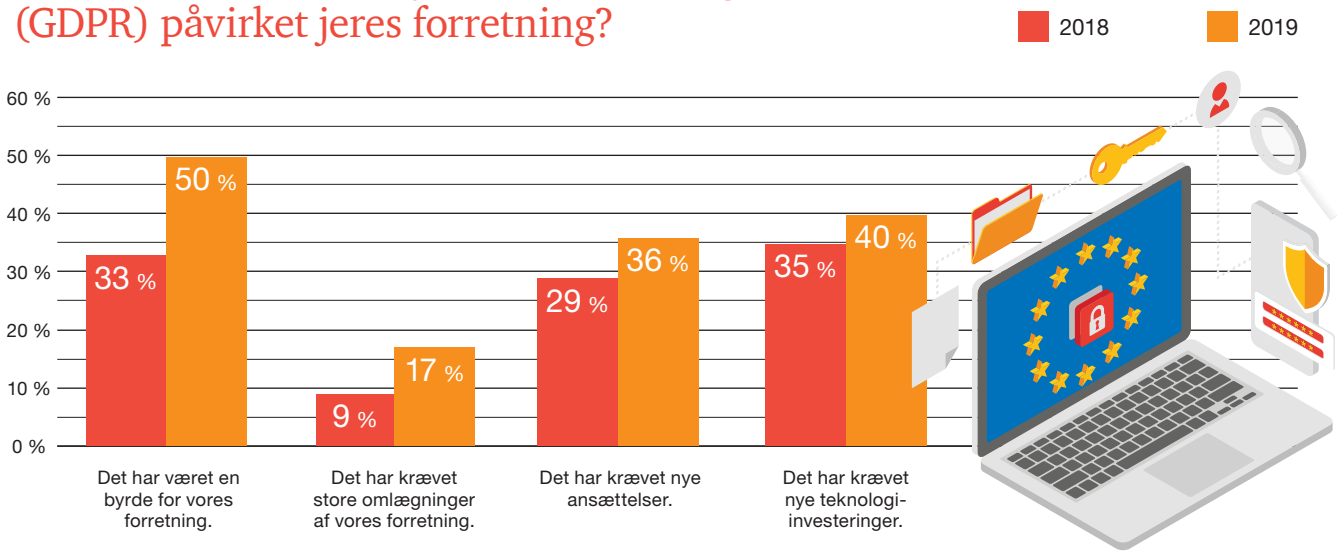
56 %

angiver, at deres data **i nogen eller i mindre grad er beskyttet** i henhold til GDPR

"De fleste virksomheder har efterhånden gennemført et GDPR-projekt i et eller andet omfang. For mange virksomheder omfattede projektet en kortlægning af virksomhedens processer, indeholdende personoplysninger, udarbejdelse af de lovpligtige dokumenter samt undervisning. Vores erfaring viser desværre, at mange virksomheders GDPR-projekt er stoppet her."

"GDPR er ikke en engangsøvelse eller et juridisk papirskjold. Det kan bedre betale sig at holde fokus på GDPR løbende, så man undgår større oprydningsprojekter, som tager tid. PwC anbefaler, at virksomhederne får indarbejdet kravene i det daglige arbejde. Implementering af GDPR skal ske såvel i de faktiske og organisatoriske processer i forretningen som i de it-systemer, hvori personoplysninger behandles."

Hvordan har databeskyttelsesforordningen (GDPR) påvirket jeres forretning?

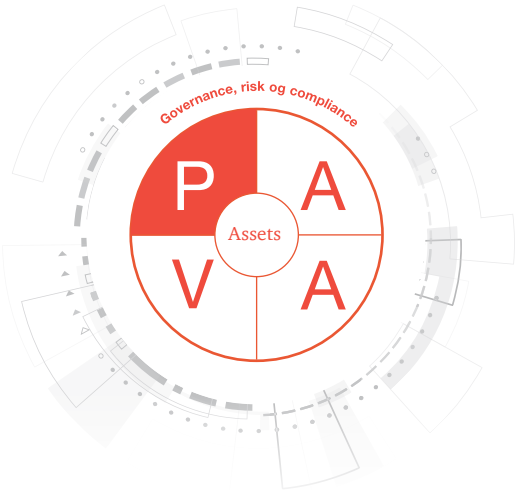


At virksomhederne er blevet mere opmærksomme på forordningen og på deres egne evner til at beskytte personoplysninger tilstrækkeligt, kan hænge sammen med, at flere har angivet, at de har oplevet en hændelse, hvor fortrolige og følsomme personoplysninger eller anden fortrolig information utilsigtet er blevet delt. Således angiver 29 % i 2019, mod 17 % i 2018, at de har oplevet en hændelse, hvor fortrolige og følsomme personoplysninger eller anden fortrolig information utilsigtet er blevet delt. Ligeledes angiver 59 %, at de er bekymrede for, at virksomheden mister personoplysninger som en konsekvens af en sikkerhedshændelse.

Ifølge Datatilsynet har der i perioden 25. maj til 31. december 2018 været 2.780 sikkerhedsbrud der vedrører personoplysninger.[8] Til sammenligning har Datatilsynet i perioden 1. januar til 30. juni 2019 modtaget 3.261 anmeldelser af brud på persondatasikkerheden.[9] At flere respondenter i år har angivet, at de har oplevet en hændelse, hvor fortrolige og følsomme personoplysninger eller anden fortrolig information utilsigtet er blevet delt, kan derfor hænge sammen med, at virksomhederne er blevet mere opmærksomme på at rapportere hændelser til Datatilsynet. Mediernes øgede fokus på hændelser kan ligeledes være med til at forklare respondenternes store bekymring for at miste personoplysninger som konsekvens af en sikkerhedshændelse.

[8] Datatilsynet, 2018. Anmeldelser af brud på persondatasikkerheden.
[9] Datatilsynet, 2019. Anmeldelser af brud på persondatasikkerheden i første kvartal 2019.
Datatilsynet, 2019. Anmeldelser af brud på persondatasikkerheden – Andet kvartal 2019.

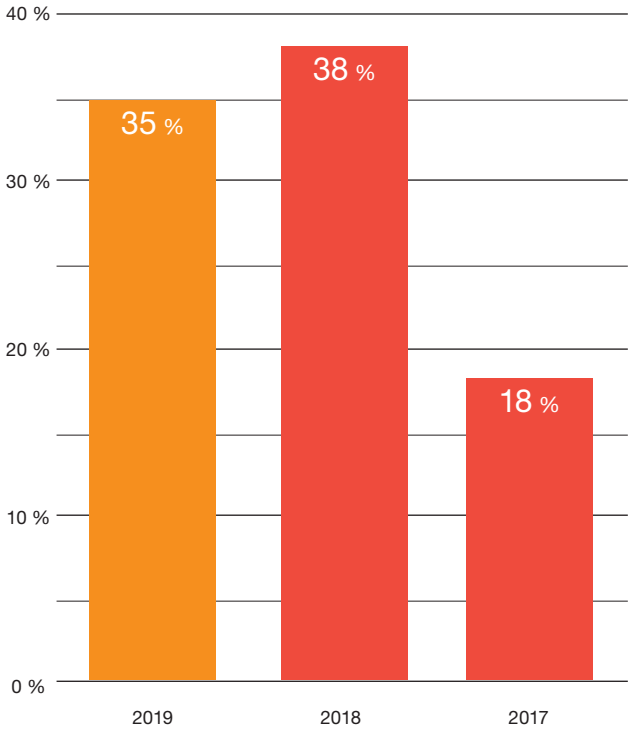
Metodeforankring er stadig en prioritet



Både offentlige organisationer og private virksomheder har i mange år arbejdet på at implementere cyber- og informationssikkerhedsmetoder og -standarder, primært ISO 27001. Et behov, som også er blevet nødvendigt i relation til GDPR.

Undersøgelsen viser, at metodeforankring fortsat i 2019 er højt prioriteret blandt virksomhedernes investeringer inden for cyber- og informationssikkerhed. Med 35 % af undersøgelsens respondenter, der angiver, at metodeforankring er blandt virksomhedens højst prioriterede investeringer, befinder metodeforankring sig således i top-3 over virksomhedernes største investeringer.[10]

Andel, der har angivet, at metodeforankring er virksomhedens højst prioriterede investering inden for cyber- og informationssikkerhed i de næste 12 måneder



[10] For at se hele grafen over virksomhedernes højest prioriterede investeringer, henvises til side 22.

"Selvom offentlige organisationer og private virksomheder i mange år har arbejdet på at implementere cyber- og informationssikkerheds-metoder og -standarder, der er forstærket af GDPR-kravene, har det ikke nødvendigvis forbedret den reelle sikkerhed. Stigningen i antallet af sikkerhedshændelser viser, at virksomheder bør ændre fokus fra compliance-orienteret sikkerhed over imod mere tekniske sikkerhedstiltag og løsninger, der gør virksomhederne i stand til at forebygge og opdage sikkerhedshændelser hurtigere. Det kan være NIST-cybersikkerheds-frameworket, som er blevet anvendt i forbindelse med den nationale strategi for cyber- og informationssikkerhed, hvor der er fokus på at forudse, forebygge, opdatere, håndtere og reetablere."

Over halvdelen af virksomhederne tester deres medarbejdere gennem awareness-træning

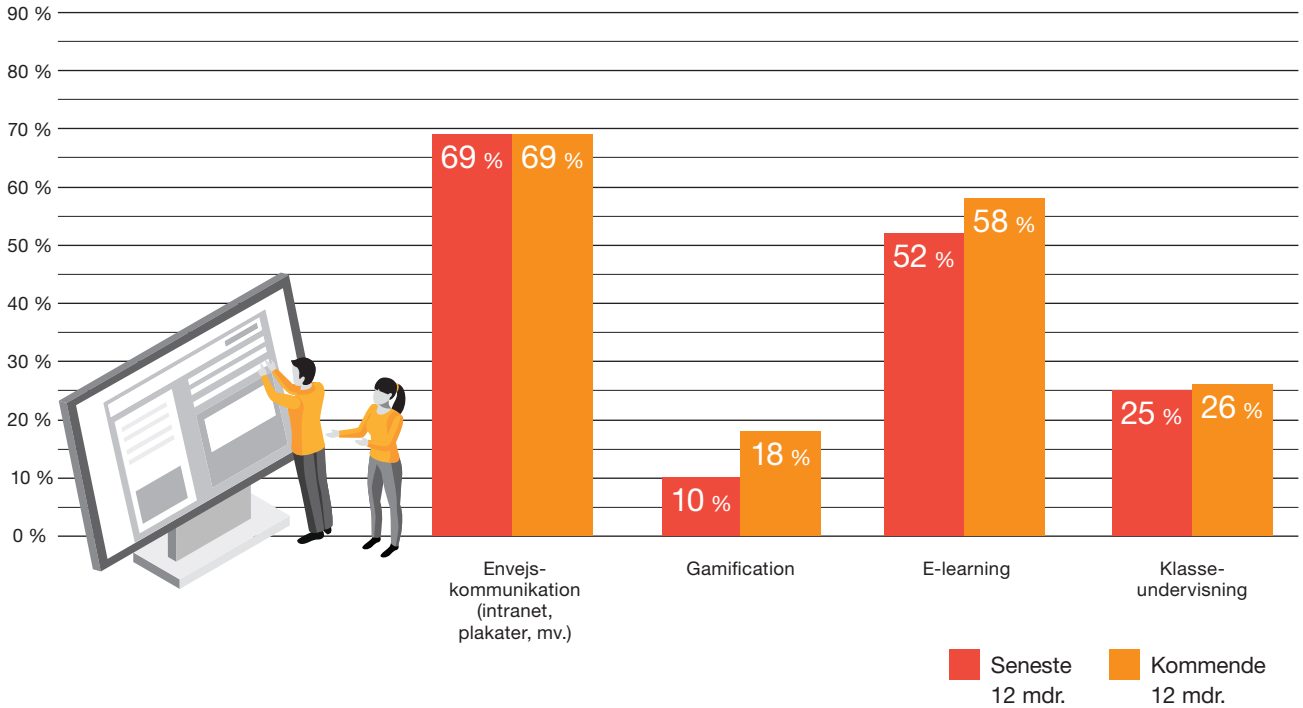
I takt med at trusselsbilledet ændrer sig, stiger også behovet for awareness-træning inden for cyber- og informationssikkerhed. Vi kan se en positiv tendens til, at mange virksomheder supplerer envejskommunikation med e-learning, og at langt de færreste gør brug af envejskommunikation som det eneste awareness-tiltag.

PwC's Cybercrime Survey 2019 viser, at flest respondenter angiver, at de gør brug af envejskommunikation i form af fx intranetnyheder og plakater i forbindelse med awareness-træning.

Således angiver 69 % af respondenterne, at de i de seneste 12 måneder har gjort brug af envejskommunikation. Herefter angiver 52 % af respondenterne, at de i de seneste 12 måneder har gjort brug af e-learning.

Selvom størstedelen tilkendegiver, at de gør brug af envejskommunikation, kan vi samtidig se, at 45 % af respondenterne angiver, at de i virksomheden gør brug af både envejskommunikation og e-learning. Ydermere er det kun 7 %, der angiver, at de i virksomheden kun har gjort brug af envejskommunikation i de seneste 12 måneder.

Hvilke af følgende tiltag gør din virksomhed brug af i forbindelse med awareness inden for GDPR samt cyber- og informationssikkerhed?



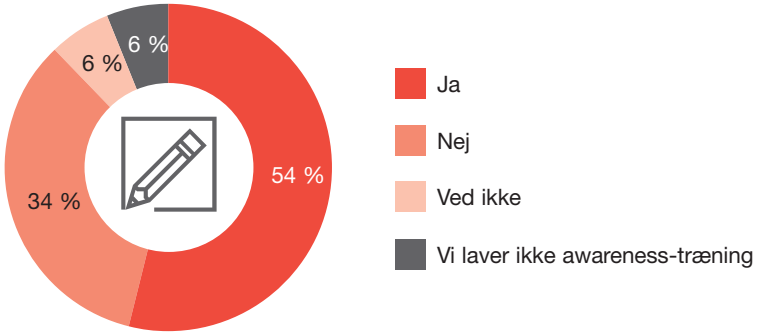
"Der har nu i en årrække været forståelse af og fokus på at teste medarbejdernes generelle awareness over for sikkerhedstrusler. Vi anbefaler, at virksomheder fortsætter med at træne og uddanne deres medarbejdere, så de kan være medvirkende til at forebygge og opdage cyberkriminalitet."

Læs mere på www.pwc.dk/cyberaware

Ser man nærmere på virksomhedernes planlagte awareness-tiltag i de kommende 12 måneder, tegner der sig et billede af, at flere virksomheder ønsker at investere i e-learning og gamification. 18 % af respondenterne svarer, at de forventer at gøre brug af gamification i de kommende 12 måneder, og 58 % af respondenterne angiver, at de forventer at gøre brug af e-learning i de kommende 12 måneder.

Undersøgelsen viser også, at 54 % af respondenterne angiver, at medarbejderne i virksomheden testes i læringsmateriale. Samtidig kan vi se, at 78 % af de respondenter, der angiver, at medarbejderne testes, også angiver, at de har gjort brug af e-learning inden for de seneste 12 måneder. Undersøgelsen viser desuden en tendens til, at det hovedsageligt er de større virksomheder, der tester deres medarbejdere. Således svarer 58 % af respondenterne fra de større virksomheder, at medarbejderne testes i læringsmaterialet, mens tallet er lavere i de mindre virksomheder, hvor 48 % svarer, at medarbejderne testes.

Testes medarbejderne i læringsmaterialet (forekommer der dokumentation)?

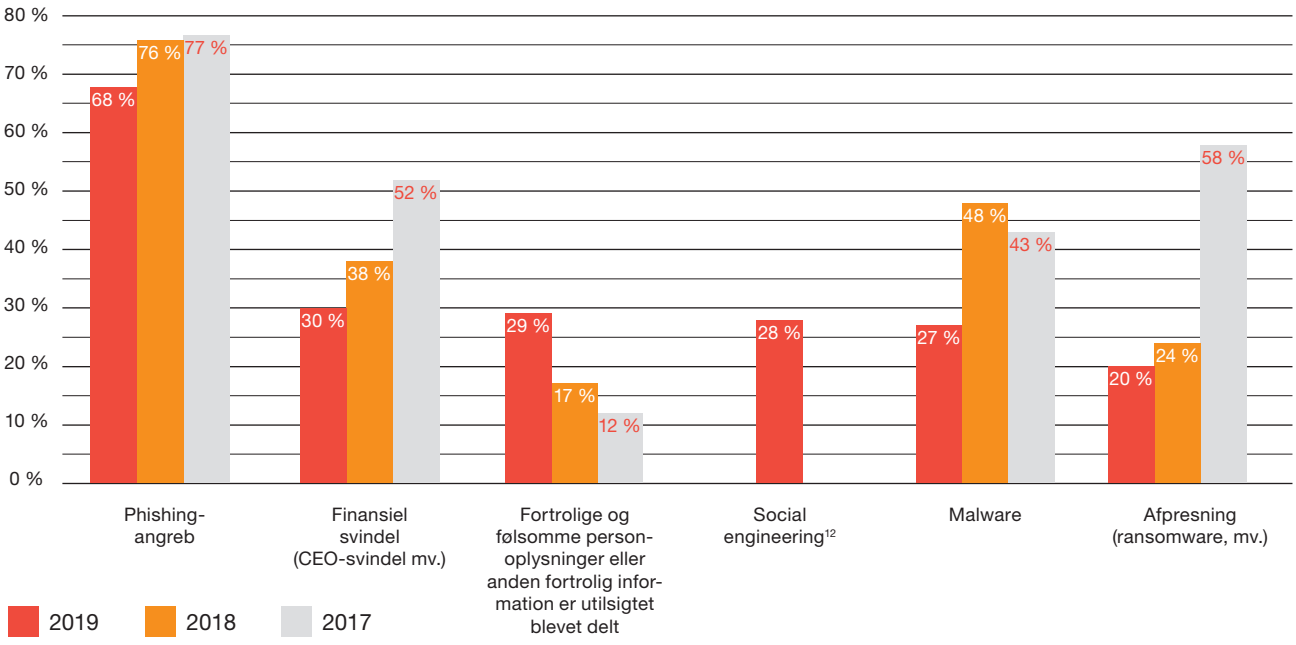


Ansattes ubevidste handlinger udgør den største cybertrussel

Cybertruslen er under konstant forandring. PwC's Cybercrime Survey 2019 viser, at phishing-angreb stadig er den hyppigst oplevede angrebstype, da hele 68 % angiver, at virksomheden har oplevet et phishing-angreb inden for de seneste 12 måneder. Andelen der peger på phishing-angreb, er dog faldet siden sidste år (fra 76 % i 2018 til 68 % i 2019), og samme tendens gælder for finansiel svindel (fra 38 % i 2018 til 30 % i 2019).

Faldet i disse angrebstyper kan hænge sammen med, at hele 57 % i 2019 angiver, at awareness-træning er blandt virksomhedens højst prioriterede investeringer inden for cyber- og informationssikkerhed. Som tidligere nævnt viser undersøgelsen ligeledes, at 17 % i 2018 mod 29 % i 2019 har oplevet en hændelse, hvor fortrolige og følsomme personoplysninger eller anden fortrolig information er blevet delt utilsigtet. På listen over hændelsestyper ser vi i år også en ny trussel i form af social engineering[11] (28 %), efterfulgt af malware (27 %) og afpresning (20 %).

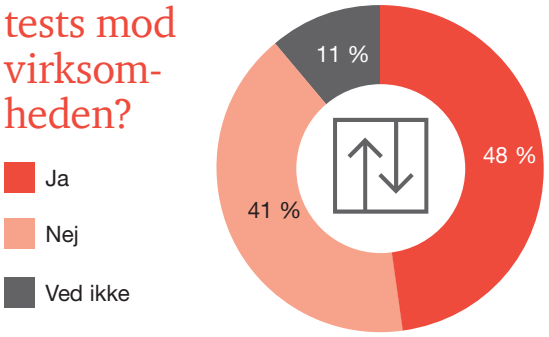
Hvilke hændelser har I i din virksomhed oplevet i de seneste 12 måneder som resultat af cyberkriminalitet eller informationssikkerhedshændelser?



På spørgsmålet om, hvorvidt der udføres tests mod virksomheden i form af fx phishing-tests, svarer 48 % af respondenterne ja, mens 41 % svarer nej. Undersøgelsen viser en forskel mellem mindre og større virksomheder, når det kommer til at udføre tests mod virksomheden. I de større virksomheder svarer 50 % ja til, at der udføres tests mod deres virksomhed, mens tallet er 43 % i de mindre virksomheder. I de mindre virksomheder svarer 16 % desuden, at de ikke ved, om der udføres tests, hvilket er ca. dobbelt så mange som i de større virksomheder.

[11] Ved social engineering anvender angriberen psykologiske greb til at opnå offerets tillid, så offeret kan manipuleres til at udføre bestemte handlinger.
[12] Social engineering er en svarmulighed tilføjet i 2019, hvorfor det ikke er muligt at angive en udvikling fra 2017 og 2018.

Udføres der tests mod virksomheden?

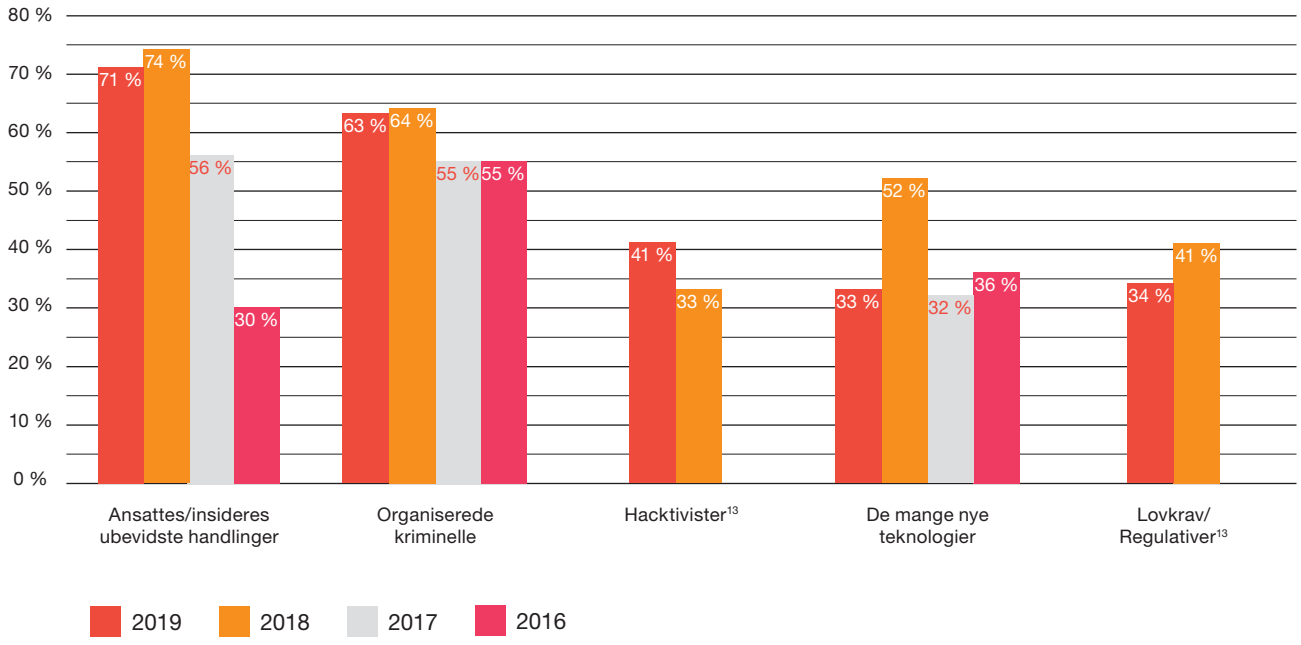


"Det er PwC's erfaring, at virksomheder, der har investeret i cybersikkerhedstiltag – herunder processer, awareness og arkitektur – ikke validerer for tilstrækkelighed og effektivitet af tiltagene. Derved er de dels ikke klar over, om de har fået værdi for investeringen, og dels ikke sikre på, at de har imødegået de forskellige cyberrisici. Det er derfor en god idé at validere virksomhedens sikkerhed jævnligt."

Undersøgelsen viser samtidig, at ansattes/insideres ubevidste handlinger fortsat udgør den største cybertrussel på trods af et fald på 3 %-point siden 2018 (fra 74 % i 2018 til 71 % i 2019). Dette stemmer overens med den store andel, der fortsat er ramt af phishing-angreb (68 % i 2018), da succesen af denne type angreb afhænger af ansattes/insideres ubevidste handlinger. Det kan derfor være nærliggende at trække en rød tråd mellem faldet i antallet af respondenter, der angiver, at ansattes/insideres ubevidste handlinger udgør den største trussel, og virksomhedernes investering i awareness-træning.

Efter ansattes/insideres ubevidste handlinger vurderes organiserede kriminelle med 63 % i 2019 ligeledes at være blandt de største cybertrusler mod virksomhederne. Herefter følger hacktivister med 41 %. En markant ændring i respondenternes tilkendegivelse af cybertrusler fra 2018 til 2019 er cybertruslen knyttet til nye teknologier, som er faldet fra 52 % i 2018 til 33 % i 2019. Også truslen fra lovkrav/regulativer er faldet fra 41 % i 2018 til 34 % i 2019, hvilket står i kontrast til respondenternes tidligere tilkendegivelser i relation til GDPR.

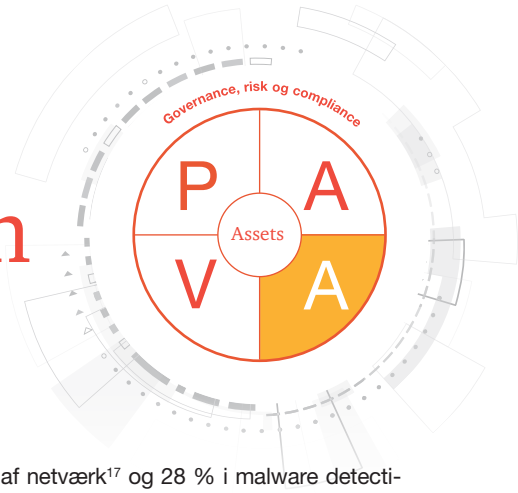
Hvad udgør de største trusler mod din virksomhed i relation til cyber-/informationssikkerhed?



"Undersøgelsen viser, at cybertruslerne stadig er en stor bekymring til trods for mindre udsving gennem årene. For at få et reelt billede af, hvad jeres virksomhed er sårbar over for, anbefaler vi, at der foretages en test af jeres samlede sikkerhedsniveau. Vi anbefaler at få foretaget et simuleret hacker-angreb i form af en red team-test, som viser, hvor sårbare I reelt er."

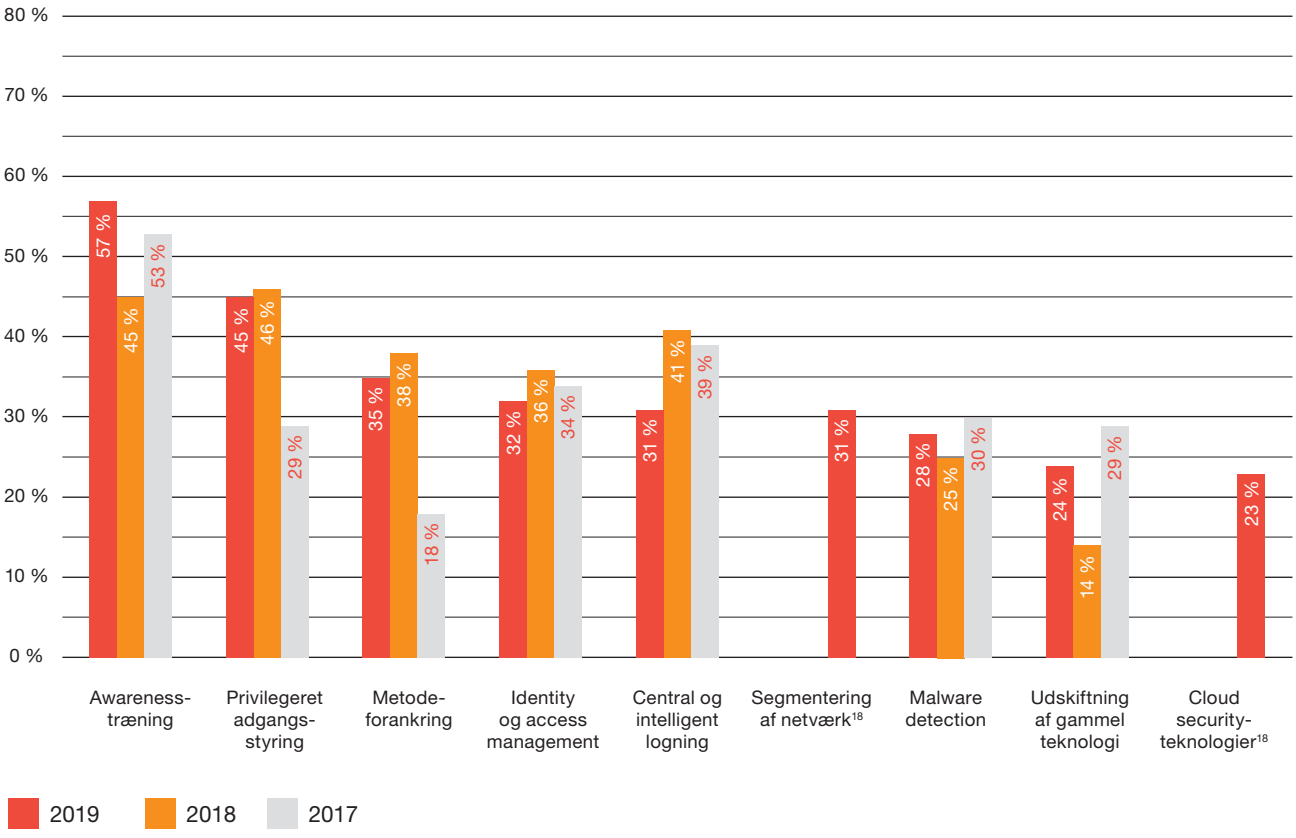
[13] Hacktivister og lovkrav/regulativer er svarmuligheder tilføjet i 2018, hvorfor det ikke er muligt at angive en udvikling fra 2016 og 2017.

Fokusinvesteringer i dansk erhvervsliv inden for cybersikkerhed



Ser man på virksomhedernes teknologiinvesteringer, så viser undersøgelsen, at 45 % planlægger at investere i privilegeret adgangsstyring[14] inden for de næste 12 måneder. Ligeledes viser undersøgelsen, at 32 % forventer at investere i identity og access management[15], 31 % i central og intelligent logning[16], 31 % i segmentering af netværk[17] og 28 % i malware detection. Derudover peger 24 % på udskiftning af gammel teknologi, også kaldet "legacy-systemer", og 23 % på cloud security-teknologier.

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



[14] Privilegeret adgangsstyring handler om at få styr på de privilegerede rettigheder i en virksomheds it-infrastruktur.
[15] Identity og access management handler om at strukturere og automatisere alle identiteter i ens virksomhed, herunder rettidigt sikre korrekt rettighedsdeling og -fratagelse.
[16] Ved central og intelligent logning sender alle systemer logdata til ét centralt system. Systemet er intelligent, i den forstand at det leder efter mønstre eller anormaliteter i logdataene.
[17] Med henblik på at forbedre sikkerheden handler netværkssegmentering om at dele eller segmentere et computernetværk i mindre separate netværk.
[18] Segmentering af netværk og cloud security-teknologier er svarmuligheder tilføjet i 2019, hvorfor det ikke er muligt at angive en udvikling fra 2017 og 2018.

57 %
Awareness-træning

45 %
Priviligeret adgangsstyring

35 %
Metode-forankring

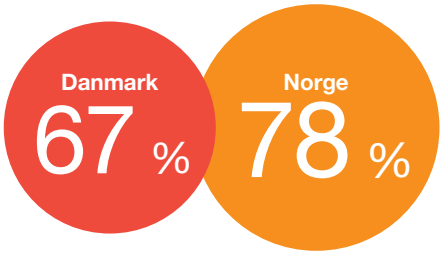
"Der er en hastig udvikling i antallet af avancerede cyberangreb mod virksomhederne med store økonomiske tab til følge. PwC anbefaler derfor, at der kommer mere fokus på investeringen i og implementeringen af sikkerhedsteknologier, der effektivt medvirker til at sikre virksomheden. Der er behov for, at teknologien hjælper medarbejderne med at forblive sikre."

Norge – flere har været udsat for en hændelse

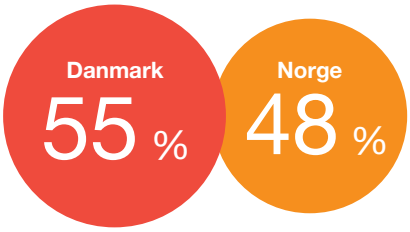
For fjerde år i træk har norske erhvervsfolk givet deres bidrag til PwC's Cybercrime Survey 2019. 71 norske virksomhedsledere, it-chefer og specialister har deltaget i undersøgelsen, og når vi sammenligner de norske og danske svar, afviger billedet især ved antallet og typen af sikkerhedshændelser.

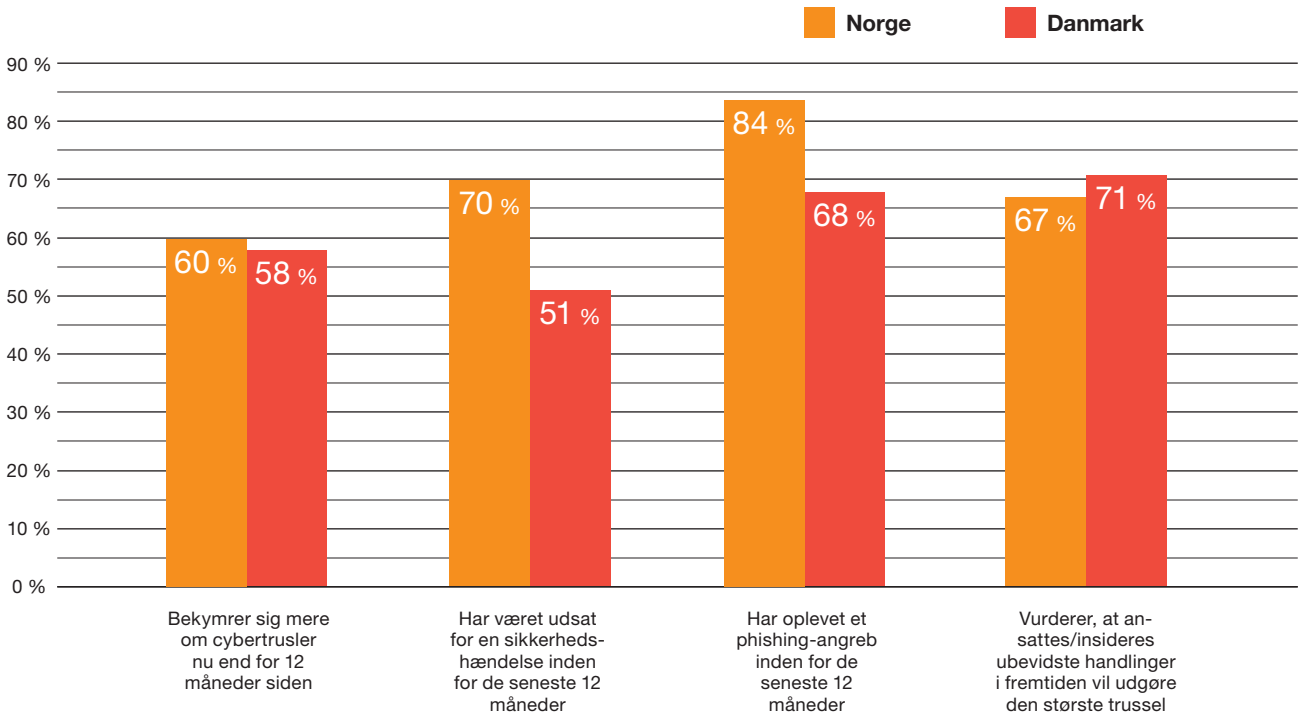
70 % af de norske respondenter angiver, at de har været udsat for en sikkerhedshændelse inden for de seneste 12 måneder, hvor det samme tal er 51 % i Danmark. Derudover vurderer 84 % af respondenterne i Norge, at de har oplevet et phishing-angreb inden for de seneste 12 måneder. Til sammenligning angiver 68 % af de danske respondenter det samme.

Har i mindre grad eller slet ikke tillid til cybersikkerheden i kommunerne



Har i mindre grad eller slet ikke tillid til GDPR-compliance-niveauet i kommunerne





Om undersøgelsen

325 danske og 71 norske virksomhedsledere, it-chefer og sikkerhedsspecialister har deltaget i PwC's Cybercrime Survey 2019. Undersøgelsen er igen i år gennemført med opbakning fra Center for Cybersikkerhed, DI Digital, Finans Danmark, Dansk Erhverv, IT-Branchen, Dansk It, KITA, Rigspolitiet NC3, Microsoft, Rådet for Digital Sikkerhed og ISACA. Analysen bygger på onlinebesvarelser.

Respondenterne er blevet stillet en række spørgsmål, som relaterer sig til cyberområdet, fx om de er blevet ramt af et cyberangreb, om de er bekymrede for truslen fra cybercrime, hvor stort deres cyber-/informationsbudget er, 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 ovenstående organisationer.

Undersøgelsens respondenter fordelt på sektorer

Den private sektor

62 %

Større virksomheder

Defineret ved
>200
medarbejdere

Mindre virksomheder

Defineret ved
<199
medarbejdere

Den offentlige sektor

25 %

Den finansielle sektor

13 %

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 vi 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?
- [ ] Har din virksomhed en CISO/sikkerhedsansvarlig?
- [ ] Omfatter arbejdet med sikkerhed både informationssikkerhed (ISO 27001) og cybersikkerhed?

Processer

- [ ] Har I foretaget en måling på jeres robusthed mod cybertruslerne (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?

Validering

- [ ] Gennemfører I løbende test til identifikation af sårbarheder i jeres infrastruktur og systemer?
- [ ] Har I en defineret og afprøvet incident response-proces?
- [ ] Har I testet beredskabsplanen for cyberhændelser?

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?
- [ ] Har I implementeret databeskyttelsesforordningen?
- [ ] Er der etableret en driftsorganisation for fortsat sikring af compliance med databeskyttelsesforordningen?

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/cybersecurity

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
Digital Trust
3945 3282
christian.kjaer@pwc.com

Om PwC

PwC arbejder 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 flere end 2.500 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi over 276.000 PwC'ere i 157 lande, og i Danmark er vi markedsledende. Mød os over hele landet. Vi er der, hvor du er.

Succes skaber vi sammen …

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 ...