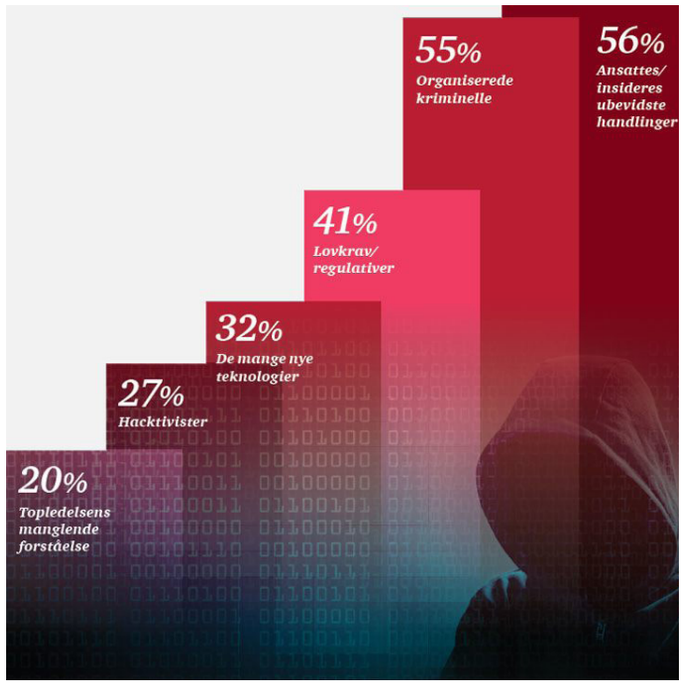
CYBERTRUSLEN BEKYMRER FLERE BESLUTNINGSTAGERE END TIDLIGERE



CYBERTRUSLEN BEKYMRER ERHVERVSLIVET OG OFFENTLIGE MYNDIGHEDER SOM ALDRIG FØR. PWC'S CYBERCRIME SURVEY 2017 VISER, AT FLERE ER MERE BEKYMREDE FOR CYBERTRUSLEN NU, END DE VAR ÅRET FØR. DEN STIGENDE BEKYMRING ER HELT REEL. 64 % AF RESPONDENTERNE I PWC'S CYBERCRIME SURVEY RAPPORTERER NEMLIG, AT DERES ARBEJDSPLADS HAR VÆRET UDSAT FOR HÆNDELSER ELLER ANGREB RELATERET TIL CYBERCRIME DET SENESTE ÅR.

Af de arbejdspladser, der er blevet ramt af cybertruslen, angiver 37 %, at de ikke blot har mistet penge som følge af hændelserne, men at de også har oplevet, at deres "brand" tog skade eller at kritiske systemer i deres forretning var utilgængelige i en længere periode. Ser man på andelen af dem, der er blevet ramt, er der et lille fald i forhold til 2016. Dog er der stadig tale om knap 2/3 af respondenterne, ligesom det fortsat er flere end i 2015, hvor 59 % svarede, at de var blevet ramt.
Der ses en tendens til, at cyberangreb i dag er mere avancerede, og man hører oftere om tilfælde i offentligheden, hvor virksomheder har mistet store summer i forbindelse med sikkerhedsbrud. Dette kan være med til at forklare, hvorfor Cybercrime Survey 2017 nu viser en stigning over de seneste tre år i andelen, som er bekymrede for cybertruslen. Det kan samtidig også være med til at forklare, at resultaterne trods alt viser et lille fald i den andel, som har været ramt af et cyberangreb, idet den øgede opmærksomhed på cybertruslen har ført til, at arbejdspladser i højere grad investerer i it-sikkerhed og dermed forebygger angreb. PwC's Cybercrime Survey 2017 viser desuden, at respondenterne forventer, at deres budgetter til cyber- og informationssikkerhed i gennemsnit øges med 25 % over de næste 18 måneder.

DEN STØRSTE TRUSSEL KOMMER INDE FRA

Respondenterne har vurderet nedenstående til at være det, der udgør de største cybertrusler for deres arbejdsplads i fremtiden. Ligesom året før er der 55 %, der peger på organiserede kriminelle som den største cybertrussel. Denne bliver dog overgået af en ny valgmulighed, nemlig ansattes/insideres ubevidste handlinger, som hele 56 % af de adspurgte mener udgør den største trussel. En bekymring for den nylige EU-persondataforordning har også sat sine spor. Dette ses ved, at 41 % af respondenterne – sammenlignet med 30 % i 2016 og 27 % i 2015 – peger på lovkrav og regulativer som en stor trussel i fremtiden. Ud over disse tre er nye teknologier, hacktivister og topledelsens manglende forståelse at finde på listen, hvilket også var tilfældet i 2016.
Bekymringen for ansattes/insideres ubevidste handlinger og organiserede kriminelle kan hænge sammen med det høje antal respondenter, som rapporterer at have været ramt af phishing* og afpresning. Blandt de respondenter, der har oplevet sikkerhedshændelser, har 77 % været udsat for phishing-angreb, mens 58 % har været udsat for afpresning.
*Phishing er ofte en mail, der er forsøgt kamufleret som en reel henvendelse. Den har til formål at få brugeren til at klikke på et link i mailen og få dem til at indtaste personoplysninger på et falsk site, som den kriminelle så kan misbruge. Alternativt planter e-mailen malware i systemet, når der klikkes på linket.

HVAD BØR VIRKSOMHEDERNE GØRE?

Cyberangrebene har vist, at de på få timer kan ødelægge teknologien i en virksomhed eller i et samfund, og de klassiske beredskabsøvelser tager ikke højde for en genskabelse af hele it-infrastrukturen i kølvandet på et cyberangreb. Derfor skal arbejdspladser tænke cybersikkerhed anderledes, end de gør i dag. Et kontrolskema kan ikke være det stærkeste værktøj i beskyttelsesfasen, og udviklingen kalder på et større fokus på under- og efter-fasen: Hvad gør man eksempelvis, hvis alle desktops i organisationen bliver ødelagt på få timer, hvordan får man så forretningen i gang igen? Man bør løbende afholde en cyberøvelse, hvor man tester sit beredskab. Vi ser i vores måling, at budgetterne til it-sikkerhed øges, og her er det vigtigt, at man finder en balance mellem investeringer i henholdsvis før-, under- og efter-fasen af et cyberangreb.
Der er behov for omstilling og handling, som gælder både staten, samfundet og erhvervslivet. Fx skal vi i højere grad forholde os til spørgsmål som: Hvordan sikres beskyttelse af borgernes data? Hvordan klædes børn og unge, som er fremtidens arbejdskraft, på til at kunne navigere i en mere digital verden? Hvordan sikrer virksomhederne, at de opnår den rette balance mellem investeringer og reelle udfordringer inden for it-sikkerhed? Og hvordan får arbejdspladser adgang til de kompetencer, de har brug for? En udfordring, som særligt bliver tydelig i PwC's Cybercrime Survey 2017, hvor over halvdelen af respondenterne planlægger at ansætte folk med it- og sikkerhedskompetencer, men meget få vurderer, at de i høj grad har adgang til dem. Hvis ikke man som ledelse prioriterer it-sikkerhed og har sikkerhedsfunktionen bemandet med tilstrækkelige og kompetente medarbejdere, står man med en meget stor udfordring. En udfordring, som er blevet endnu større, efter EU-persondataforordningen er trådt i kraft. Det er derfor vigtigt at tage fat på udfordringerne hurtigst muligt.

BESØG PWC OG LÆS MERE PÅ WWW.PWC.DK/CYBERSURVEY

DIGI 0101
MES 111 0
SEN 01 11