Uddannelses- og Forskningsministeriet

Prækvalifikation af videregående uddannelser - IT sikkerhed

Udskrevet 7. april 2026

Professionsbachelor (overbygning) - IT sikkerhed - UCL Erhvervsakademi og professionshøjskole

Institutionsnavn: UCL Erhvervsakademi og professionshøjskole
Indsendt: 01/02-2018 07:45
Ansøgningsrunde: 2018-1
Status på ansøgning: Godkendt
Afgørelsesbilag
Samlet godkendelsesbrev
Download den samlede ansøgning
Læs hele ansøgningen

Ansøgningstype

Nyt udbud

Udbudssted

Erhvervsakademi Lillebælt Odense

Kontaktperson for ansøgningen på uddannelsesinstitutionen

Anders Christian Frederiksen Specialkonsulent Tlf. (direkte): 65434584 Mobil: 23833822 E-mail: acfr@eal.dk

Er institutionen institutionsakkrediteret?

Påbegyndt

Er der tidligere søgt om godkendelse af uddannelsen eller udbuddet?

Nej

Uddannelsestype

Professionsbachelor (overbygning)

Uddannelsens fagbetegnelse på dansk fx. kemi

IT sikkerhed

Uddannelsens fagbetegnelse på engelsk fx. chemistry

IT security

Den uddannedes titel på dansk

Professionsbacheloruddannelsen i it-sikkerhed

Den uddannedes titel på engelsk

Bachelor in IT security

Hvilket hovedområde hører uddannelsen under?

It-faglige område

Hvilke adgangskrav gælder til uddannelsen?

For at blive optaget på uddannelsen, skal man have én af følgende uddannelser:

- Datamatiker
- IT-teknolog

Hvis man har en anden uddannelsesbaggrund, kan man eventuelt blive optaget på baggrund af en individuel vurdering.

Er det et internationalt uddannelsessamarbejde, herunder Erasmus, fællesuddannelse og lign.?

Nej

Hvis ja, hvilket samarbejde?

Hvilket sprog udbydes uddannelsen på?

Dansk

Er uddannelsen primært baseret på e-læring?

Nej

ECTS-omfang

90

Beskrivelse af uddannelsens formål og erhvervssigte

Uddannelsens mål er, at den færdiguddannede selvstændigt kan varetage arbejdet med at analysere, planlægge og vurdere it- sikkerhedsmæssige forhold ved drift, kontrol og udvikling i både private og offentlige virksomheder.

Uddannelsens struktur og konstituerende faglige elementer

Uddannelsen varer 1½ år og indeholder seks fagmoduler, en række valgmoduler, et praktikforløb og et afsluttende bachelorprojekt.

De seks fagmoduler er følgende:

- Introduktion til it-sikkerhed
- Sikkerhed i it-governance
- Systemsikkerhed
- Netværks- og kommunikationssikkerhed
- Softwaresikkerhed
- Videregående sikkerhed i it-governance

Valgmodulerne kan fx være:

- Network Penetration Testing
- Forensic Analysis
- Security Information and Event Management

På tredje semester skal man i praktik i en virksomhed. Her får man mulighed for at koble den teoretiske viden, man har fået på første og andet semester med praktisk erfaring. De studerende afprøver arbejdsområder og målretter deres uddannelse i forhold til deres karriereplaner.

Uddannelsen afsluttes med udarbejdelse af et bachelorprojekt.

Begrundet forslag til taxameterindplacering

ikke relevant

Forslag til censorkorps

Censorsekretariatet Porthusgade 1 – 9000 Aalborg – 7269 8700

Dokumentation af efterspørgsel på uddannelsesprofil - Upload PDF-fil på max 30 sider. Der kan kun uploades én fil.

cybercrime-survey-2017-rapport.pdf

Kort redegørelse for hvordan det nye udbud bidrager til at opfylde behovet for uddannelsen nationalt og/eller regionalt

Danmark er et af de mest digitaliserede lande i verden. Det betyder, at vi er sårbare over for bl.a. hackerangreb og cyberkriminalitet, der kan lamme vitale samfundsfunktioner og vores virksomheder. Det er derfor afgørende, at der er styr på it-sikkerheden, og at vi løbende tilpasser os udviklingen i trusselbilledet. Cyber- og informationssikkerhed har derfor høj prioritet for regeringen, som har besluttet at styrke indsatsen på området yderligere.

”Danmark er en digital frontløber, og det skal vi blive ved med at være. Men det er afgørende for den fortsatte digitalisering og ikke mindst borgernes tillid, at der er styr på it-sikkerheden, så vi er bedst muligt rustet til at imødegå truslen fra blandt andre it-kriminelle. Og de seneste måneders store hackerangreb har vist, at det er nødvendigt at styrke indsatsen. Derfor sætter vi ekstra 100 mio. kr. af til arbejdet med en ny strategi for cyber- og informationssikkerhed”, siger innovationsminister Sophie Løhde.

”Cybertrusler er en af vor tids største trusler, som både har sikkerhedspolitiske og samfundsøkonomiske konsekvenser for Danmark. Alvorlige cyberangreb vil kunne lamme centrale samfundsfunktioner som hospitaler og elforsyning. Det er derfor nødvendigt løbende at forholde sig til truslerne og forbedre sikkerheden. Den kommende strategi for cyber- og informationssikkerhed er en vigtig brik i det arbejde. Her styrker regeringen indsatsen yderligere med både flere penge, mere tid og stærkere koordination”, siger forsvarsminister Claus Hjort Frederiksen.

IT-sikkerhed er ikke kun et regeringsspørgsmål, men har også en vital betydning for at danske virksomheder kan overleve et angreb på virksomhedernes IT-systemer. Ifølge www.systemgruppen.dk rapporterede mellem 32-41% af alle virksomheder i 2015 om cyberkriminalitet på globalt plan. Dermed er IT-sikkerhed blevet og bliver i højere grad essentielt – og potentielt set en eksistentiel nødvendighed – for verdens virksomheder i takt med den voldsomme, stigende udvikling i cyberkriminalitet, som er et område, der er vokset fra at bestå af enkelte amatørhackere til at være en reel industri med velstrukturerede organisationer i besiddelse af aktiver, motivation, målsætninger og højtkvalificerede hackere, der udfører målrettede angreb.

Cyberkriminaliteten er således stigende i omfang og kompleksitet. Denne trend med øget, organiseret og mere kompleks cyberkriminalitet gør sig gældende på global plan, hvor virksomheder overvåget af IBM – ifølge systemgruppen.dk - i gennemsnit oplevede ca. 53 millioner cybersikkerheds episoder og en stigning i angreb på 64%. Det samlede antal angrebsforsøg mod verdens virksomheder er således et enormt antal, hvoraf op til 70% forbliver uopdaget, og hvor de avancerede angreb i gennemsnit tager 205 dage at opdage.Derudover detekterede Symantec i 2015 mere end 430 millioner nye, unikke malware, hvilket var 36% mere end året før, mens det samme tal hos Dell var 73% flere. Den samme tendens ses hos McAfee, hvis database nu tæller 650 millioner varianter. Grundet den store trussel fra cyberkriminalitet har World Economic Forum også vurderet risici relateret til cyberkriminalitet som værende den femte og sjette største globale risiko i 2017.

I Danmark og herunder også danske virksomheder er økonomien i høj grad afhængig af internetbaserede interaktioner. Ifølge Deloitte vurderes Danmark til at være det fjerde mest sårbare land i verden, når det gælder cyberkriminalitet. Danmark og danske virksomheder er således seks gange mere sårbare over for cyberangreb end de mindst sårbare Top 50 lande. Angrebsfladen er altså uhyggeligt bred, og der er stort set frit spil.

Deloittes analyse af Danmarks udsathed er i overensstemmelse med vurderingen fra Center for Cybersikkerhed, der er en del af Forsvarets Efterretningstjeneste. I deres trusselvurdering fra februar 2017 vurderer de, at truslen fra cyberspionage og – kriminalitet mod danske virksomheder er ”Meget Høj”. Dette er det højeste trusselsniveau og dækker over, at der findes en specifik trussel, der er kapacitet, hensigt samt planlægning, og at forestående angreb er helt sikre.

Underbygget skøn over det regionale behov for dimittender

Ifølge Computerworld rapporterede 21% af de danske virksomheder om cyberkriminalitet i 2011. I 2013 blev 36% af de danske virksomheder ramt af cyberangreb, i 2015 var det 59% virksomhederne, mens 69% havde oplevet angreb inden for de seneste 12 måneder i 2016. Denne udvikling ses på ejendom, personfølsomme data og produktions- og forretningshemmeligheder, forretningsafbrydelse (downtime), omsætningstab og skade på udstyr. 95% af omkostningerne til eksterne konsekvenser fordeles på Informationstab/-tyveri, forretningsafbrydelse og omsætningstab. Cyberkriminalitet har således en stor direkte konsekvens på virksomhedernes bundlinje og konkurrenceevne.

Cyberkriminalitet er også i Danmark en voksende trend, der ikke viser nogen tegn på at opbremsning. Alle typer og størrelser af virksomheder kan i dag blive ofre for cyberkriminalitet. I 2015 var 43% af alle angreb rettet mod de mindre og mellemstore virksomheder, som er karakteristisk for Region Syddanmark. Denne udvikling kan skyldes, at disse virksomheder har færre ressourcer til at forsvare sig med, og de kan bruges som springbræt til at angribe større virksomheder, der bruger dem som leverandører. Ydermere viser statistikken, at 60% af de små virksomheder, der har været udsat for et succesfuldt cyberangreb er gået konkurs efter seks måneder.

I IT branchen har man ikke haft tradition for at anmelde datakriminalitet. Denne tendens ser imidlertid ud til at ændre sig som det fremgår af den vedlagte pwc analyse.

Ifølge Fyns Politi er anmeldte tilfælde af databedrageri på Fyn steget fra 53 sager i 2012 til 1026 sager i 2016, og samtidig er opmærksomheden i forhold til sikkerhed stigende. Det fremgår bl.a. af Danmarks Statistik at der er sket en stigning fra 77 % til 83 % (fra 2015-2017) i antallet af virksomheder i Region Syddanmark, der har mere end 10 ansatte og som har implementeret én eller flere typer it-sikkerhedsmæssige foranstaltninger.

Ud fra Danmarks Statistiks analyser viser der sig følgende billede af virksomhederne i Region Syddanmark:

- Har en nedskrevet it-sikkerhedspolitik – i 2017: 45%
- Har retningslinjer for it-sikkerhed og databeskyttelse til medarbejdere – i 2017: 57%
- Har dataklassifikation (fx adgangsrettigheder) – i 2017 40%
- Har foretaget risikoanalyse – i 2017 39%
- Har grundlæggende sikkerhedstiltag (fx antivirus, firewall, back up) – i 2017: 79%
- Har avancerede sikkerhedstiltag (fx logs, penetrationstests, it-sikkerheds beredskab) – i 2017: 31%
- Har krav til leverandører vedr. it-sikkerhed og databeskyttelse – 2017: 42%
- Har andre it-sikkerhedsmæssige foranstaltninger – 2017: 29%
- Havde oplevet udfordringer ved at anvende it-sikkerhedsløsninger i foregående kalenderår – i 2017: 6%
- Havde brud på IT-sikkerheden i foregående kalenderår – 2017: 11%
- Indført nye maskiner eller udstyr indenfor de sidste 2 år - som indeholder it – i 2017: 63%
- Stigende niveau for investeringer i it-sikkerhed i foregående kalenderår – i 2017: 28%
- Uændret niveau for investeringer i it-sikkerhed i foregående kalenderår– i 2017: 65%

- Faldende niveau for investeringer i it-sikkerhed i foregående kalenderår – i 2017: 2%

Truslen rettes ikke kun mod enkelte industrier, men virksomheder fra alle brancher ses ramt af cyberkriminalitet. Dog er service-, retail-, sundheds-/medicin-, finans-, produktions-, teknologi- og informations-/kommunikationsvirksomheder særligt udsatte, netop brancher som er stærkt repræsenteret i Region Syddanmark med 37.781 virksomheder i 2015.

For at kunne håndtere cybertruslen er virksomhederne nød til at have adgang til de fornødne kompetencer. Men at finde den arbejdskraft, man har brug for, er ikke altid nemt viser PwC's CXO Survey 2017. Manglende adgang til kvalificeret arbejdskraft er den andenstørste bekymring blandt ledelseslaget. Ser man specifikt på adgangen til kompetencer inden for informations- og cybersikkerhed, så viser Cybercrime Survey 2017, at der er nogle udfordringer på kompetenceområdet:

- 56 % angiver, at de skal ud og hyre nye ansatte inden for informations- og cybersikkerhed inden for de næste 18 måneder.
- 37 % vurderer, at de i lav grad eller slet ikke har adgang til de kompetencer, de har brug for inden for området.
- 47 % vurderer, at de kun i nogen grad har adgang til de rette kompetencer, mens blot
- 16 % vurderer, at de i høj grad har adgang til de talenter og evner, de forventer at skulle bruge.

Det potentielle behov for professionsbachelorer i IT sikkerhed i Region Syddanmark er således meget stort, udviklingen i cyberkriminalitet i små og mellemstore virksomheder taget i betragtning.

Hvilke aftagere har været inddraget i behovsundersøgelsen?

Behovsanalysen som bl.a. danner baggrund for uddannelsen på nationalt plan er udarbejdet af PwC: https://www.pwc.dk/da/nyt/publikationer/cybercrime-survey-2017.html. Målingerne er gennemført med opbakning fra Finansrådet, Dansk Erhverv, Kita, IT-Branchen, Center for Cybersikkerhed, ISACA og DI Digital. Målingen bygger på onlinebesvarelser afgivet i perioden 1. maj til 14. august 2017. Respondenterne er bl.a. 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 meget de investerer i it-sikkerhed, hvordan deres virksomhed forholder sig til kommende samt gældende lovgivning på området mv. Virksomhederne kommer fra et bredt udsnit af brancher/ industrier/sektorer, herunder handel, den finansielle sektor, professionelle services og rådgivning, teknologi, industrielle virksomheder, offentlige institutioner, energi og forsyning, transport, pharma mv.

På regionalt plan har Erhvervsakademiet Lillebælts uddannelsesudvalg for Medie- og IT-området været involveret og anbefalet udbud i Odense. Uddannelsesudvalget består bl.a. af repræsentanter fra:

- Teknisk Landsforbund
- Dansk Erhverv
- HK
- Prosa

Virksomhedsnetværket Technology Denmark har desuden udarbejdet følgende udtalelse:

"Indstilling fra Technology Denmark vedr. PBA uddannelse i IT-sikkerhed, på Erhvervsakademiet Lillebælt. Technology Denmark er en interesseorganisation og et partnerskab mellem tech virksomheder, uddannelsesinstitutioner og offentlige myndigheder. Vi arbejder med at understøtte udviklingen af tech virksomheder med behov for højtkvalificerede IT-kompetencer. Derfor har vi et stort fokus på de uddannelser, der udvikler og uddanner studerende til at kunne matche arbejdsmarkedets behov. Tech virksomhederne i Danmark har konstant behov for veluddannede medarbejdere til at videreudvikle og flytte virksomheden til næste trin og behovene ændrer sig løbende. Technology Denmark bidrager til talentudvikling og understøtter at der bygges bro mellem uddannelserne og arbejdsmarkedet. Vi ser meget positivt på etableringen af nye IT-uddannelser, som kan bidrage til innovative løsninger og imødekommer behovet i virksomheder. Igennem de sidste år er efterspørgslen og behov for viden om IT-sikkerhed øget. En udvikling, der ikke vil mindskes på sigt. Derfor bakker vi op om at Erhvervsakademiet Lillebælt vil udbyde en uddannelse, som har fokus på IT-sikkerhed og vi hilser således uddannelsen velkommen."

Flere af vores praktikvirksomheder har været involveret i vores regionale behovsafklaring. I den sammenhæng har vi blandt andet fået følgende udtalelser fra virksomheder på Fyn:

”Jeg mener at der helt klart er behov for kandidater som har en professionsbachelor med specialisering i IT- sikkerhed, da fokus på netop dette område er i stærk stigning - ikke kun på grund af EU forordninger. Jeg ser helt klart beskæftigelsesmulighederne i de større virksomheder” udtaler Jesper Veber Jeppesen, Bygkontrol ApS, Svendborg

"Jeg ser klart et behov for uddannelsen i IT-Sikkerhed. IT-sikkerhed er kommet mere i fokus og derfor mener jeg at der er jobmuligheder for kandidater også i virksomheder som vores” udtaler Stig Wulff Christensen, INFOWISE ApS, Odense

”En overbygningsuddannelse, som giver ekstra, nyttige kompetencer inden for IT-sikkerhed, kan kun gavne branchen. Jeg ser jobmulighederne især i de lidt større virksomheder, men selv de mindre virksomheder har behov for viden inden for IT sikkerhedsområdet”, udtaler Morten Møller, LET Software ApS, Odense

”En overbygningsuddannelse med det skitserede indhold er absolut relevant. Med de skærpede krav til IT sikkerhed, ser jeg klart jobmuligheder for kandidater, ikke mindst i produktionsvirksomhederne” udtaler Kim Sneum Madsen, UMBRACO A/S, Odense

”Uddannelsen er relevant for alle, som skal beskæftige sig med udvikling og produktion i IT branchen. Uddannelsens indhold er meget relevant, og jeg forventer at der vil være et godt jobmarked for kandidaterne” udtaler Yoel Caspersen, Kviknet.dk ApS, Odense

Beskriv ligheder og forskelle til beslægtede uddannelser, herunder beskæftigelse og eventual dimensionering.

Professionsbacheloruddannelsen IT - sikkerhed er en professionsbachelor uddannelse på niveau 6. Uddannelsen er - ifølge Uddannelsesguiden- beslægtet med følgende uddannelser:

Diplomuddannelsen IT Sikkerhed, som er en professions efteruddannelse på niveau 6

Teknologisk diplomuddannelse: It-diplomuddannelse (TD), som er en akademisk efteruddannelse på niveau 6

Kandidatuddannelsen Datalogi, som er en akademisk uddannelse på niveau 7

Kandidatuddannelsen Sofware Engineering, som er en akademisk uddannelse på niveau 7

Som det fremgår af ovenstående oversigt findes der to uddannelsestilbud på niveau 6:

1. Diplomuddannelsen IT Sikkerhed

2. Teknologisk diplomuddannelse: It-diplomuddannelse (TD)

Begge disse uddannelser er dog efteruddannelser og henvender sig derfor til en anden målgruppe end fuldtidsuddannelsen Professionsbachelor i IT-Sikkerhed.

Rekrutteringsgrundlag og videreuddannelsesmuligheder
Rekrutteringsgrundlag:

På nuværende tidspunkt udbydes uddannelsen udelukkende i København og Århus. Der er således ifølge uddannelsesguiden ikke udbud af fuldtidsuddannelsen i Region Syddanmark. Diplomuddannelsen, som er en deltidsuddannelse udbydes også kun i København og Århus. Herudover udbydes en deltidsuddannelse, IT-diplomuddannelse, i Horsens og i Ballerup.

Det naturlige rekrutteringsgrundlag for uddannelsen er nyuddannede, som har bestået én af følgende uddannelser:

- Datamatiker
- It-teknolog

Begge uddannelser udbydes af Erhvervsakademiet Lillebælt.

I Region Syddanmark udbydes IT teknolog udelukkende i Odense. IT – teknologerne har på nuværende tidspunkt mulighed for at videreuddanne sig med overbygningsuddannelserne Produktudvikling og teknisk integration, samt Innovation og Entrepreneurship.

Datamatiker uddannelsen udbydes i Region Syddanmark i Vejle og Odense. Herudover udbydes den i Esbjerg og Sønderborg. Datamatikere har i Region Syddanmark top-up mulighed inden for professionsbacheloruddannelse i: Innovation og entrepreneurship, Webudvikling, Softwareudvikling eller Digital konceptudvikling.

Ca. 20% af de færdiguddannede datamatikere og 16% af IT-teknologerne fra Erhvervsakademiet Lillebæt er uden beskæftigelse. Top up uddannelsen kunne således også være et alternativ for denne gruppe dimittender.

Videreuddannelsesmuligheder:

Man vil have mulighed for at udbygge sin viden med en videregående uddannelse på deltid, som man senere kan tage sideløbende med et arbejde. Det kan være en diplomuddannelse eller en masteruddannelse. Efter en konkret vurdering kan man også have mulighed for optagelse på en kandidatuddannelse.

Forventet optag på de første 3 år af uddannelsen

25 studerende pr. år

Hvis relevant: forventede praktikaftaler

På baggrund af den store interesse for uddannelsen blandt både private og offentlige virksomheder, og på baggrund af erhvervsakademiets store kontaktflader blandt virksomheder og hidtidige gode erfaringer med at skaffe praktikpladser forventes det ikke at blive et problem at skaffe 25 praktikpladser årligt.

Øvrige bemærkninger til ansøgningen

Hermed erklæres, at ansøgning om prækvalifikation er godkendt af institutionens rektor

Ja

Status på ansøgningen

Godkendt

Ansøgningsrunde

2018-1

Afgørelsesbilag - Upload PDF-fil

C1 Foreløbig godkendelse af professionsbachelor i It-sikkerhed.pdf

Samlet godkendelsesbrev - Upload PDF-fil

Orientering til UCL - Godkendelse af nyt udbud - PBO it-sikkerhed.pdf

***Danmark og cybersikkerhed:** Cybertruslen bekymrer flere end tidligere, og vi ser et skærpet fokus på den kommende EU-persondataforordning*

Cybercrime Survey 2017

Oktober 2017

pwc

250 danske og 100 norske virksomhedsledere, it-chefer og it- og sikkerhedsspecialister har delt deres syn på forskellige forhold i relation til cyberkriminalitet. De har bl.a. taget stilling til trusselsbilledet, samt hvorvidt de er klar til at efterleve kravene i den nye EU-persondataforordning.

77%

af respondenterne har været udsat for såkaldte phishing-angreb.

74%

af de adspurgte er mere bekymrede for cybertruslen nu, end de var for 12 måneder siden.

70%

vil investere i at overholde den kommende EU-persondataforordning.

Cybercrime Survey 2017

Cybercrime: Udviklingen kræver omstilling og handling – nu

Den teknologiske og digitale udvikling foregår eksponentielt, og mange virksomheder skal i højere grad omstille sig til at prioritere de øgede krav til sikkerhed, som den teknologiske og digitale udvikling fordrer.

Cybertruslen bekymrer erhvervslivet som aldrig før; 74 % af respondenterne i PwC's Cybercrime Survey 2017 svarer således, at de er mere bekymrede for cybertruslen nu end tidligere, hvilket er det højeste, siden vi gennemførte målingen første gang i 2015. Og intet tyder på, at fremtidens udfordringer bliver mindre. Skandinavien har i høj grad været ramt af ransomware og CEO fraud, og angrebene tager til i omfang. Der er nu ikke længere udelukkende tale om kriminelle, der forsøger at lokke penge fra virksomhederne; angrebene har nu også til formål at ødelægge forretningen. PwC's Cybercrime Survey 2017 viser fx, at de virksomheder, der har været ramt af en cyberhændelse, ikke blot har mistet penge, men at deres brand har taget skade, de har mistet kunder, og/eller kritiske systemer har været utilgængelige i en længere periode.

Ser man derudover på de hændelser, der sker i offentligheden, så ses der en tendens til, at disse bliver mere ekstreme og strækker sig ud over det materielle – tænk fx på, når hospitaler får lukket alt it-udstyr ned og af den grund ikke kan tage imod patienter – angreb, som potentielt kan have alvorlige konsekvenser for mennesker.

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 virksomhederne 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 fx, hvis alle virksomhedens desktops 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 som virksomhed 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 virksomhederne 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 virksomhed prioriterer it-sikkerhed og har sikkerhedsfunktionen bemandet med tilstrækkelige og kompetente medarbejdere, står man med en meget stor udfordring. En udfordring, som bliver endnu større, når EU-persondataforordningen træder i kræft i maj 2018. Det er derfor vigtigt at tage fat på udfordringerne hurtigst muligt.

I PwC vil vi gerne være med til at bidrage til cybercrime-agendaen for at belyse et område af stigende væsentlighed – for virksomheder og mennesker. Det kan vi kun lykkes med i fællesskab med erhvervslivet og samfundsaktører. Derfor skal der også lyde en stor tak til alle dem, der har givet sig tid til at dele deres indsigt og erfaringer via PwC's Cybercrime Survey 2017.

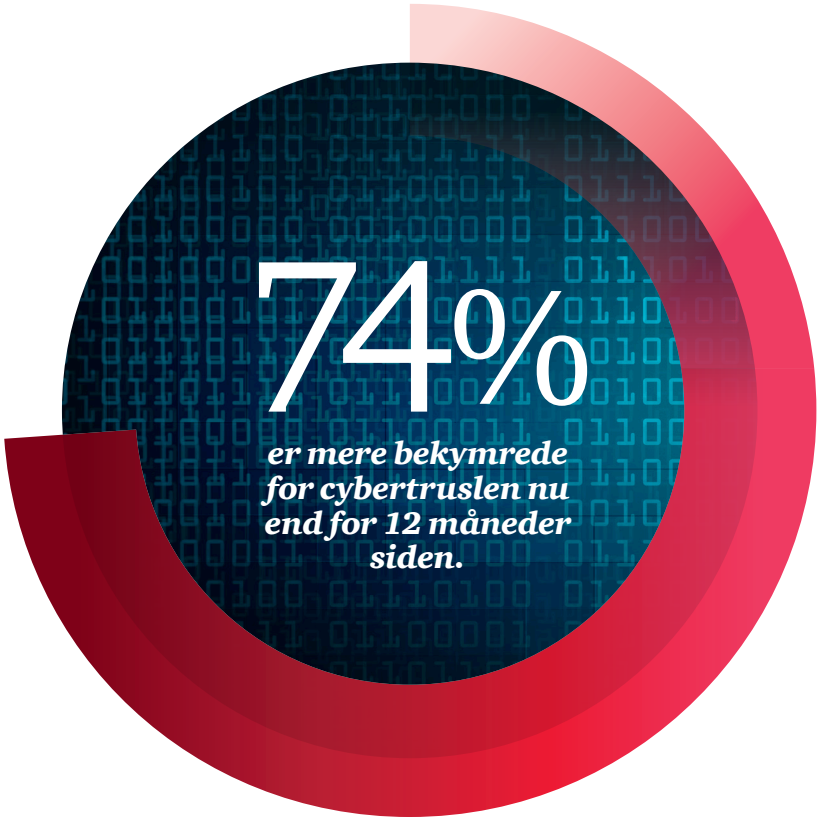
Mads Nørgaard Madsen
Partner
Security & Technology

64%

af virksomhederne har været udsat for cybercrime de seneste 12 måneder.

37%

af de ramte virksomheder mistede ikke blot penge som følge af cyberhændelserne, deres brand tog skade, de mistede kunder, og/eller kritiske systemer var utilgængelige.



Cybertruslen bekymrer flere end tidligere

Cybertruslen bekymrer erhvervslivet som aldrig før. 74 % af respondenterne svarer således, at de er mere bekymrede for cybertruslen nu, end de var for 12 måneder siden. Dette er højere end i både 2016 og 2015, hvor henholdsvis 65 % og 68 % svarede det samme. Den stigende bekymring er ikke ubegrundet. Hele 64 % af respondenterne rapporterer nemlig, at deres virksomhed har været udsat for hændelser eller angreb relateret til cybercrime de seneste 12 måneder. Af de ramte virksomheder angiver 37 %, at de ikke blot har mistet penge som følge af cyberhændelserne, men at de også har oplevet, at deres brand tog skade, at de mistede kunder, eller at kritiske systemer var utilgængelige i en længere periode. Ser man på andelen af dem, der er blevet ramt, er der et lille fald i forhold til de 69 %, der rapporterede, at de havde været ramt af cyberangreb i 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 havde været ramt.

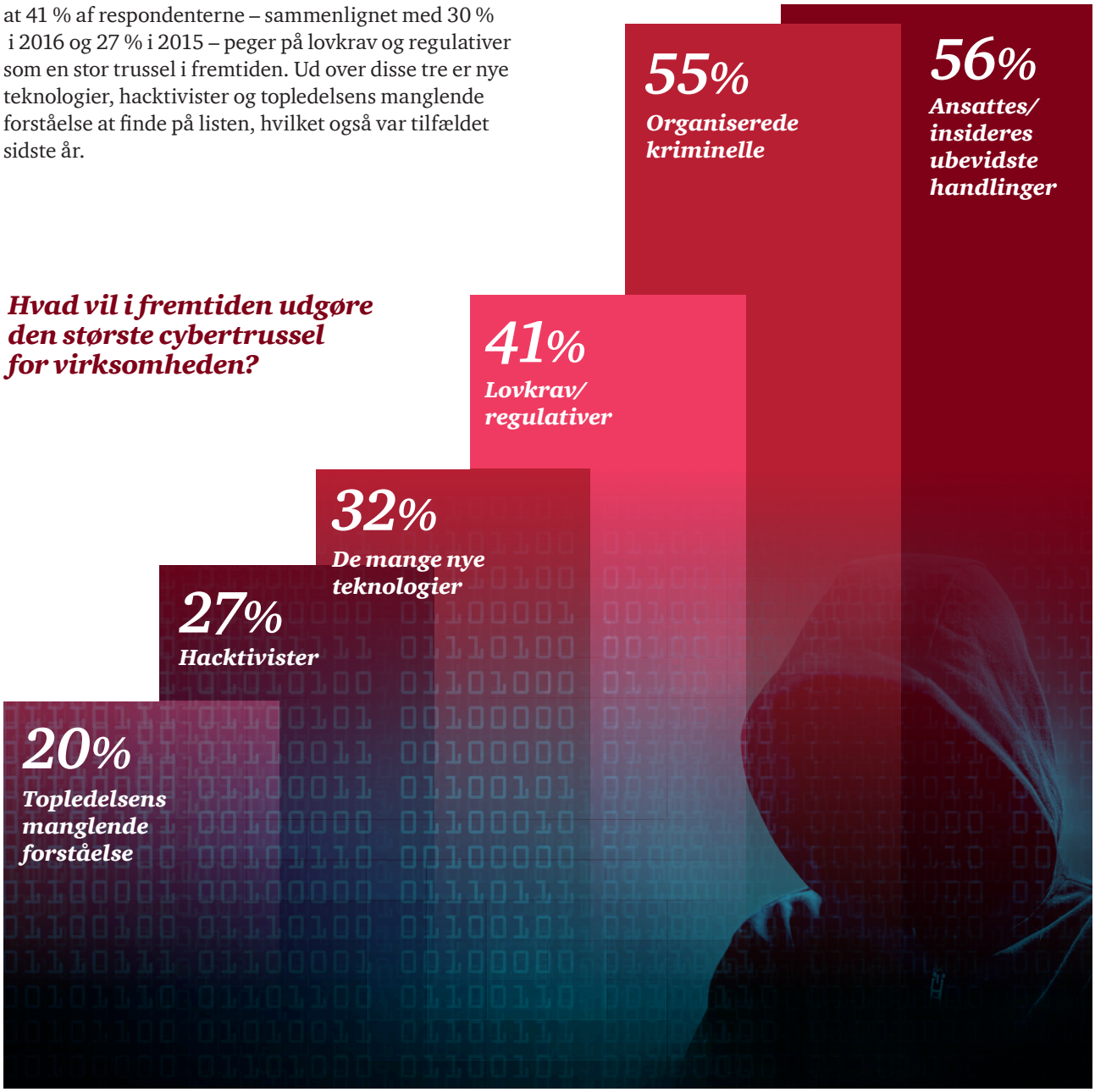
Der ses en tendens til, at cyberangreb i dag er mere avancerede, og man hører oftere om tilfælde i offentligheden, hvor virksomheder har mistet store summer i forbindelse med sikkerhedsbrud. Dette kan være med til at forklare, hvorfor Cybercrime Survey 2017 viser en stigning over de seneste tre år i andelen, som er bekymrede for cybertruslen. Det kan samtidig også være med til at forklare, at resultaterne trods alt viser et lille fald i andelen, som angiver, at deres virksomhed har været ramt af et cyberangreb, idet den øgede opmærksomhed på cybertruslen kan give anledning til, at virksomhederne i højere grad investerer i it-sikkerhed og dermed forebygger angreb. Denne tendens viste PwC's CXO Survey 2017, hvor andelen af dem, der har valgt it-sikkerhed som et af deres fem primære investeringsområder, er steget 13 procentpoint til 30 % mod 17 % i 2016. 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.

Ansattes/insideres ubevidste handlinger udgør den største trussel

I år har respondenterne vurderet nedenstående til at være det, der vil udgøre de største cybertrusler for deres virksomhed i fremtiden. Ligesom sidste år er der 55 %, der peger på organiserede kriminelle som den største cybertrussel for deres virksomhed. Denne bliver dog overgået i år af en ny valgmulighed, nemlig ansattes/insideres ubevidste handlinger, som hele 56 % af de adspurgte mener udgør den største trussel. En bekymring for den kommende EU-persondataforordning sætter også sine spor i år. 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 sidste år.

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.

Hvad vil i fremtiden udgøre den største cybertrussel for virksomheden?



*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.

Cyberangreb har økonomiske konsekvenser for virksomhederne

64 % svarer, at de har været udsat for hændelser eller angreb relateret til cyberkriminalitet de seneste 12 måneder. En stor andel af disse hændelser har haft økonomiske konsekvenser for virksomhederne. Således angiver mere end hver anden (53 %) af de ramte respondenter, at deres virksomhed har haft økonomiske omkostninger som følge af et cyberangreb. 42 % rapporterer om øgede omkostninger til udbedring og efterforskning af cyberhændelser, og hver femte respondent har oplevet stigninger på 16 % eller mere i forhold til sidste år, når det kommer til omkostninger til udbedring og efterforskning af cyberhændelser.

1 ud af 10 respondenter meddeler desuden, at deres totale omkostninger det seneste år, som følge af cyberangreb, overstiger 1 mio. kr. Omkostningerne ved et cyberangreb eller -hændelse kan variere meget, men baseret på svarene i Cybercrime Survey 2017 er et estimat, at den gennemsnitlige årlige omkostning for en dansk virksomhed, forbundet med cyberhændelser og -angreb, ligger på knap 900.000 kr.

Også i 2017 har Danmark været hårdt plaget af bølger af finansielt motiverede cyberangreb. 58 % af de virksomheder, der har været ramt af cyberangreb, har været ramt af afpresningsangreb eller såkaldt ransomware. 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. Samtidig rapporterer over halvdelen af respondenterne (52 %), at de har været ramt af finansiel svindel som fx "CEO fraud", hvor angriberen udgiver sig for at være et højtstående medlem af organisationen og anmoder om overførsler af virksomhedens midler til angriberens konti. Dette er en markant stigning i forhold til 2016, hvor kun 23 % af respondenterne rapporterede at have været ramt af finansiel svindel. 77 % har været ramt af phishing-angreb.

Phishing

77%

af respondenterne har været ramt af phishing-angreb

PwC anbefaler ...

at medarbejderne i organisationen løbende gennemgår awareness-træning, da phishing-forsøg oftest sker ved, at en medarbejder modtager en inficeret e-mail. Dette kan kobles med at teste organisationen uden konsekvenser ved at benytte sig af såkaldte "positive phishing".

Ransomware

58%

af respondenterne har været ramt af ransomware-angreb

PwC anbefaler ...

at man ved ransomware-sager sidestiller angreb med en sikkerhedshændelse. Det vil sige, at man straks bør kontakte sin sikkerhedsafdeling, hvis man har mistanke om et angreb, så man kan håndtere sagen med mindst mulig skade for forretningen.

CEO fraud

52%

af respondenterne har været ramt af CEO fraud

PwC anbefaler ...

at virksomheder benytter sig af ledelsesspecifik awareness-træning i kraft af ledelsens udsatte position i henhold til risiko for cyberkriminalitet. Derudover anbefaler vi, at organisationen reviewer sine procedurer for godkendelse af større beløb.

Topledelsens manglende forståelse for cybertruslen bekymrer

Det er tankevækkende, at kun 32 % af respondenterne i PwC's Cybercrime Survey 2017 svarer, at de mener, at topledelsen i høj grad har fokus på at opnå den rette balance mellem de trusler, organisationen står over for, og virksomhedens investeringer i cybersikkerhed. Det er status quo i forhold til sidste år, på trods af at der de seneste år har været en lang række alvorlige sager om cybercrime, og at PwC's CXO Survey 2017 viser, at cybercrime og manglende it-sikkerhed er CXO-lagets største bekymring.

PwC's Cybercrime Survey 2017 viser dog, at respondenterne forventer en gennemsnitlig budgetforøgelse på 25 % i budgetterne til cyber- og informationssikkerhed. Ledelsen har altså fokus på at nedbringe risici for organisationen, men famler måske en anelse i blinde, når det kommer til udførelsen. For selvom investeringslysten stiger, kan det være en udfordring for ledelsen at træffe den rigtige prioritering i kraft af det manglende fokus – man kan reelt investere uendeligt i sikkerhed. Det kræver tæt dialog mellem ledelsen og den sikkerhedsansvarlige – en løbende dialog, der ikke ser ud til at være etableret. 37 % af respondenterne rapporterer, at virksomhedens sikkerhedsansvarlige kun informerer ledelsen om risici ved cybertrusler en gang om året eller sjældnere. 10 % af respondenterne rapporterer sågar, at dette aldrig sker. Og netop topledelsens manglende forståelse er grundlag for bekymring. Respondenterne har i år vurderet topledelsens manglende forståelse som den sjettestørste trussel for deres virksomhed i fremtiden.

Kommunikationen om cyberrisici mellem bestyrelse og ledelse ser også ud til at være mere eller mindre fraværende. 66 % af respondenterne, tilhørende ledelseslaget, rapporterer nemlig, at organisationens bestyrelse kun i mindre grad eller slet ikke bruger tid på at drøfte problemstillinger vedrørende cyber- og informationssikkerhed på bestyrelsesmøderne.

PwC anbefaler ...

at man fokuserer på at sikre den rette kommunikation mellem ledelse og sikkerhedsrådgiver, så risici benyttes i prioriteringsarbejdet.

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.

Bekymring over mangel på arbejdskraft

For at kunne håndtere cybertruslen er virksomhederne nødt til at have adgang til de fornødne kompetencer. Men at finde den arbejdskraft, man har brug for, er ikke altid nemt. I PwC's CXO Survey 2017 er den andenstørste bekymring blandt ledelseslaget manglende adgang til kvalificeret arbejdskraft. Og ser man specifikt på adgangen til kompetencer inden for informations- og cybersikkerhed, så viser Cybercrime Survey 2017, at der er nogle udfordringer her. 56 % angiver, at de skal ud og hyre nye ansatte inden for informations- og cybersikkerhed inden for de næste 18 måneder. Samtidig vurderer knap 4 ud af 10 (37 %), at de i lav grad eller slet ikke har adgang til de kompetencer, de har brug for inden for området. 47 % vurderer, at de kun i nogen grad har adgang til de rette kompetencer, mens blot 16 % vurderer, at de i høj grad har adgang til de talenter og evner, de forventer at skulle bruge.

EU-persondataforordningen trækker mange ressourcer

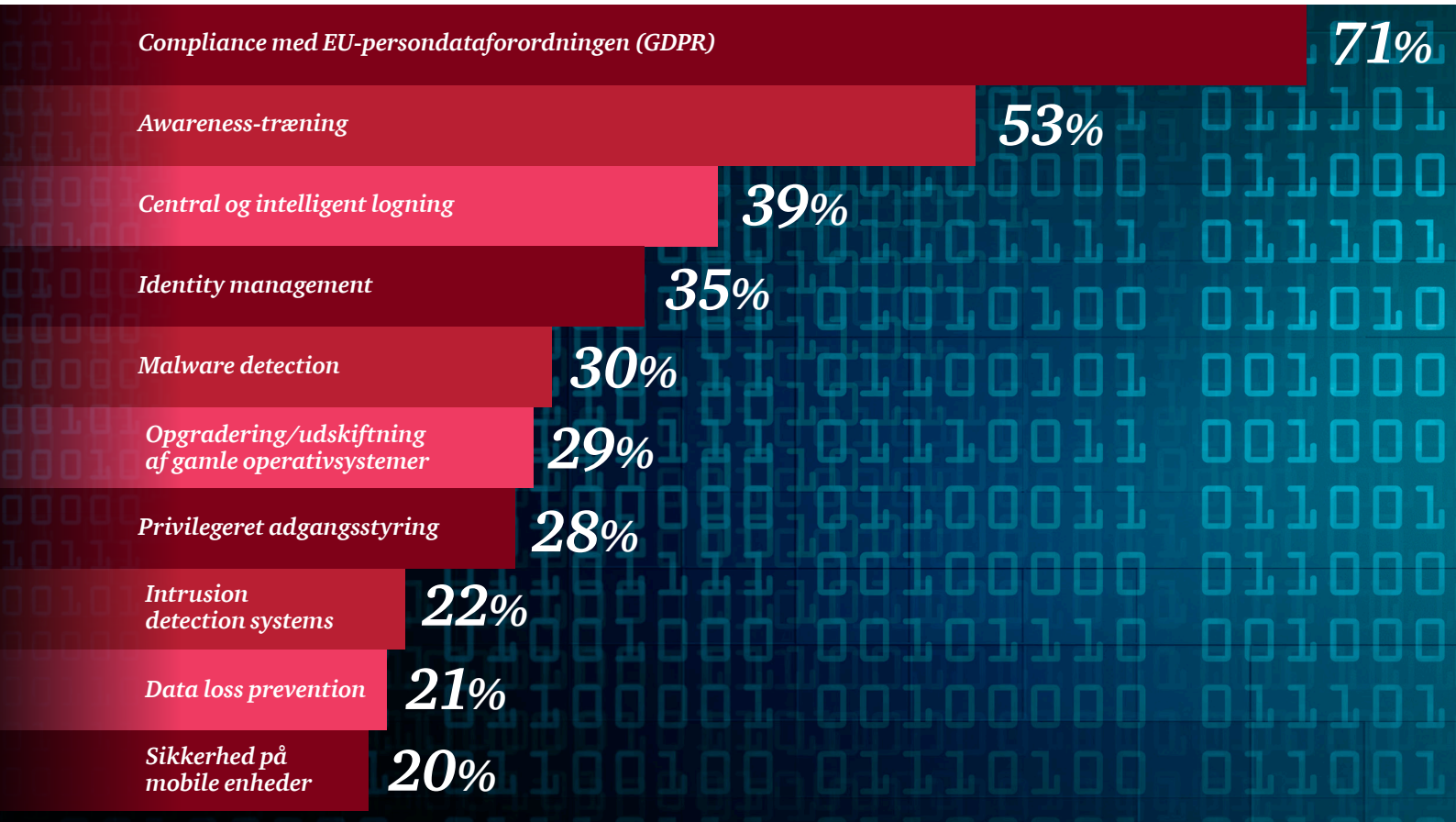
Årets højdespringer inden for sikkerhedsinvesteringer er investering i overholdelse af den kommende EU-persondataforordning. 71 % af respondenterne forventer at investere i netop dette i det kommende år. Persondataforordningen er en kompleks størrelse og rammer på tværs af organisationen. Derfor er det naturligt, at så mange respondenter forventer at sætte ressourcer af til at imødekomme kravene.

Awareness-træning er igen i år et område, der prioriteres højt, hvilket kan hænge sammen med den store bekymring for ansattes/insideres ubevidste handlinger og den høje andel af organisationer, der rammes af bl.a. phishing-angreb. Det kræver kun én enkelt uforsigtig eller uopmærksom medarbejder, der klikker på det forkerte link, for at udrette stor skade på organisationen.

Noget andet, som adskiller sig fra sidste års sikkerhedsinvesteringer, er, at opgradering eller udskiftning af gamle operativsystemer, som er en ny valgmulighed, optræder i top-10 (valgt af 29 %). At knap en tredjedel har peget på denne som en af deres højest prioriterede investeringer kan forklares med den seneste bølge af cyberangreb set i offentligheden, hvor kriminelle udnytter sårbarheder i gamle systemer til at foretage et angreb. Ofte er de gamle systemer enten ikke opdaterede, eller også er de ikke længere understøttet af leverandøren, hvorfor de udgør en risiko for organisationen.

Flere af de top-10-prioriterede investeringer adresserer centrale grundpiller inden for cybersikkerhed. Områder såsom malware detection, intrusion detection-systemer og data loss prevention er essentielle som led i at beskytte sig mod angreb samt i at mindske den skade, som et cyberangreb kan gøre på en organisation. Endvidere er disse elementer også gode sikkerhedstiltag, der medvirker til at sikre compliance med den kommende EU-persondataforordning.

Højest prioriterede investeringer de næste 12 måneder – 2017/2018



Mange virksomheder forventer at være klar til persondataforordningen

EU-persondataforordningen er blandt de adspurgte vurderet til at være den tredjestørste trussel for virksomhederne i de kommende 12 måneder – kun overgået af organiserede kriminelle og ansattes/insideres ubevidste handlinger. Den kommende EU-persondataforordning træder i kraft i maj 2018 og medfører en risiko for bødekrav på op til 4 % af omsætningen eller 20 mio. euro for de virksomheder, der ikke overholder kravene i forordningen, herunder krav til sikkerheden.

Ca. 60 % af respondenterne vurderer, at de i høj grad vil være i stand til at beskytte deres følsomme data i overensstemmelse med persondataforordningen, når den træder i kraft. Dette kan kobles sammen med, at overholdelse af kravene i forordningen er den højest prioriterede investering for virksomhederne det næste års tid. Til sammenligning er det kun ca. 32 % af respondenterne, der vurderer, at de i høj grad beskytter deres data i henhold til den gældende danske persondatalovgivning.

Selvom en stor del af virksomhederne vurderer, at de i høj grad vil være i stand til at beskytte deres personfølsomme data i overensstemmelse med persondataforordningen, rapporterer hver femte respondent, at deres virksomhed i mindre grad eller slet ikke vil være i stand til at beskytte deres følsomme data i henhold til kravene i EU-persondataforordningen, når den træder i kraft. Disse virksomheder vil derfor være i fare for at blive idømt store bøder for – bevidst eller ubevidst – at forbryde sig mod kravene i forordningen.

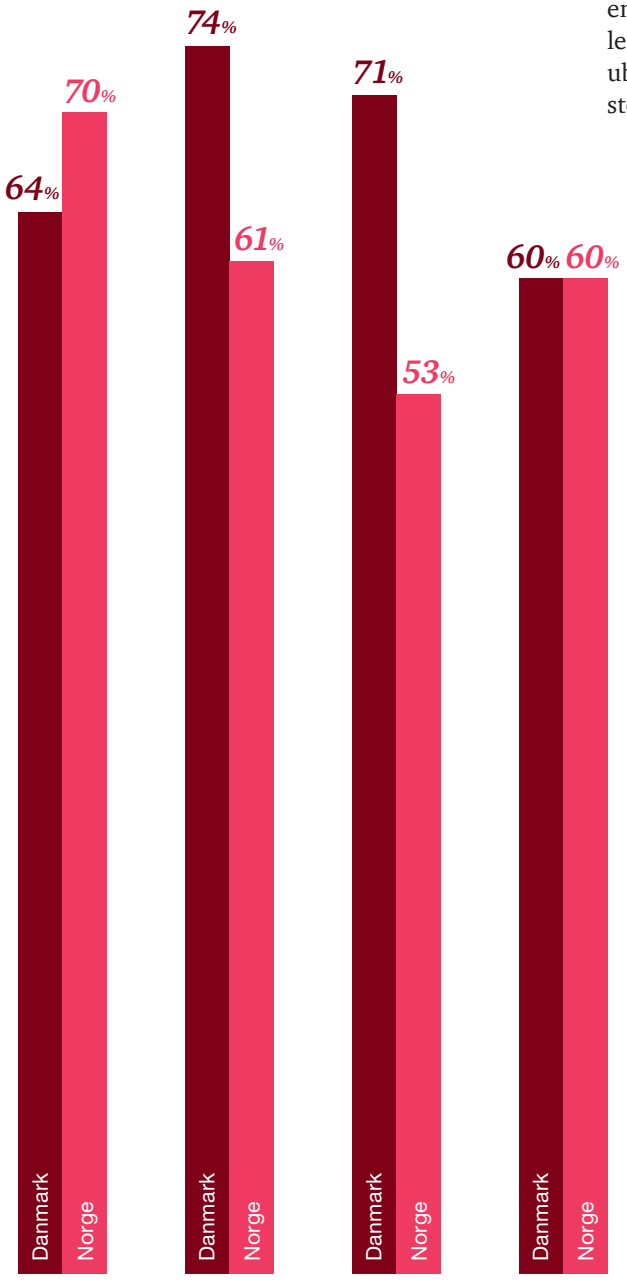
PwC anbefaler ...

at man opstarter et projekt, der kører i flere parallelle spor. Disse spor skal dække det styringsmæssige, de juridiske-, holdnings- og uddannelsesmæssige processer, it-sikkerhed samt det it-tekniske. Projektet vil være meget omfattende og komplekst, så fokusér på en stram styring via en projektleder, og sørg for opbakning fra topledelsen. Selvom der har været meget snak om EU-persondataforordningen, så er der behov for, at projektdeltagerne, der skal arbejde med projektet, får en dybere forståelse og viden om de reelle krav, som forordningen stiller til virksomheden.

Lignende tendenser i Norge

Igen i år har norske erhvervsfolk deltaget i PwC's Cybercrime Survey 2017. Knap 100 norske erhvervsfolk har givet deres svar, og der tegner sig generelt set en tendens, når vi sammenligner de norske svar med de danske. Både i Norge og i Danmark har man fokus på den kommende EU-persondataforordning, og det er den højest prioriterede investering i begge lande.

I begge lande svarer 60 % endda, at de i høj grad vil være i stand til at beskytte deres følsomme data i overensstemmelse med EU-persondataforordningen, når den træder i kraft. Det interessante er, at bekymringen for cybertruslen i fremtiden er en del højere i Danmark. Og til forskel fra Danmark er det de organiserede kriminelle, der bekymrer nordmændene mest, men dog en del mindre end det ses blandt de danske topledere, som har ansattes/insideres ubevidste handlinger som deres største bekymring.



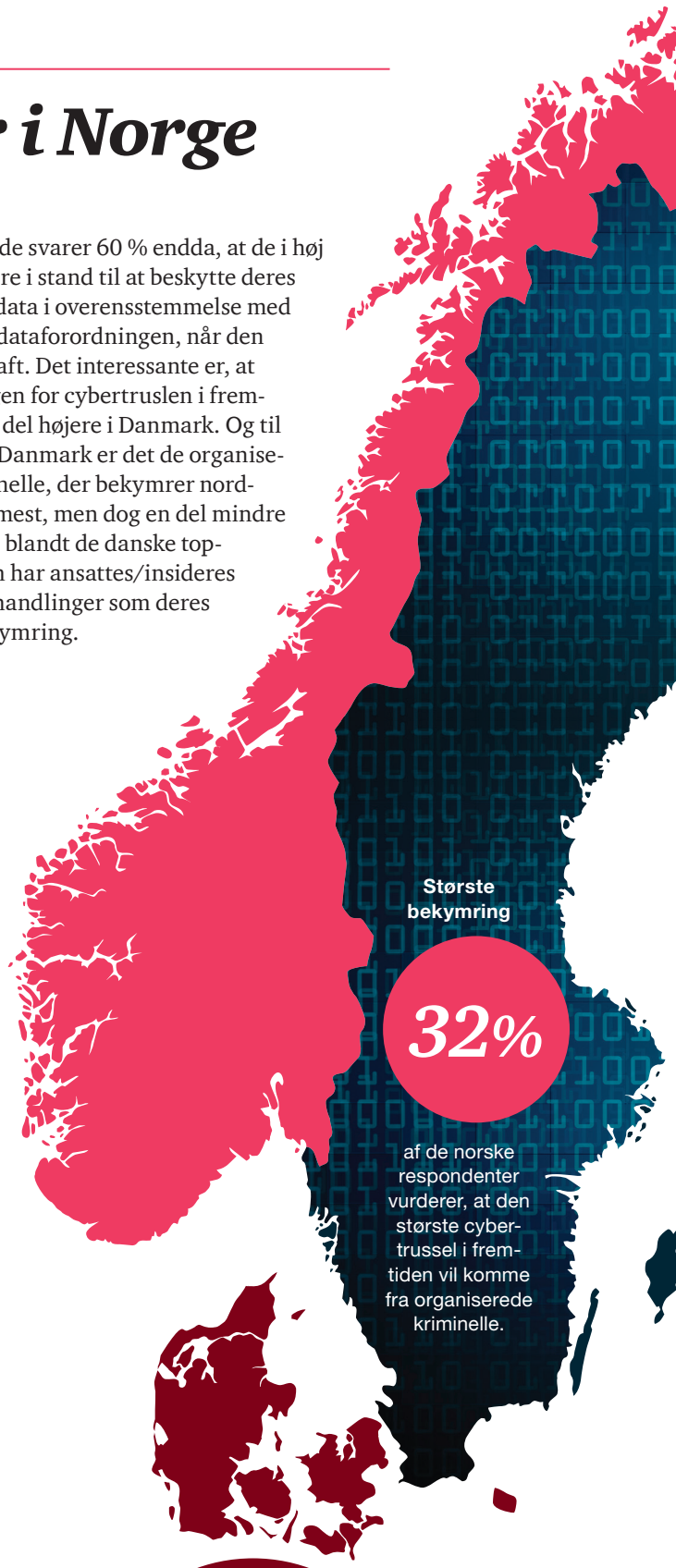
Har været udsat for et cyberangreb de seneste 12 måneder.

Er mere bekymrede for cybertruslen nu end for 12 måneder siden.

Prioriterer, at investere i at overholde den kommende EU-persondataforordning.

Vurderer, at de i høj grad vil være i stand til at beskytte deres følsomme data i overensstemmelse med persondataforordningen, når den træder i kraft.

Danmark
Norge



Største bekymring

56%

af de danske respondenter vurderer, at den største cybertrussel i fremtiden vil komme fra ansattes/insideres ubevidste handlinger.

Om undersøgelsen

Knap 250 danske og 100 norske virksomhedsledere, it-chefer og it- og sikkerhedsspecialister har deltaget i PwC's Cybercrime Survey 2017.

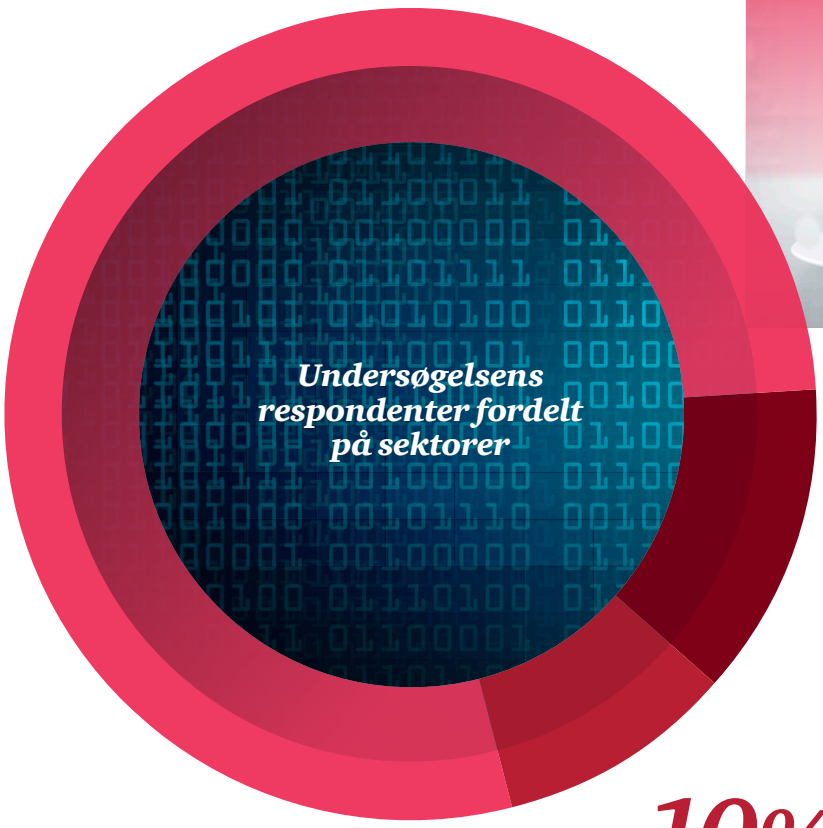
Målingen er i år gennemført med opbakning fra Finansrådet, Dansk Erhverv, Kita, IT-Branchen, Center for Cybersikkerhed, ISACA og DI Digital. Målingen bygger på onlinebesvarelser afgivet i perioden 1. maj til 14. august 2017. Respondenterne er bl.a. blevet stillet en række spørgsmål, som relaterer sig til cyberområdet, fx om de er blevet ramt af et cyberangreb, om de er bekymrede for truslen fra cybercrime, hvor meget de investerer i it-sikkerhed, hvordan deres virksomhed forholder sig til kommende samt gældende lovgivning på området mv. Virksomhederne kommer fra et bredt udsnit af brancher/industrier/sektorer, herunder handel, den finansielle sektor, professionelle services og rådgivning, teknologi, industrielle virksomheder, offentlige institutioner, energi og forsyning, transport, pharma mv.

Målingens spørgsmål og svarmuligheder er udarbejdet af PwC, og online-spørgeskemaet er udsendt i samarbejde med ovenstående organisationer.

Cyber Incident Response-team

Da et fortsat stort antal virksomheder bliver udsat for cyberangreb, har PwC fokus på at hjælpe kunder med at forebygge og håndtere cybersikkerhedshændelser.

Vi har etableret en central cyberhotline for kunder, så de 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 kan der implementeres forbedringer af sikkerheden og udarbejdes en rapport til brug for bl.a. ledelsen, forsikringen og politiet.



12%
Finansielle sektor

10%
Offentlige virksomheder

78%
Private virksomheder

Er din virksomhed forberedt?

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

1

Har vi et sikkerheds-program, der er tilpasset vores forretningsstrategi?

2

Har vi de kompetencer, der skal til for at identificere de strategiske trusler og de potentielle angreb mod vores forretning?

4

Ved vi, hvilke informationer der er mest kritiske for forretningen?

5

Har virksomheden etableret et cyberkrise-beredskab, der kan styre den sikkert igennem en kompleks it-relateret hændelse?

3

Kan vi forklare vores sikkerhedsstrategi til vores interessenter?

Inspiration

Få helt styr på
EU-persondataforordningen inden maj 2018

Med PwC's e-learning om EU-persondataforordningen sikrer I, at jeres virksomhed får den fornødne viden og dermed bliver rustet til at overholde forordningens krav. Med PwC's e-learning har I mulighed for at tilpasse indholdet, så det understøtter medarbejdernes individuelle behov.

Læs mere på www.pwc.dk/persondataforordningen

Bliv tryg
med "Managed security services"

I takt med at den digitale udvikling skaber nye og innovative løsninger, bliver vi også mere eksponeret overfor cyberkriminalitet. PwC tilbyder en trygheds-aftale, hvor vi i et tæt samarbejde med jeres sikkerhedsansvarlige har fokus på kontinuerlig monitorering af interne og eksterne sårbarheder og trusler. Sammen kortlægger vi, hvilke ydelser I har behov for.

Læs mere på www.pwc.dk/mss

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 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
2811 1592
mxm@pwc.dk

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

Christian Kjær
Partner
IT Risk Assurance
5132 1270
cik@pwc.dk

PwC's Incident Response team
70 22 24 44

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

www.pwc.dk

Succes skaber vi sammen ...

Uddannelses- og Forskningsministeriet

Erhvervsakademi Lillebælt

E-mail: eal@eal.dk

Foreløbig godkendelse af nyt udbud
Uddannelses- og forskningsministeren har på baggrund af gennemført præ-kvalifikation af Erhvervsakademi Lillebælts ansøgning om godkendelse af nyt udbud truffet følgende afgørelse:

12. april 2018

Styrelsen for Forskning og Uddannelse
Professions- og Erhvervsrettede Videregående Uddannelser

Bredgade 40
1260 København K
Tel. 3544 6200
Fax 3544 6201
sfu@ufm.dk
www.ufm.dk

CVR-nr. 1991 8440

Sagsbehandler
Camilla Badse
Tel. 72 31 86 16
cba@ufm.dk

Ref.-nr.
18/006466-21

Foreløbig godkendelse af nyt udbud af professionsbacheloruddannelse (overbygning) i it-sikkerhed

Afgørelsen er truffet i medfør af § 20 i bekendtgørelse nr. 205 af 13. marts 2018 om akkreditering af videregående uddannelsesinstitutioner og godkendelse af videregående uddannelser og § 2 i bekendtgørelse nr. 271 af 22. marts 2014 om særlige betingelser for godkendelse af udbud af erhvervsakademiuddannelser, professionsbacheloruddannelser, akademiuddannelser og diplomuddannelser.

Godkendelsen er betinget af en efterfølgende positiv institutionsakkreditering opnået senest 1. juli 2020.

Udbudsgodkendelsen kan bortfalde efter § 16 i lov om erhvervsakademiuddannelser og professionsbacheloruddannelser, jf. lovbekendtgørelse 986 af 18. august 2017.

Uddannelsen er omfattet af reglerne i bekendtgørelse nr. 100 af 8. af 2018 om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser.

Ansøgningen er blevet vurderet af Det rådgivende udvalg for vurdering af udbud af videregående uddannelser (RUVU). RUVU's vurdering er vedlagt som bilag.

Titel:
Uddannelsens titel fastlægges til:

Dansk: Professionsbachelor i it-sikkerhed.

Engelsk: Bachelor of IT Security.

Hovedområde:
It-faglige område.

Udbudssted:
Odense

Sprog:
Dansk.

Normeret studietid:
90 ECTS.

Censorkorps:
Uddannelsen tilknyttes det eksisterende censorkorps for it-uddannelserne på professionsbacheloruddannelserne.

Maksimumramme/dimensionering:
Ministeriet har ikke fastsat en maksimumsramme for tilgangen til uddannelsen.

Med venlig hilsen

Camilla Badse
Specialkonsulent

Bilag. RUVU's vurdering

Nyt udbud– prækvalifikation (forår 2018)			
Ansøger og udbudssted:	Erhvervsakademi Lillebælt		
Udbudssted	Odense		
Uddannelsestype:	Professionsbacheloruddannelse (1 ½ årig overbygningsuddannelse)		
Uddannelsens navn (fagbetegnelse):	Professionsbachelor it-sikkerhed		
Den uddannedes titler på hhv. da/eng:	-Professionsbachelor i it-sikkerhed. - Bachelor of IT Security		
Hovedområde:	IT-faglige område		
Sprog:	Dansk	**Antal ECTS:**	90 ECTS
Beskrivelse af uddannelsen, herunder erhvervssigte	Professionsbacheloruddannelsen er en 1 ½ -årig(top-op), som har til formål at kvalificerer de studerende til selvstændigt kunne varetage arbejdet med at analysere, planlægge og vurdere it- sikkerhedsmæssige forhold i forbindelse med drift, kontrol og udvikling i såvel private som offentlige virksomheder. Adgang til uddannelsen forudsætter en erhvervsakademiuddannelse som datamatiker eller IT-teknolog		
RUVU's vurdering	RUVU vurderer, at ansøgningen opfylder kriterierne, som fastsat i bekendtgørelse nr. 205 af 13. marts 2018, bilag 4. RUVU vurderer, at det er dokumenteret, at der nationalt er et væsentligt behov for uddannede dimittender med kompetencer inden for IT-sikkerhed. RUVU finder endvidere, at ansøger har dokumenteret et regionalt behov for udbud af uddannelsen.		