Danmark og cybersikkerhed: Virksomhederne er bekymrede

Cybercrime Survey 2015

Omkring 250 virksomhedsledere, it-chefer og specialister fra danske virksomheder har delt deres aktuelle indtryk af cyberkriminalitet i Danmark. De tager bl.a. stilling til udviklingen i trusselsbilledet og angiver, hvordan eller hvorvidt deres virksomheder arbejder med udfordringen.

59 %

har oplevet ***cyberangreb*** inden for det seneste år, og antallet af angreb er stigende og med større konsekvenser.

68 %

er mere bekymrede for ***cybertruslen*** end for 12 måneder siden.

61 %

mener, at bestyrelserne ikke bruger nok tid på ***cybersikkerhed.***

pwc

www.pwc.dk/cybersecurity

Cybercrime Survey 2015
Introduktion

Cybersikkerhed er ikke længere en opgave, der kun er relevant for it- og sikkerhedsafdelingerne. Konsekvenserne af cyberkriminalitet er nået til ledelsesgangene i de danske virksomheder og organisationer.

Nyhedsindslag om sikkerhedshændelser og trusler er blevet et næsten dagligt fænomen, og gennem de seneste 12 måneder er de fleste industrier og brancher blevet påvirket af én eller anden form for cybertrussel.

Vi har derfor fundet det vigtigt at undersøge, hvordan danske virksomheder og organisationer opfatter truslen fra cyberkriminalitet, hvad de gør for at beskytte sig, og hvor de mener, at der bør sættes mere ind for at håndtere den.

Bekymringer og muligheder

Danskerne udtrykker stor bekymring over cyberkriminalitet i fremtiden, og det er der også god grund til. Mange danske virksomheder har gennem de seneste år ikke formået at følge med udviklingen på sikkerhedsområdet.

It-landskabet er komplekst og består af mange knopskydninger, og med et øget trusselsniveau risikerer virksomhederne at blive taget med bukserne nede. Det er en lang og kompleks rejse, men udnyttes muligheden for at skabe forandringer nu, vil der være store gevinster ved at effektivisere via nye digitale muligheder og opbygge en stærkere digital beskyttelse.

Fremtiden vil kun byde på flere krav til digitalisering, og et stigende antal love vil løbende tvinge virksomhederne til at gøre mere. For at håndtere cybertruslen bedst muligt er det nødvendigt ikke kun at prioritere området højere, men også at arbejde for en fælles indsats, hvor alle – fra bestyrelsesformanden til den menige medarbejder – er bevidste om udfordringerne og deres rolle og ansvar.

Mads Nørgaard Madsen

Christian Kjær

68 % bekymrer sig mere om cybertruslen

Risikoen for cyberangreb er for alvor kommet i fokus hos danske virksomheder og organisationer, der oplever en stigende bekymring over denne trussel.

Hændelser, som er relateret til cyberkriminalitet, er blevet mere og mere markante, både hvad angår hyppighed og i den konsekvens, som hændelserne har for de påvirkede organisationer. I dag er det heller ikke længere kun de mest prominente virksomheder med stor offentlig bevågenhed, der udsættes for angreb. Mindre organisationer står også for skud.

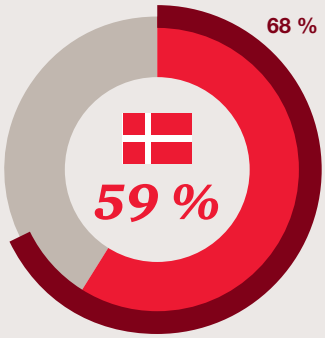
Denne undersøgelse peger tydeligt på en stigende opmærksomhed på og bekymring om cyberkriminalitet blandt private virksomheder og offentlige organisationer i Danmark. Det gælder for 68 % af respondenterne, at de er mere bekymrede for cyberangreb lige nu, end de var for 12 måneder siden. Tendensen stemmer overens med billedet fra vores amerikanske undersøgelse, hvor hele 76 % af respondenterne udtrykker en stigende bekymring.

Bekymringen er velbegrundet. I Danmark har 59 % allerede oplevet angreb eller hændelser, som er relateret til cyberkriminalitet, i det seneste regnskabsår, sammenlignet med 49 % det forrige år. Samtidig kan andelen reelt være endnu større, da 25 % af de danske respondenter ikke ved, hvor mange hændelser de har haft. Endnu mere udbredt er cyberangreb blandt amerikanske virksomheder, hvor 79 % har oplevet hændelser inden for de seneste 12 måneder.

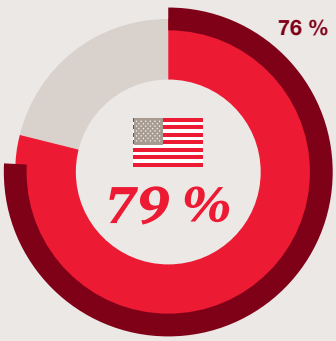
25 %

af de danske respondenter ved ikke, hvor mange hændelser de har haft.

Bekymringen er velbegrundet



59 % af de danske respondenter har oplevet hændelser, og 68 % er bekymrede for fremtiden.



I USA har 79 % af respondenterne oplevet hændelser, mens 76 % er bekymrede for fremtiden.

Større opmærksomhed – men fortsat lav prioritering

2015 har været en øjenåbner for mange i forhold til de risici, som virksomheder og organisationer må forholde sig til i relation til cyberkriminalitet. En logisk forventning må derfor være, at virksomhederne også erkender nødvendigheden af at investere budgetmæssigt i cybersikkerhed.

Denne undersøgelse viser, at på trods af et stigende antal angreb og større opmærksomhed på truslen prioriterer virksomhederne ikke arbejdet med cybersikkerhed særligt højt. Kun omkring en tredjedel af respondenterne angiver stigninger i sikkerhedsbudgettet i det seneste regnskabsår.

Private virksomheder prioriterer cybersikkerhed en smule højere end det offentlige. I alt angiver 36 % af de private virksomheder budgetforøgelser mod 27 % af de offentlige organisationer, og de store virksomheder, målt på antal medarbejdere, prioriterer ligeledes sikkerhedsarbejdet højere end de små og mellemstore.

Stor opmærksomhed, lille indsats

Hvad gør virksomhederne ved den nye trussel?

Ifølge undersøgelsen er svaret:

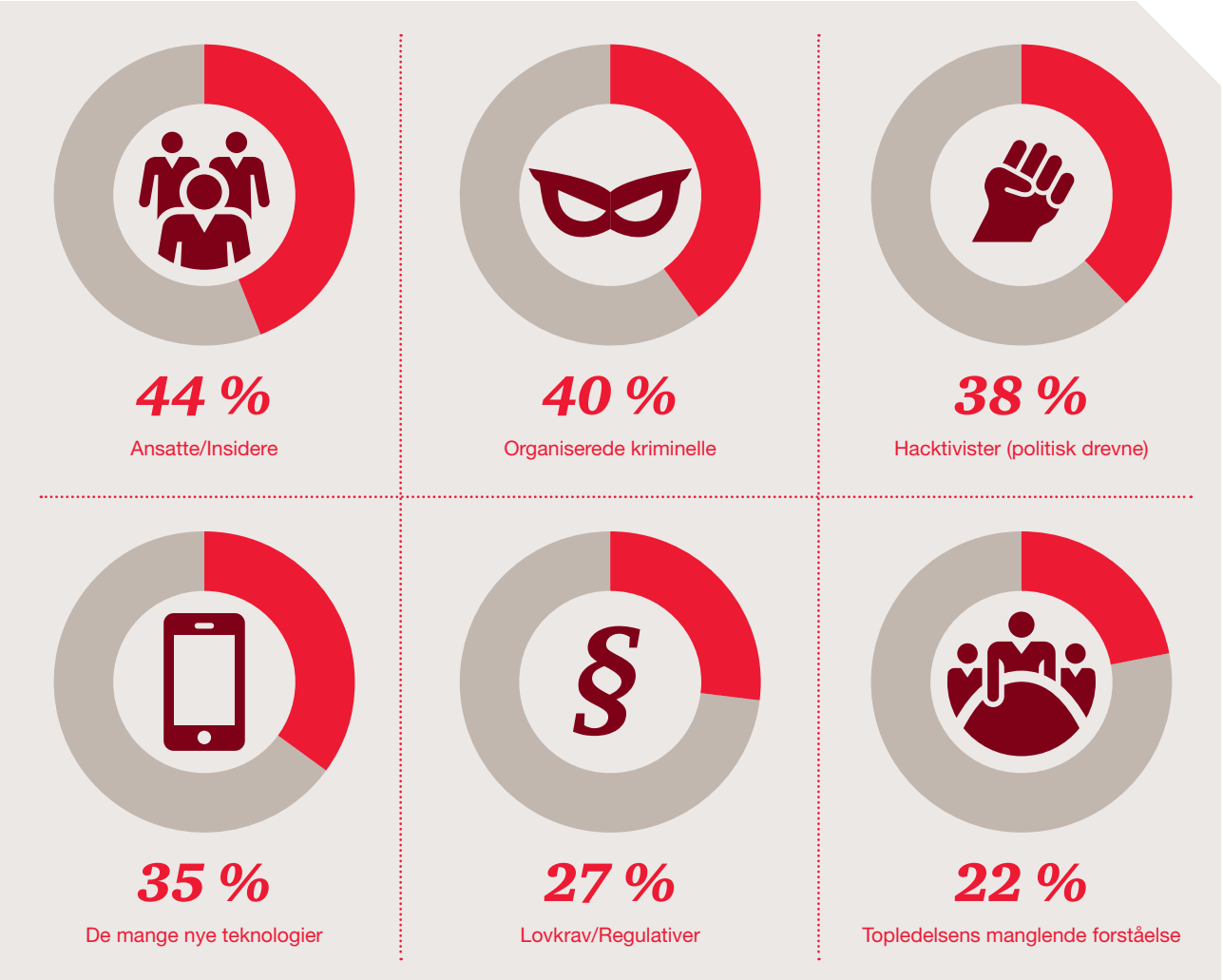
"Ikke nok endnu"

Største bekymring: Egne medarbejdere

En af de interessante observationer fra undersøgelen er, at næsten halvdelen af respondenterne vurderer, at deres egne ansatte eller insidere vil udgøre én af de største trusler mod virksomheden i fremtiden.

Selvom der er brodne kar – også i danske virksomheder – så er resultatet ikke ensbetydende med, at alle virksomhederne ser deres medarbejdere som potentielt kriminelle. Derimod kan uvidende medarbejdere generelt forårsage stor skade ved deres handlinger, eksempelvis ved at klikke ukritisk på links i mails eller høfligt at holde døren for uvedkommende, der derefter tilgår virksomhedens lokaler og informationsaktiver uden berettigelse.

Hvad vil i fremtiden udgøre den største cybertrussel for virksomheden?



Cyberangreb med større konsekvenser

I 2014 var der én milliard tilfælde af datakompromittering på globalt plan[1]. Tidligere kom disse hændelser kun sjældent til offentlighedens kendskab, men nu fylder den slags sager meget i mediebilledet, hvor begreber som cybersikkerhed, hackerangreb og datatab er blevet alment kendte. Netop på baggrund af dette resultat er der tilsyneladende et stort behov for kompetent uddannelse af medarbejdere i virksomhederne.

Grunden til den større mediebevågenhed er dels, at angribernes tiltag er blevet mere ekstreme, dels at hændelserne har større konsekvenser for de ramte virksomheder. Angrebsformerne udvikler sig hele tiden, og med enkle midler kan de forårsage stor skade, så det er svært for virksomhederne at følge med.

For eksempel har 22 % af respondenterne været ramt af såkaldt "ransomware", hvor virksomhedens data bliver taget som gidsel, ved at angriberne krypterer dataene og efterfølgende afpresser virksomheden ved at tilbyde krypteringsnøglen for et vist beløb. Den første større bølge af ransomware-angreb ramte danske virksomheder i foråret 2015.

[1] Gemalto, Gemalto Releases Findings of 2014 Breach Level Index, February 12, 2015

22 %

af respondenterne har været ramt af ransomware.

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 der kan lægges en plan for, hvordan man bedst muligt håndterer sagen.

Cyber Incident Response-team

PwC's dedikerede team af medarbejdere, der hjælper kunder med at forebygge og reagere på cybersikkerheds-hændelser, har bemærket en stærkt stigende aktivitet i den seneste periode. Især Ransomware har optaget vores kunder, og på grund af de mange henvendelser har PwC etableret en central cyber-hotline for kunder, så muligheden for akut hjælp lokalt og globalt bliver øget.

Teamet hjælper med at skabe ro og overblik over en given trussel, og cyber forensics-specialister identificerer angrebets art og de udnyttede sårbarheder. Derefter kan der udarbejdes en rapport til brug for forebyggelse og til politiet.

Få hjælp

Før
Forebyggelse af angreb, sikring af væsentligt vigtige data.

Under
Brandslukning og minimering af skade.

Efter
Sporing og indsamling af viden om angrebet.

22 %

mener, at topledelsens manglende forståelse udgør en af de største trusler for virksomheden

Manglende prioritering hos ledelsen

Arbejdet med informationssikkerhed har længe været betragtet som en it- eller compliance-opgave. Vores amerikanske undersøgelse viser, at 49 % af bestyrelsesmedlemmer stadig ser cybersikkerhed som en it-udfordring, selvom en hændelse potentielt kan få store konsekvenser for forretningen og virksomhedens omdømme.

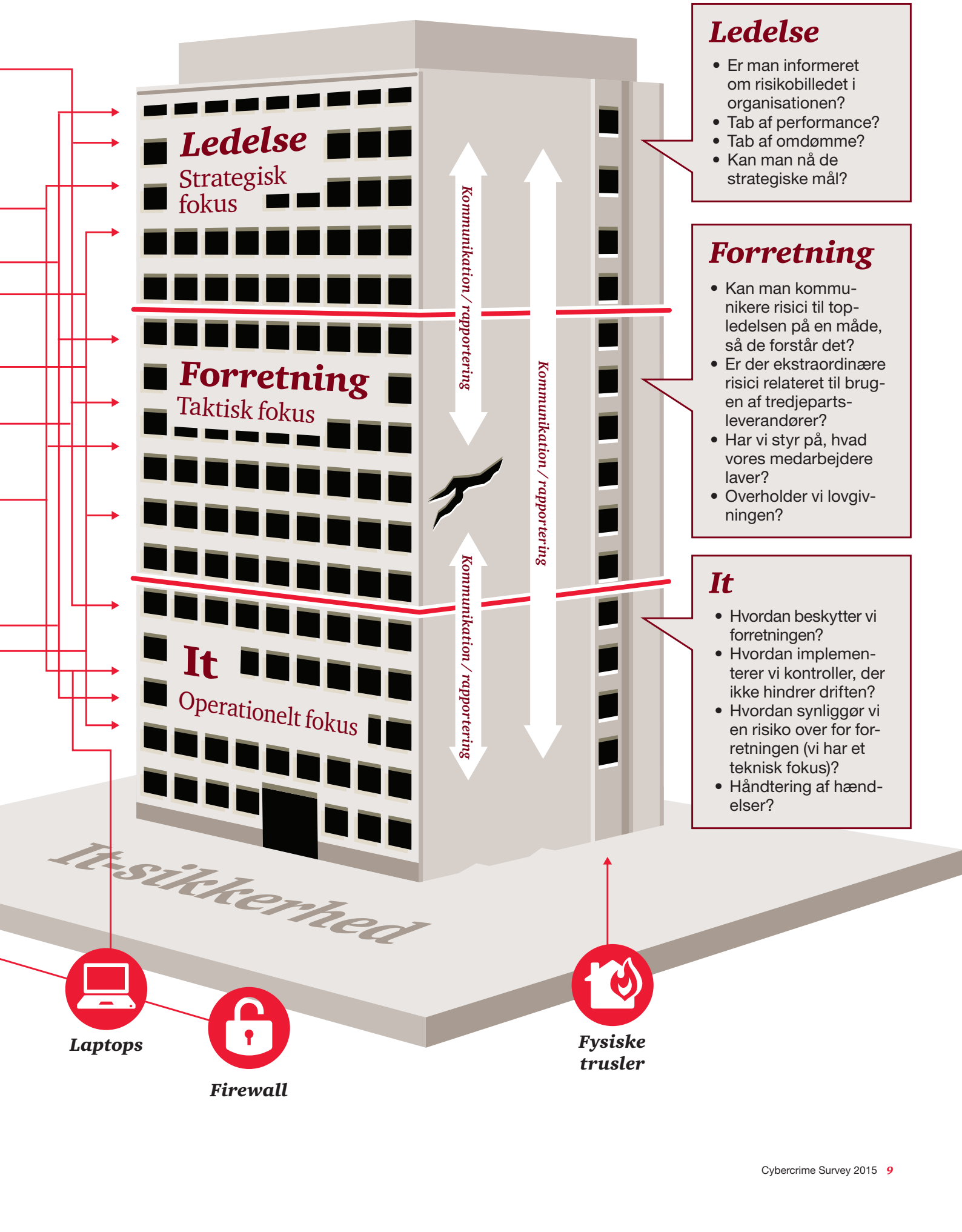
Topledere og bestyrelser er blevet mere opmærksomme på cybersikkerhed de seneste år, men hvor stor er deres konkrete involvering i arbejdet? 42 % af respondenterne mener, at direktionen ikke har tilstrækkeligt fokus på cybersikkerhed. I samme ånd vurderer 61 %, at virksomhedens bestyrelse ikke bruger nok tid på at drøfte cybersikkerhed på bestyrelsesmøder. Denne undersøgelse viser, at 33 % aldrig briefer topledelsen om it- og informationsrelaterede risici.

Dermed kan det være svært for ledelsen at sikre etablering af et passende sikkerhedsprogram, der tilgodeser ledelsens forventninger til risikostyring og en passende beskyttelse af virksomhedens vigtigste informationsaktiver.

Resultaterne er alarmerende i et perspektiv, hvor kunde- eller persondata kan kompromitteres. Tilsynsmyndigheder kan konkludere, at ledelsen ikke har skabt det rette kontrolmiljø, og at bestyrelsen ikke har ført tilstrækkeligt tilsyn. Det er derfor afgørende, at cybersikkerhed ses som en virksomhedsrisiko snarere end en it-udfordring, og at virksomheder kan vise deres interessenter, at de har forstået risikoens omfang og har etableret et kontrolmiljø og en governance-struktur, der adresserer udfordringen.

[2] 2015 US State of Cybercrime Survey.

Cybertruslen medfører udfordringer for alle lag i en organisation – lige fra den indledende vurdering af forretningskonsekvens til implementering og vedligeholdelse af de rette sikkerhedsmekanismer. Det er af afgørende betydning at have en sikkerhedsstrategi og en styringsform, der medvirker til løbende at synliggøre risikoen for ledelsen, så denne på et oplyst grundlag kan træffe de rette beslutninger, der sikrer, at forretningen og it-afdelingen kan implementere et passende sikkerhedsniveau. Vi anbefaler derfor, at virksomheder opretter et cybersikkerhedsprogram.



Ledelse

- Er man informeret om risikobilledet i organisationen?
- Tab af performance?
- Tab af omdømme?
- Kan man nå de strategiske mål?

Forretning

- Kan man kommunikere risici til topledelsen på en måde, så de forstår det?
- Er der ekstraordinære risici relateret til brugen af tredjepartsleverandører?
- Har vi styr på, hvad vores medarbejdere laver?
- Overholder vi lovgivningen?

It

- Hvordan beskytter vi forretningen?
- Hvordan implementerer vi kontroller, der ikke hindrer driften?
- Hvordan synliggør vi en risiko over for forretningen (vi har et teknisk fokus)?
- Håndtering af hændelser?

Hvordan prioriterer virksomhederne deres sikkerheds-investeringer?

Da medarbejderne ses som en af de største trusler mod virksomheden, kan ét af de vigtigste sikkerhedstiltag fremadrettet forventes at være interne awareness-aktiviteter. Derudover investerer virksomhederne i en række centrale områder:

- Styring af virksomhedernes brugere og begrænsning af deres adgange til systemer og data er en udfordring, som mange prioriterer med tiltag inden for bl.a. identity management, privilegeret adgangsstyring og mobilsikkerhed.
- Identifikation af systemsårbarheder og reducering heraf adresseres ved sårbarhedsscanninger og opgradering af gamle operativsystemer.
- Detektive kontroller som malware detection, intrusion detection og intelligent logning medvirker til, at man tidligt kan reagere på hændelser og tegn på ulovlig indtrængen.
- Anvendelsen af kendte standarder (som ISO 2700x og NIST) kan medvirke til, at man får en holistisk tilgang til sikkerhedsarbejdet og (for offentlige myndigheders vedkommende) overholder lovgivningen.

Højest prioriterede investering de næste 12 måneder

Awareness-træning	39,9 %
Mobil-sikkerhed	33,1 %
Opgradering/ udskiftning af gamle operativsystemer	32,6 %
Central og intelligent logning	32,0 %
Identity management	28,1 %
Metodeforankring som ISO 2700x eller NIST	27,0 %
Sårbarheds-scanninger	24,7 %
Privilegeret adgangsstyring	19,7 %
Malware detection	16,3 %
IDS – intrusion detection	15,2 %

Er din virksomhed forberedt?

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

1. Hvor modent er vores cybersikkerhedsprogram?
2. Er vores cybersikkerhedsprogram tilpasset vores forretningsstrategi?
3. Har vi de kompetencer, der skal til for at identificere de strategiske trusler mod forretningen samt potentielle angribere?
4. Kan vi forklare vores cybersikkerhedsstrategi for vores interessenter, investorer, samarbejdspartnere, kunder og andre tilsynsførende?
5. Ved vi, hvilke informationer der er mest kritiske for forretningen, og hvad angriberne vil gå efter?
6. Har virksomheden etableret et kriseberedskab, der kan styre os sikkert igennem en kompleks it-relateret hændelse?

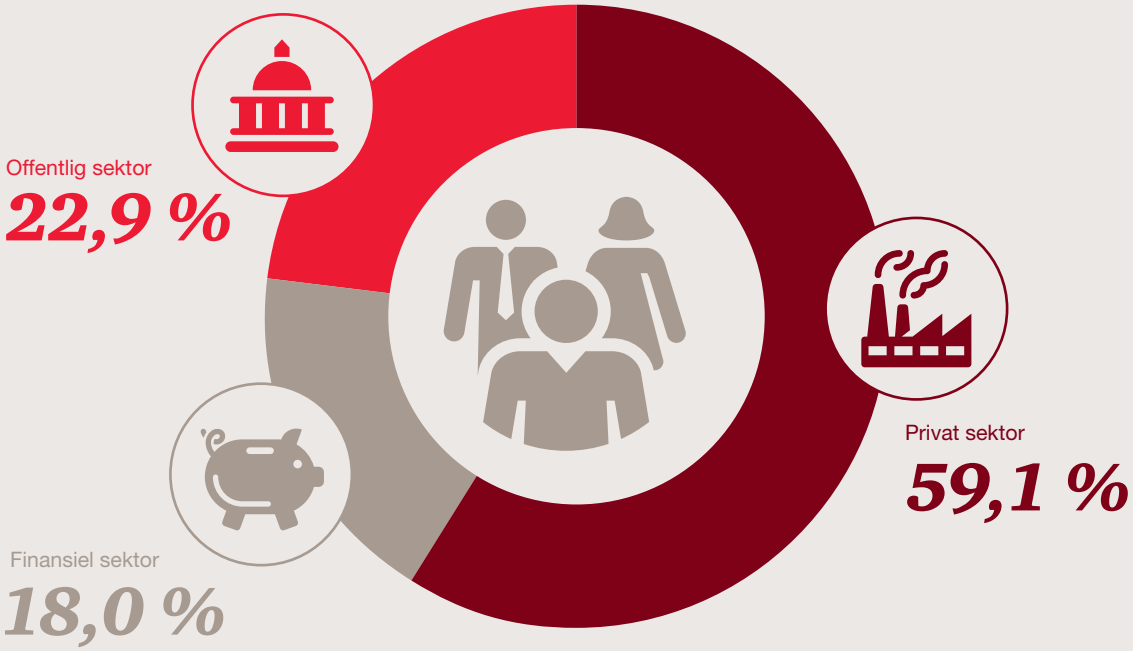
Om undersøgelsen

Denne undersøgelse er gennemført via internettet og sociale medier i perioden 1. maj til 31. juli 2015 blandt et bredt udsnit af PwC's kunder og relationer samt andre topledere og eksperter i målgruppen.

Desuden har en række brancheforeninger og -organisationer opfordret deres medlemmer eller kunder til at deltage i undersøgelsen, herunder DI ITEK, Finansrådet, CFIR, ISA-CA og Center for Cybersikkerhed. Resultaterne bygger på besvarelser fra i alt 249 respondenter fra danske virksomheder og offentlige organisationer, og besvarelserne kommer primært fra virksomhedsledere, it-chefer eller sikkerhedsspecialister.

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

Respondenternes fordeling på brancher



Få hjælp

Har din virksomhed brug for sparring omkring håndteringen af cybertruslen, så er vi klar til at hjælpe.

Mads Nørgaard Madsen
Partner og leder af Security & Technology, PwC's Consulting afdeling
M: 2811 1592
E: mxm@pwc.dk

William Sharp
Director, IT Risk Assurance/ Information Security
M: 4040 1074
E: wis@pwc.dk

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

Claus Bartholin
Senior manager, IT Risk Assurance/ Information Security
M: 2363 9921
E: cbt@pwc.dk