Danmark og cybersikkerhed: Virksomhederne er fortsat bekymrede, og ledelsen er begyndt at tage initiativ

Cybercrime Survey 2016

Ca. 300 virksomhedsledere, it-chefer og -specialister fra danske virksomheder har delt deres syn på forskellige forhold i relation til cyberkriminalitet. De har fx taget stilling til udviklingen i trusselsbilledet og angivet, hvorledes og i hvilket omfang de arbejder med udfordringerne. Dette års survey indeholder desuden svar fra ca. 200 norske erhvervsfolk.

69 %

af de danske respondenter har været udsat for ***cyberangreb*** inden for det seneste år.

67 %

af de danske respondenter, mod 22 % i 2015, har været udsat for ***afpresning*** (fx ransomware) inden for de sidste 12 måneder.

77 %

af de danske respondenter vurderer, at de i fremtiden vil være nødt til som minimum at ***ændre forretningsgange og procedurer*** for at tilpasse sig den kommende EU-persondataforordning.

pwc

www.pwc.dk/cybersecurity

Indhold

Er din virksomhed forberedt?

Ledelsen bør forholde sig til problematikken angående cybersikkerhed og stille følgende spørgsmål:

1. ***Er vores sikkerheds-program tilpasset vores for-retnings-strategi?***
2. ***Har vi de kompetencer, der skal til for at identificere de strategiske trusler og de potentielle angreb mod vores for-retning?***
3. ***Kan vi for-klare vores sikkerheds-strategi til vores interes-senter?***
4. ***Ved vi, hvilke informationer der er mest kritiske for forretningen?***
5. ***Har virksom-heden etable-ret et krise-beredskab, der kan styre den sikkert igen-nem en kom-pleks it-relate-ret hændelse?***

Cybercrime Survey 2016
Introduktion

Den digitale og teknologiske udvikling er i fuld gang, og flere virksomheder* vurderer i øjeblikket, hvorledes de kan udnytte nye muligheder til fordel for deres forretning. Nye digitale forretningsmodeller udvikles, nye teknologier bliver mere og mere aktuelle, og flere begynder at anvende data til at forstå deres kunder bedre.

Det gør cybersikkerhed mere relevant end nogensinde før. Selvom PwC's Cybercrime Survey 2016, som gennemføres for andet år i træk, viser positive tendenser – fx i form af at flere oftere briefer deres ledelse om cybertrusler – viser den også, at mange er mere bekymrede for cybertrusler, end de var for 12 måneder siden. Derudover oplyser flere end sidste år, at de har været udsat for cyberangreb inden for de seneste 12 måneder. Det kan være dyrt for virksomhederne, hvis de udsættes for et angreb, og på trods af at undersøgelsen ikke indikerer store milliontab hos alle virksomheder, så viser den, at mange rammes økonomisk, og at der generelt er forbedringspotentiale, når det kommer til at forebygge, opdage og håndtere cyberhændelser.

Årets survey viser en stor stigning i andelen af virksomheder, som har været udsat for afpresning, fx ransomware, hvor filer bliver krypteret, og kriminelle kræver penge for at frigive dem. Der er altså en udfordring i og et behov for at øge sikkerhedsbevidstheden hos eksempelvis ansatte, så man i højere grad kan forhindre disse former for angreb. At virksomhederne er blevet mere opmærksomme på denne udfordring ses af PwC's Cybercrime Survey 2016, ved at over halvdelen – og hele 17 procentpoint flere end sidste år – peger på awareness-træning som én af deres prioriterede investeringer i relation til cybersikkerhed.

Ud over at den digitale og teknologiske udvikling har gjort cybertruslen mere aktuel end nogensinde før, har den også afstedkommet en ny EU-persondataforordning, som er vedtaget med virkning fra maj 2018. Blot halvdelen af undersøgelsens respondenter mener, at om 18 måneder vil deres virksomheds personfølsomme data i høj grad være tilstrækkeligt beskyttet i henhold til den på dette tidspunkt gældende lovgivning. Det kan betyde, at flere risikerer store bøder, hvis kravene til sikkerhed ikke overholdes.

En stor tak til alle de erhvervsfolk, der har svaret på PwC's Cybercrime Survey 2016, og rigtig god læselyst.

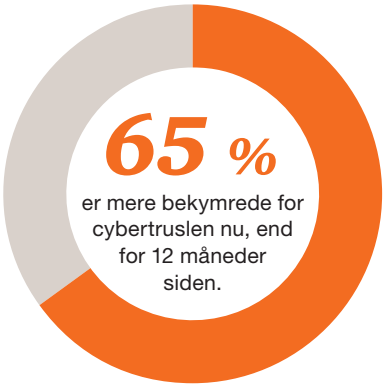
* I denne rapport rapporteres der primært på de danske svar. På side 12 finder du et særskilt afsnit, hvor de danske svar sammenlignes med de norske.

Truslen fra cyberkriminalitet bekymrer fortsat mange, og flere rammes af cyberhændelser

Cybertruslen ligger igen i år de danske virksomheder og organisationer tungt på sinde. 65 % af respondenterne, mod 68 % sidste år, svarer, at de er mere bekymrede for cybertruslen nu, end de var for 12 måneder siden. Selvom andelen er faldet en smule, er der fortsat en stor del af de adspurgte, som er bekymret, og undersøgelsen understreger, at bekymringen er berettiget. Hele 69 % af respondenterne har været udsat for angreb eller hændelser, relateret til cyberkriminalitet, i det seneste regnskabsår. Det er en stigning, når man sammenligner med sidste års resultat, hvor 59 % svarede det samme.

Specielt de store virksomheder er hårdt ramt. Undersøgelsen viser, at de store virksomheder* har oplevet en stigning på 16 % i antallet af angreb og hændelser, hvor de mindre organisationer til sammenligning har oplevet et fald på 7 %.

* Virksomheder med mere end 2.500 ansatte.



De store virksomheder har oplevet en stigning på

16 %

i antallet af angreb og hændelser, som er relateret til cyberkriminalitet.

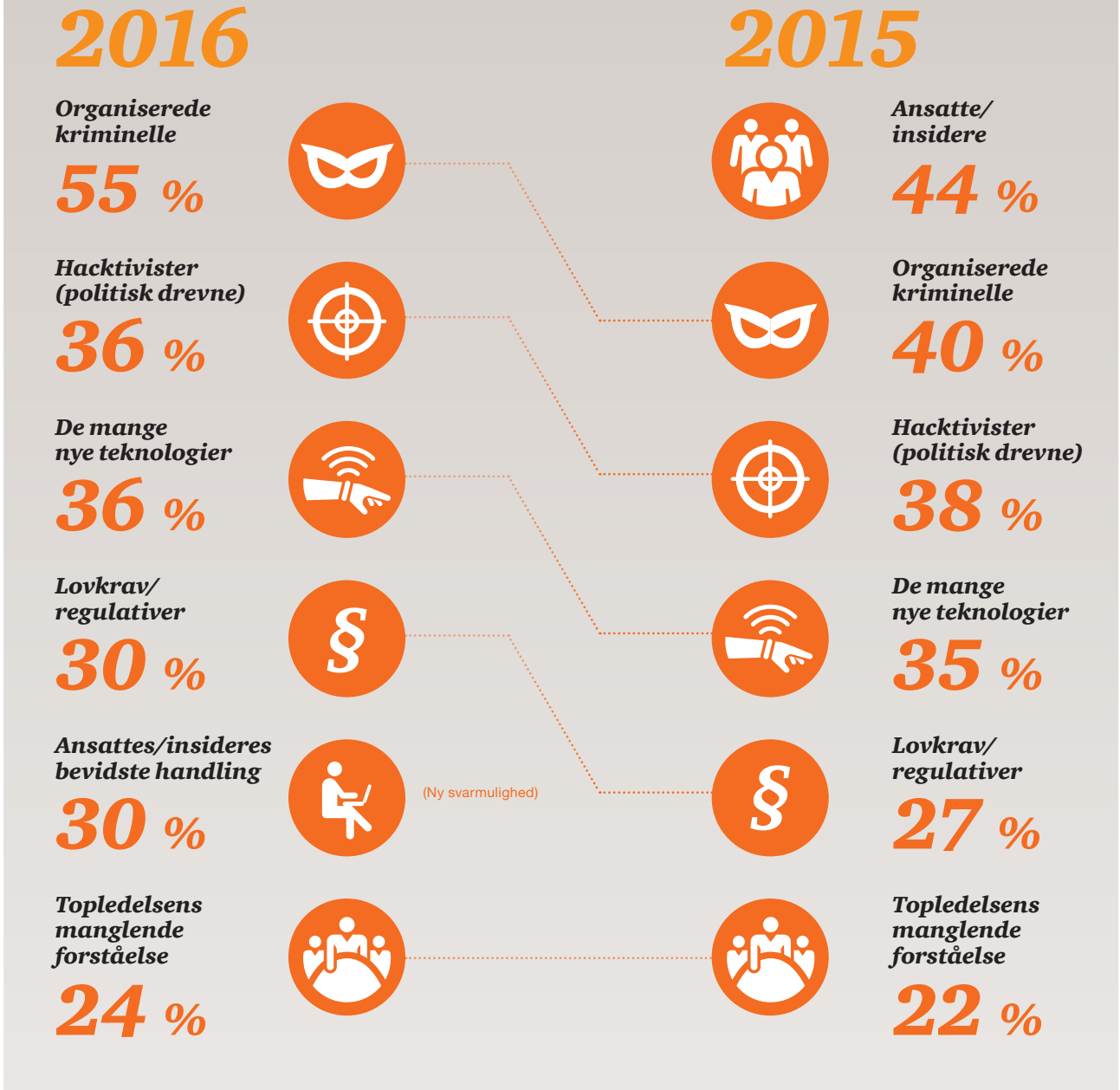
Organiserede kriminelle udgør den største bekymring

I år har respondenterne vurderet nedenstående seks trusler til at være dét, der vil udgøre den største cybertrussel for dem i fremtiden, og vi ser en stor stigning i andelen, der har peget på organiserede kriminelle. 55 % af respondenterne mod 40 % sidste år mener, at organiserede kriminelle vil udgøre den største trussel for deres virksomhed i fremtiden.

Sidste år pegede flest på ansatte/insidere som værende den største trussel – valgt af 44 %. I år er svarmuligheden præciseret til ansattes/indsideres bevidste handling, og andelen, som har peget på dette som en trussel, er 30 %. Forskellen kan skyldes, at det ofte er en utilsigtet handling, som kan udgøre truslen fra ansatte/insidere.

PwC's Cybercrime Survey 2016 viser en kraftig stigning i andelen, der rammes af afpresning (fx ransomware, hvor filer krypteres, og virksomheden skal betale penge for at få dem frigivet), hvilket som regel sker, ved at en ansat kommer til at klikke på et forkert link eller lignende.

Hvad vil i fremtiden udgøre den største cybertrussel for virksomheden?



Flere cyberangreb – øgede udgifter

Hele 69 % af respondenterne har været udsat for hændelser eller angreb, relateret til cyberkriminalitet, de seneste 12 måneder, og dette har økonomiske konsekvenser for virksomhederne.

64 % svarer, at der har været monetære omkostninger for virksomheden som følge af cyberangreb det seneste år. En tredjedel angiver sågar, at deres omkostninger overstiger 1 million kr., og halvdelen af respondenterne har øgede udgifter til udbedring og efterforskning af sikkerhedshændelser.

Disse øgede udgifter og omkostninger kan muligvis forklares ved, at vi ser en kraftig stigning i antallet af cyberangreb, fx ransomware-angreb.

67 %

af respondenterne har været ramt af ransomware i 2016 mod blot 22 % i 2015.

Tredobling i ransomware-angreb

Ved ransomware-angreb tages en virksomheds data som gidsel, ved at angriberne krypterer virksomhedens data og efterfølgende afpresser virksomheden ved at tilbyde krypteringsnøglen for et givent beløb. I årets undersøgelse svarer hele 67 % af respondenterne, at de har været udsat for ransomware-angreb, hvilket er en tredobling, sammenlignet med 2015.

2016 har også været året for en voksende bølge af phishing- og afpresningsangreb via sms. Angriberne har forsøgt at få oplyst bankoplysninger, NemID og adgangskoder ved at udgive sig for at være fra en virksomhed, som er kendt af den brede befolkning.

Ramt af ransomware?

Vi anbefaler de kunder, som vi hjælper med ransomware-sager, at de sidestiller angreb med en sikkerhedshændelse og ikke en driftshændelse.

Det vil sige, at man straks bør kontakte sin sikkerhedsafdeling, hvis man har mistanke om et angreb, så man kan eksekvere en foruddefineret og velafprøvet procedure for håndtering af den givne cyberhændelse.

Cyber Incident Response-team

En stigende andel af virksomhederne oplever cyberangreb. PwC hjælper dem med at forebygge og håndtere cyberhændelser og har bl.a. etableret en central cyberhotline for kunder, så muligheden for akut hjælp lokalt og globalt bliver øget.

Teamet hjælper med at skabe overblik over en given trussel, og cyber forensics-specialister identificerer angrebets art og de udnyttede sårbarheder. Derefter kan der implementeres forbedringer af sikkerheden og udarbejdes en rapport til brug for bl.a. ledelsen, forsikringsselskabet og politiet.

Se kontaktinfo på side 15.

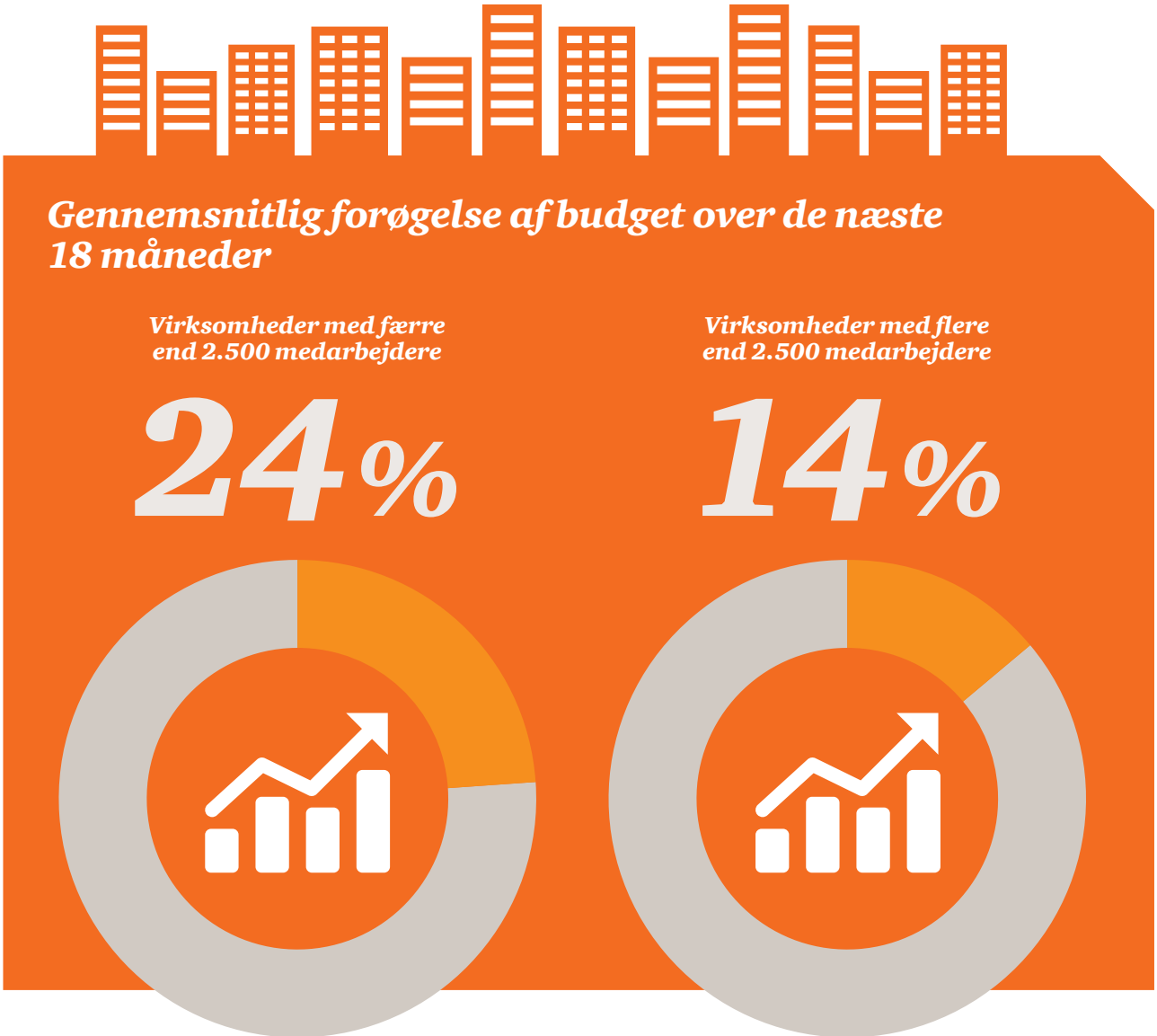
Ledelsen inddrages i højere grad, og investeringerne i it-sikkerhed øges

De problemstillinger, virksomheder står over for i relation til cybertrusler, bør have ledelsens bevågenhed.

PwC's Cybercrime Survey 2016 viser en positiv udvikling, hvad angår andelen af dem, som svarer, at den sikkerhedsansvarlige i deres virksomhed briefer ledelsen kvartalsvist eller oftere om risikoen ved cybertrusler. Andelen er øget fra 46 % i 2015 til 56 % i 2016; og blot 11 % mod 17 % i 2015 svarer, at dette aldrig sker. En anden udvikling, vi ser, er, at hele 40 % i år mod 27 % sidste år svarer, at bestyrelsen bruger tid på at drøfte spørgsmål om cyber- og/eller informationssikkerhed. Dog svarer over halvdelen (53 %), at dette sker i mindre grad eller slet ikke.

Med den store bekymring over truslen fra cyberkriminalitet og et stigende antal hændelser bliver det mere og mere nødvendigt for virksomhederne at afsætte de fornødne ressourcer til at forebygge og bekæmpe denne trussel. Og undersøgelsen viser, at virksomhederne gør netop dette; den viser fx, at virksomhederne i gennemsnit planlægger at øge deres budgetter til bekæmpelse og forebyggelse af cyberkriminalitet med 15 % over de kommende 18 måneder.

Det er specielt de mindre organisationer, målt på antal ansatte, der planlægger den største gennemsnitlige budgetforøgelse. En af grundene til dette kan være, at de mindre virksomheder nu har erkendt behovet for at afsætte flere midler til bekæmpelse og forebyggelse af cyberkriminalitet.



Sikkerhedsinvesteringer målrettet medarbejdere topper listen

Awareness-træning er igen i år det område, der prioriteres højest, når det kommer til virksomhedernes sikkerhedsinvesteringer, og fokus på dette er endnu større end sidste år.

Derudover er malware detection nu rykket op fra en niendeplads til en andenplads med mere end dobbelt så mange respondenter, der angiver dette som en prioriteret investering for de næste 12 måneder.

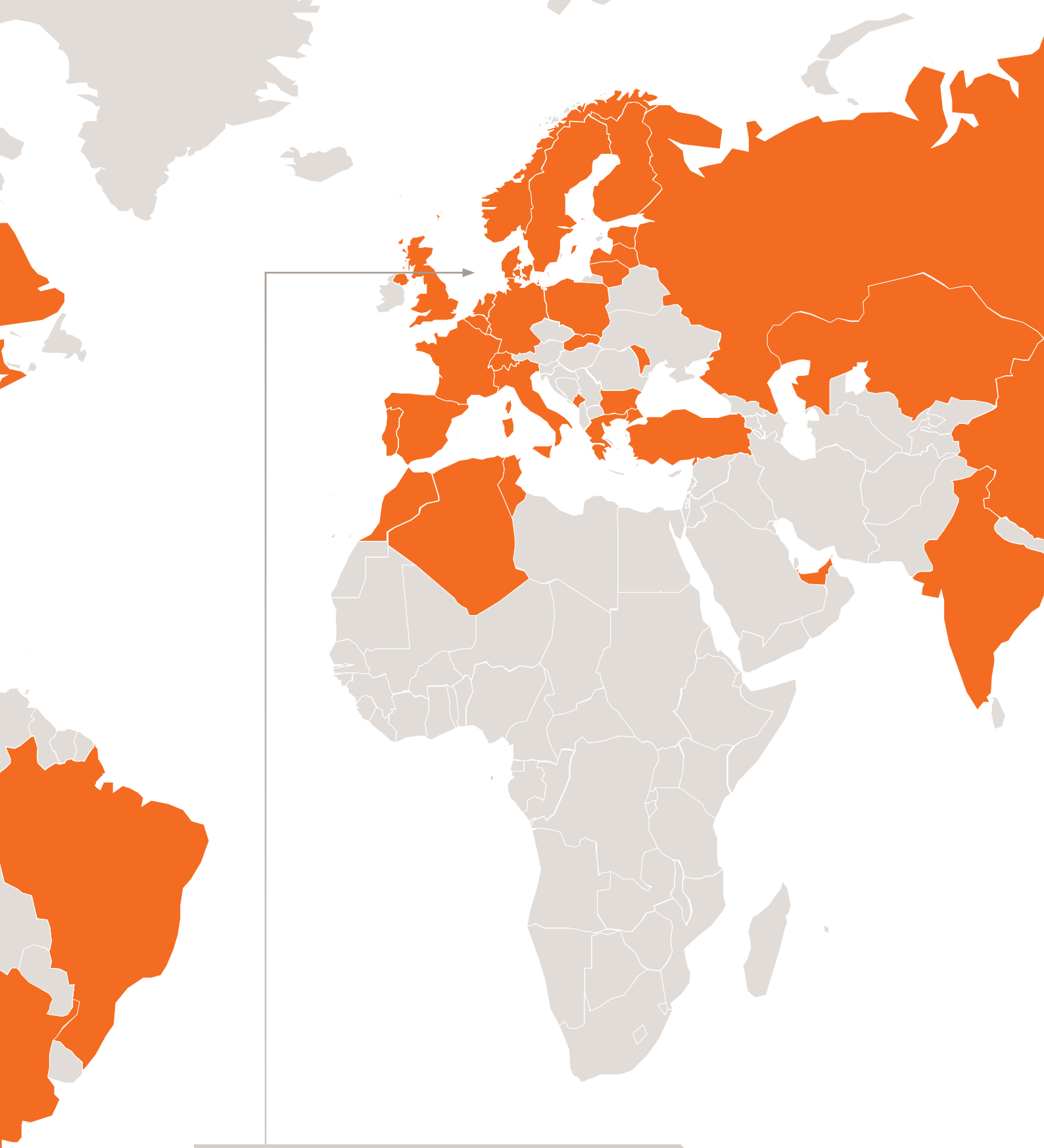
Et område, som i år er kommet på top-10-listen over de højest prioriterede investeringsområder for de næste 12 måneder, er data loss prevention. Det kan dels skyldes de persondatakrav, der følger med den nye EU-persondataforordning, dels det stigende antal cyberhændelser. Data loss prevention kan i denne forbindelse være et utroligt vigtigt tiltag i bestræbelserne på at forhindre, at data går tabt.

Også patch management tools optræder nu i top-10, hvilket viser, at virksomhederne har fokus på én af grundstenene inden for sikkerhed – nemlig at sørge for, at systemerne er og forbliver opdaterede, hvilket kan medvirke til at mindske risikoen for et succesfuldt cyberangreb.

Generelt for mange af disse sikkerhedstiltag er, at de har fået et solidt nøk opad i forhold til antallet af respondenter, der planlægger at investere i dem. Og med et stigende antal virksomheder, der udsættes for cyberkriminalitet, er dette ikke uforståeligt. Det kan også være med til at forklare, hvorfor blot 5 % angiver, at de ikke investerer i cybersikkerhed.

Højest prioriterede investeringer i de næste 12 måneder

		Difference i forhold til 2015
Awareness-træning	57,2 %	+17,3 pp. ▲
Malware detection	37,9 %	+21,6 pp. ▲
Central og intelligent logning	35,2 %	+3,2 pp. ▲
Sikkerhed på mobile enheder	33,8 %	+0,7 pp. ▲
Identity management	32,4 %	+4,3 pp. ▲
Sårbarhedsscanninger	31,0 %	+6,3 pp. ▲
Privilegeret adgangsstyring	29,7 %	+10,0 pp. ▲
Metodeforankring som ISO 2700x eller NIST	25,5 %	÷1,5 pp. ▼
Patch management tools	22,1 %	+9,7 pp. ▲
Data loss prevention	20,0 %	+9,3 pp. ▲



PwC's Globale Privacy Practice

Med PwC's Globale Privacy Pratice kan vi hjælpe din virksomhed med at omsætte juridiske krav i den nye EU-persondataforordning til operationelle og pragmatiske procedurer og processer, som understøttes af tekniske løsninger, der sikrer en effektiv efterlevelse af kravene, ligesom vi kan assistere med kontrol og opfølgningsarbejdet.

Ny EU-persondataforordning

Nye regler medfører ændringer for danske virksomheder

Den nye EU-persondataforordning, som er blevet vedtaget, træder i kraft i maj 2018. Den indeholder en lang række nye og skærpede krav til virksomheder, der behandler data, som direkte eller indirekte kan relateres til en fysisk person.

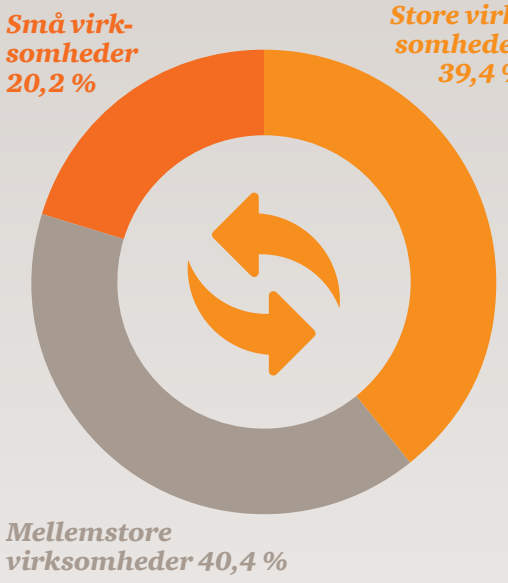
77 % af respondenterne vurderer, at de i fremtiden vil være nødt til som minimum at ændre forretningsgange og procedurer for at tilpasse sig den kommende persondataforordning, mens det kun er 52 %, der mener, at de om 18 måneder i høj grad har sikret deres persondata tilstrækkeligt.

Dermed står en stor del af virksomhederne med en risiko for at skulle imødekomme de bødekrav på op til 4 % af omsætningen eller 20 millioner euro, det vil kunne afstedkomme, hvis kravene i EU-persondataforordningen, herunder krav til sikkerheden, ikke overholdes.

Dette aktualiseres endvidere, ved at hele 69 % af respondenterne har været udsat for hændelser eller angreb, relateret til cyberkriminalitet, i de seneste 12 måneder. Angreb, der i fremtiden meget vel kan tænkes at omfatte tyveri af persondata, og som har til formål at presse penge ud af virksomhederne, mod at deres data ikke lækkes på internettet og dermed medfører bøde fra EU.

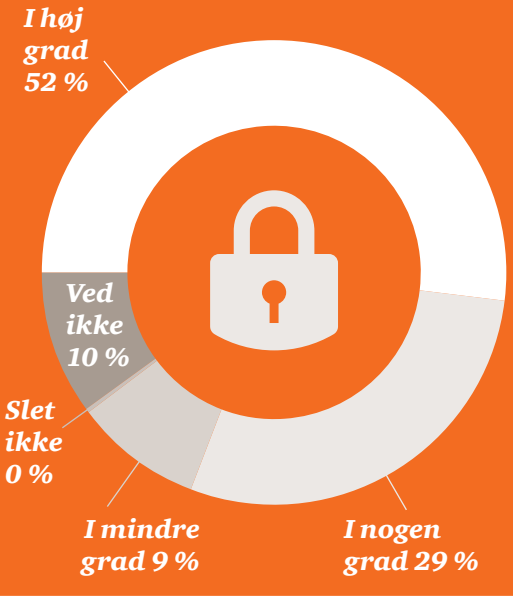
77 %

vil ændre forretningsgange og procedurer for at tilpasse sig den kommende EU-persondataforordning. De 77 % fordeler sig således:



Beskyttelse af personfølsomme data

I hvilken grad er din virksomheds personfølsomme data tilstrækkeligt beskyttet om 18 måneder i henhold til gældende lovgivning?



Norge – et lignende billede

I år har næsten 200 norske erhvervsfolk deltaget i PwC's Cybercrime Survey, og der tegner sig et lignende billede, når vi sammenligner de norske svar med de danske. Også i Norge vurderes organiserede kriminelle at udgøre den største trussel i fremtiden (50 %) – dog meget tæt efterfulgt af ansattes/insideres bevidste handling (48 %).

De danske og norske svar afviger mest fra hinanden, når det kommer til de typer af cyberangreb, som virksomhederne har været udsat for. Næsten to tredjedele (64 %) af de norske respondenter har været ramt af "orme" og vira; til sammenligning angiver ca. halvdelen (48 %) af de danske respondenter det samme.

69 %	58 %	*... har været udsat for et cyberangreb i de seneste 12 måneder.*
65 %	57 %	*... er mere bekymrede for cybertruslen nu end for 12 måneder siden.*
55 %	50 %	*... vurderer, at organiserede kriminelle vil udgøre den største cybertrussel i fremtiden.*
67 %	55 %	*... har været ramt af afpresning (fx ransomware) inden for de seneste 12 måneder.*
77 %	66 %	*... vurderer, at de i fremtiden vil være nødt til som minimum at ændre forretningsgange og procedurer for at tilpasse sig den kommende EU-persondataforordning.*

cybercrime
internet hacking malware
phishing
firewall privacy

Om undersøgelsen

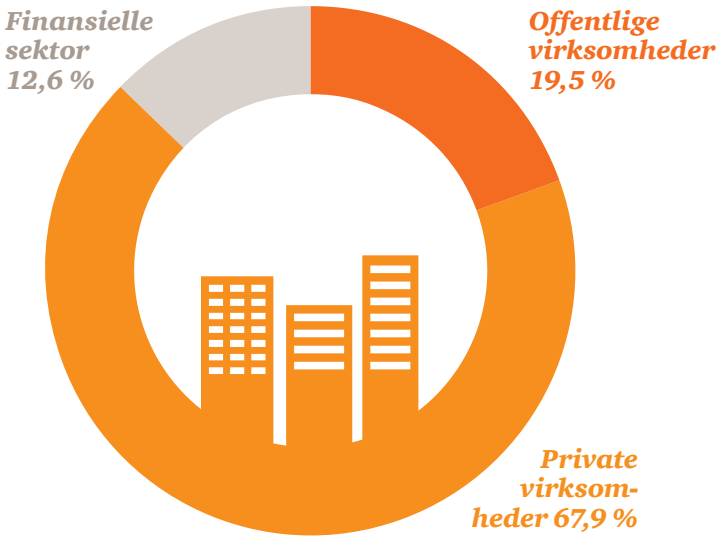
297 danske og 191 norske virksomhedsledere, it-chefer og -specialister har deltaget i PwC's Cybercrime Survey 2016, som i år er gennemført med opbakning fra DANVA, Finansrådet, Dansk Erhverv, Kita, IT-Branchen, Center for Cybersikkerhed og DI Digital. Undersøgelsen bygger på onlinebesvarelser, afgivet i perioden 1. juni til 2. september 2016.

Respondenterne er blevet stillet en række spørgsmål, som relaterer sig til cyberområdet – fx om de er blevet ramt af et cyber-angreb, hvor meget de investerer i it-sikkerhed, og om de er bekymrede over truslen fra cybercrime, ligesom de er blevet spurgt til, hvordan deres virksomhed forholder sig til den nye EU-persondataforordning mv.

Ca. 55 % er SMV'er, og ca. 20 % er store virksomheder; de resterende har valgt ikke at angive antal ansatte, som i denne undersøgelse anvendes til at definere virksomhedens størrelse. Virksomhederne kommer fra et bredt udsnit af brancher/industrier/sektorer, herunder handel og forbrug, den finansielle sektor, professionelle services og rådgivning, teknologi, industrielle virksomheder, offentlige institutioner, energi og forsyning, transport, farma mv.

Undersøgelsens spørgsmål og svarmuligheder er udarbejdet af PwC og udsendt i samarbejde med tidligere nævnte organisationer.

Brancheforddeling

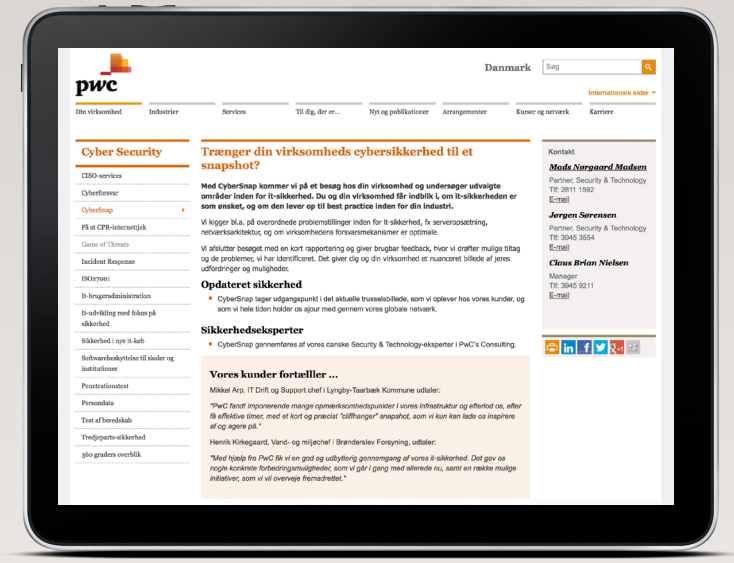


Inspiration

Trænger din virksomheds cybersikkerhed til et snapshot?

Få overblik over din virksomheds sikkerhedsniveau med PwC's CyberSnap.

Med CyberSnap kommer vi på besøg i din virksomhed og undersøger udvalgte områder inden for it-sikkerhed. Du og din virksomhed får indblik i, om it-sikkerheden er som ønsket, og om den lever op til best practice inden for din industri. Læs mere på www.pwc.dk/cybersnap



Game of Threats™ – spil din ledelse stærk

Med PwC's unikke Game of Threats™ får I mulighed for at få simuleret forskellige former for hackerangreb mod jeres virksomhed, træne forskellige cyberforsvar og opnå en bedre forståelse for de nødvendige tiltag, I bør implementere for at imødegå cyberangreb.

Se video

Se video af workshoppen og læs mere på www.pwc.dk/got

Få hjælp

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 it-sikkerhed på www.pwc.dk/cybersecurity

Mads Nørgaard Madsen
Partner
Security & Technology
M: 2811 1592
E: mxm@pwc.dk

Jørgen Sørensen
Partner
Security & Technology
T: 3945 3554
E: jgs@pwc.dk

Christian Kjær
Director
IT Risk Assurance
M: 5132 1270
E: cik@pwc.dk

PwC's Incident Response team
T: 70 222 444

Vi har kontorer i 15 byer – også en tæt på dig.

Succes skaber vi sammen ...

Revision. Skat. Rådgivning.