Styrelsen for Samfundssikkerhed

TRUSSELSVURDERING

Cybertruslen mod den danske universitetssektor

April • 2025

Indhold

Datavej 20
3460 Birkerød
Telefon: + 4516 1666
E-mail: samsik@samsik.dk

April 2025

Cybertruslen mod den danske universitets-sektor

Denne trusselsvurdering belyser cybertruslen mod den danske universitets-sektor. Vurderingen er særligt målrettet it-sikkerhedsmedarbejdere og ledere, der kan bruge vurderingen som led i deres risikovurdering for de enkelte universiteter.

Hovedvurderinger

- Truslen fra cyberspionage mod den danske universitetssektor er **MEGET HØJ**. Det er meget sandsynligt, at danske universiteter er udsat for en trussel fra cyberspionage, der særligt udspringer fra statslige aktører i Kina og Rusland. Styrelsen for Samfunds-sikkerhed (SAMSIK) vurderer, at den danske universitetssektor er et interessant mål for fremmede staters cyberspionage, fordi den er blandt de førende inden for en række forskningsområder.

- Truslen fra cyberkriminalitet mod danske universiteter er **MEGET HØJ**. Det er i høj grad ransomware-angreb, som udgør en trussel mod sektoren, selvom cyberkriminelle også retter andre angrebstyper mod sektoren.

- Truslen fra cyberaktivisme mod danske universiteter er **HØJ**. Formålet med cyber-aktivistiske angreb er at skabe opmærksomhed omkring en specifik dagsorden. Derfor er omtalen af angrebene næsten lige så central som angrebene i sig selv for aktivisterne.

- Truslen fra destruktive cyberangreb mod danske universiteter er **MIDDEL**. Truslen kommer primært fra Rusland. Hvis Rusland iværksætter angreb mod Danmark, herunder danske universiteter, vil det primære formål sandsynligvis være at påvirke befolkningen og beslutningstagere.

- Truslen fra cyberterror mod den danske universitetssektor er **INGEN**.

Indledning

Universitetssektoren i Danmark

I Danmark findes otte universiteter: Aalborg Universitet, Aarhus Universitet, Copenhagen Business School, Danmarks Tekniske Universitet, IT-Universitetet i København, Københavns Universitet, Roskilde Universitet og Syddansk Universitet. Det er disse institutioner, der falder ind under universitetssektoren i Danmark, og som trusselsvurderingen omfatter.

Truslen fra cyberangreb mod universiteter har været synlig i mange år. Alt fra ransomware-angreb, der låser systemer, til overbelastningsangreb, der gør universiteternes hjemmesider utilgængelige, har løbende ramt universiteter verden over. Danske universiteter har gennem de seneste år også været udsat for cyberangreb. Eksempelvis fik hackere adgang til en mindre del af infrastrukturen på Danmarks Tekniske Universitet (DTU) i august 2022. DTU kunne imidlertid hurtigt begrænse hackernes adgang og undgå yderligere kompromittering.

Universiteter er kendt for deres åbenhed. Døre til læsesale og laboratorier står åbne for studerende og ansatte, forskningsresultater lægges åbent op til download via internettet, og forskere fra hele verden bliver lukket ind for at udføre forskning inden for deres felt. Det er en enestående egenskab for universiteter, men med åbenheden følger også en risiko for at lukke uvedkommende ind. Universiteterne kan f.eks. utilsigtet lukke hackere eller ondsindede insidere ind, der kan skade universitetet. Det kan bl.a. være i form af bevidst placeret malware på universiteternes enheder eller decideret cyberspionage. Det er risici, universiteter skal være opmærksomme på, når de sætter niveauet for cybersikkerhed på institutionerne. I de senere år har universiteterne dog skærpet sikkerheden omkring forskningen og udviklingen af kritisk teknologi. Dette som konsekvens af den geopolitiske situation og offentliggørelsen af URIS-retningslinjerne, som har til formål at øge opmærksomheden på risiciene i internationalt forsknings- og innovationssamarbejde. Politiets Efterretningstjeneste har ligeledes styrket sin indsats for at beskytte kritisk forskning inden for bl.a. kvanteteknologi på universiteterne.

SAMSIK vurderer, at universiteter i Danmark er udsat for truslen fra cyberangreb, bl.a. fordi de er førende inden for en række forskningsområder. Værdifuld og innovativ forskning betyder, at danske universiteter kan være særligt oplagte mål for cyberangreb fra fremmede stater, der via cyberspionage kan opnå indsigt i viden og teknologi, som de kan bruge til at fremme egne interesser. Cyberkriminelle er interesserede i danske universiteter med henblik på at opnå økonomisk berigelse.

Vurderingen belyser cybertruslens mange facetter gennem en række kategorier. SAMSIK anvender følgende fem kategorier af cyberangreb: cyberspionage, cyberkriminalitet, cyberaktivisme, destruktive cyberangreb og cyberterror.

Cyberspionage

Truslen fra cyberspionage mod danske universiteter er **MEGET HØJ**. Truslen er vedvarende og kommer fra fremmede stater, som går efter universiteter globalt.

Statslige aktører, der udfører cyberspionage, har i flere tilfælde tidligere forsøgt at ramme danske universiteter, af og til med succes. Det understreger, at fremmede stater også har interesse for danske universiteter.

Det er meget sandsynligt, at danske universiteter er udsat for en trussel fra cyberspionage, der særligt udspringer fra statslige aktører i Kina og Rusland. Begge stater har betydelige cyberkapaciteter, som de bl.a. bruger til at udføre cyberspionage mod mål i Danmark og udlandet. Også Iran har betydelige cyberkapaciteter og har tidligere forsøgt at angribe vestlige universiteter.

Eksempelvis har Microsoft beskrevet, hvordan iranske hackere i 2023 og 2024 målrettede en spear phishing-kampagne mod forskere på europæiske universiteter. Hackerne forsøgte at få modtagerne til at downloade ondsindede filer med det formål at opnå adgang til ofrenes system.

Fremmede stater udfører cyberspionage mod universiteter med forskellige formål
Den danske universitetssektor er et interessant mål for fremmede staters cyberspionage. SAMSIK vurderer, at sektoren bl.a. er i søgelyset, fordi den er blandt de førende inden for en række forskningsområder. Det drejer sig bl.a. om medicinalforskning og felter inden for kvante-forskning. Den viden, institutioner i sektoren genererer inden for disse områder, kan derfor være af særlig værdi for aktørerne bag cyberspionagen. Også områder inden for sikkerheds- og udenrigspolitik og militære forsknings- og uddannelsesinstitutioner kan være interessante for fremmede stater at spionere mod.

Alle forskningsområder kan dog være i risiko for at blive udsat for cyberspionage. Fremmede stater forsøger ofte med opportunistiske angreb at ramme mål bredt. Et forskningsområde kan også komme i fremmede staters søgelys, hvis der sker en udvikling i, hvilken type viden staterne interesserer sig for, f.eks. som konsekvens af globale hændelser eller en ændring i staternes efterretningsbehov. Et eksempel herpå er COVID-19-pandemien, som bl.a. medførte cyberspionage mod vaccineforskning og -udvikling verden over.

SAMSIK vurderer, at fremmede stater i nogle tilfælde forsøger at kompromittere danske universiteter for at fremskynde national forskning og udvikling og samtidig opnå konkurrencemæssige fordele.

Fremmede stater interesserer sig bl.a. for organisationer med viden på områder, som er strategisk vigtige for deres økonomiske og militære udvikling. For Kina drejer det sig eksempelvis om informations- og kommunikationsteknologi, kvanteteknologi, kunstig intelligens, kemi og lægemidler samt dual use-teknologier.

Dual use-teknologier er teknologier, der kan bruges til både civile og militære formål. Det kan f.eks. være kunstig intelligens, navigationsudstyr og kvante-, satellit-, drone- og laserteknologi. Dual use-teknologier kan være særlig værdifulde for fremmede stater, og både Kina og Rusland har interesse i denne type teknologi. SAMSIK vurderer, at fakulteter, der udvikler eller forsker inden for dette område, er oplagte mål for cyberspionage.

Hackere bruger forskellige metoder til cyberspionage
Flere fremmede stater råder over veludviklede cyberkapaciteter og kan derfor udføre både målrettede og teknisk krævende angreb, når de vurderer det nødvendigt.

Statslige hackere bruger både simple og avancerede metoder i deres forsøg på at kompromittere deres mål, herunder bl.a. spear phishing, brute force-angreb og udnyttelse af nye og gamle sårbarheder i software. Det er meget sandsynligt, at statslige hackere har brugt nogle af disse angrebsmetoder mod danske universiteter.

Brute force-angreb

Brute force-angreb dækker over angrebstyper, hvor hackere forsøger at gætte kombinationer af brugernavne og passwords, f.eks. ved udnyttelse af passwords fra tidligere datalæk.

Hackere, der udfører cyberspionage, forsøger ofte at få adgang til tværgående it-netværk som f.eks. mailsystemer i deres angreb. Adgang til disse giver dem mulighed for potentielt at spionere mod flere fagområder inden for de enkelte universiteter samtidigt.

Hacking af leverandører er også en effektiv måde for statslige hackere at skaffe sig den viden, de går efter. Ved denne type angreb kan hackerne gennem leverandører som f.eks. softwareudbydere forsøge at få adgang til mange kunders netværk eller systemer på én gang.

Insidertruslen hos universiteter

Universiteter kan være særligt udsatte for en trussel fra insidere. Insidere dækker over personer, som ved deres handlinger udgør en risiko for den organisation, de er tilknyttet. Universiteter er bl.a. særligt udsatte grundet deres åbenhed, hvilket bevirker, at potentielle insidere relativt ukompliceret kan få adgang til universiteters data og systemer.

I universitetssektoren kan insidere både være ansatte eller studerende tilknyttet et universitet. Insidere kan handle enten forsætligt eller uforsætligt ved at misbruge deres autoriserede adgang til den organisation, de er tilknyttet. Det kan bl.a. ske i cyberdomænet via placeret malware, datatyveri, videregivelse af beskyttelsesværdige oplysninger eller lignende.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod danske universiteter er **MEGET HØJ**. Der er en vedvarende trussel fra cyberkriminalitet mod sektoren. Sektoren udgør et mål for cyberkriminelle, bl.a. grundet mængden af sensitivt data, som sektoren råder over, men også grundet sektorens offentlige eksponering og store angrebsflade.

Universiteter er oplagte mål grundet omfang af viden og data
Universiteter verden over kan komme i de cyberkriminelles søgelys af flere grunde. SAMSIK vurderer, at en af de primære årsager er, at universiteter har adgang til personfølsomme oplysninger og værdifuldt forskningsdata. Hvis hackerne kompromitterer et universitet og får adgang til systemer eller data, kan de videresælge dette på kriminelle undergrundsmarkeder eller afpresse offeret ved at true med at lække det på internettet.

Kompromittering af universiteters data kan få store konsekvenser i form af bl.a. økonomiske tab og tab af omdømme.

Ransomware udgør en trussel for danske universiteter
Den danske universitetssektor er udsat for en trussel fra mange forskellige typer af cyberkriminalitet, herunder ransomware-angreb. I ransomware-angreb forsøger cyberkriminelle at afpresse offeret ved at gøre deres data og systemer utilgængelige, ofte ved at kryptere disse. De kriminelle kræver en løsesum, typisk i form af kryptovaluta, for at gøre data og systemer tilgængelige igen.

Tyske tekniske universiteter ramt af ransomware-angreb

I sommeren 2023 blev det tyske tekniske universitet Hochschule Kaiserslautern offer for et ransomware-angreb. Angrebet påvirkede hele universitetets infrastruktur, inklusive telefonsystem og mailkonti. Alle systemer lukkede ned som konsekvens af angrebet.

Universitetet var endnu et i rækken af tyske universiteter, som de seneste år har været ramt af cyberangreb. I november 2022 blev universitetet i Duisburg-Essen ramt af ransomware, ligesom det også var tilfældet for det tekniske universitet i Hamborg i marts 2023.

Universitets- og uddannelsessektoren på globalt plan fremgår ofte af cyberkriminelles Dedicated Leak Sites (DLS). DLS er hjemmesider, hvor cyberkriminelle offentliggør navnene og potentielt også data fra de ofre, som de hævder at have kompromitteret. For eksempel har kriminelle hackere på deres DLS påstået at have ramt flere amerikanske universiteter med ransomware i løbet af sommeren 2024 og et fransk universitet i oktober 2024.

Kriminelle grupper afpresser universiteter

På de cyberkriminelles DLS afpresser de verden over universiteter for at opnå økonomisk vinding. Hvis ofrene ikke betaler en løsesum, risikerer de, at de cyberkriminelle hackere, udover at hænge dem ud offentligt, også offentliggør eventuelt stjålet data. I nogle tilfælde krypterer de cyberkriminelle ikke offerets data eller systemer, men vælger i stedet blot at stjæle data, som de efterfølgende truer med at lække.

Flere cyberkriminelle aktiviteter truer danske universiteter

Universiteter kan også blive ramt af andre typer cyberkriminelle angreb, herunder salg af adgange. Nogle kriminelle hackere sælger adgange til systemer, som købere kan bruge til at udføre yderligere angreb, herunder ransomware-angreb.

Business E-mail Compromise (BEC-svindel) udgør også en trussel mod universiteter. Ved BEC-svindel forsøger de kriminelle at franarre organisationer penge gennem falske anmodninger om pengeoverførsler. Nogle gange kompromitterer hackerne en legitim mailkonto hos en virksomhed eller hos dennes samarbejdspartnere for derefter at manipulere medarbejdere til at overføre penge til de kriminelle.

Amerikansk universitet blev offer for BEC-svindel

I 2022 blev det offentliggjort, at Virginia Commonwealth University havde været udsat for BEC-svindel. Angrebet kostede dem flere hundredetusinde amerikanske dollars.

Hackeren bag angrebet foregav i en række mailkorrespondancer at være en medarbejder i et amerikansk byggefirma, som havde et igangværende byggeprojekt på universitetet.

I disse mails narrede hackeren universitetet til at overføre knap 500.000 amerikanske dollars til en konto, hackeren styrede. Det lykkedes kun universitetet at genvinde ganske få af de overførte penge.

Cyberaktivisme

Truslen fra cyberaktivisme mod danske universiteter er **HØJ**.

Formålet med cyberaktivistiske angreb er at skabe opmærksomhed omkring en specifik dagsorden. Pro-russiske hackere retter løbende Distributed Denial of Service-angreb (DDoS) mod hjemmesider tilhørende vestlige myndigheder, organisationer samt virksomheder. Danske universiteter har ligeledes været mål for aktivisternes DDoS-angreb.

DDoS er et overbelastningsangreb, hvor hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside eller et netværk. Målet er at gøre hjemmesiden eller netværket utilgængelig for legitim trafik, mens angrebet står på.

Cyberaktivister påstår også at have rettet defacement-angreb mod universiteter rundt om i verden. Defacement af en hjemmeside er et angreb, der ændrer hjemmesidens visuelle udtryk. Angriberen kan f.eks. indsætte tekst eller billede på hjemmesiden med et særligt budskab.

Begge angrebsformer er relativt simple. De virker forstyrrende og kan påvirke tilgængeligheden af de ramte hjemmesider, men har hverken varig eller ødelæggende effekt for ofrenes systemer.

Selvom truslen fra cyberaktivisme mod danske universiteter er **HØJ**, er sektoren dog ikke blandt de hyppigst ramte i Danmark. Truslen har i stedet ofte været rettet mod finans- og transportsektoren og mål inden for Forsvarsministeriets myndighedsområde.

Cyberaktivisme kan være andet end DDoS
Selvom det primært er DDoS-angreb, der fylder i trusselsbilledet, udfører nogle cyberaktivister også andre former for cyberangreb.

For eksempel har enkelte pro-russiske cyberaktivister også udført simple og opportunistiske destruktive cyberangreb mod mål i vestlige lande. Omfanget af disse angreb er dog begrænset sammenlignet med de mange DDoS-angreb, som rammer mål i Danmark og Vesten, og angrebene har primært også været rettet mod mål med lav beskyttelse. Blandt andet derfor vurderer SAMSIK, at truslen fra destruktive, cyberaktivistiske angreb er mindre relevant for universitetssektoren.

Cyberaktivister overdriver for at skabe opmærksomhed

Aktivistiske hackeres kommunikation omkring deres angreb er ofte misvisende og overdreven. Dette betyder, at der i mange tilfælde er usikkerhed om, hvorvidt cyberaktivistiske angreb har fundet sted, samt hvilken effekt angrebene har haft. SAMSIK vurderer, at aktivisters kommunikation om både falske og reelle angreb har til hensigt at skabe offentlig opmærksomhed omkring deres dagsorden. De cyberaktivistiske grupper søger således omtale i vestlige medier og deler vestlige, herunder danske, mediers artikler om gruppernes angreb.

Selvom SAMSIK er bekendt med gruppernes navne, bliver de derfor ikke nævnt i publikationer, medmindre det er afgørende for at give et retvisende trusselsbillede.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod danske universiteter er **MIDDEL**, ligesom det er tilfældet for Danmark generelt. Rusland er villig til at bruge hybride virkemidler med destruktive effekter mod europæiske NATO-lande, og SAMSIK vurderer, at dette også omfatter destruktive cyberangreb.

Cyberspionage vil ofte være en del af forberedelsen af destruktive cyberangreb, men er ikke en forudsætning for dem alle. Hackere kan i nogle tilfælde med begrænset forberedelse udføre simple, destruktive cyberangreb mod systemer med dårlig beskyttelse.

Destruktive cyberangreb

SAMSIK definerer destruktive cyberangreb som cyberangreb, hvor den forventede effekt er:

- død eller personskade
- betydelig skade på fysiske objekter
- ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning

Hackere, der udfører destruktive cyberangreb, bruger især såkaldt wiper-malware til at opnå deres mål. Wiper-malware er en type malware, der sletter, overskriver eller krypterer data, så det ikke længere er tilgængeligt.

SAMSIK vurderer, at mange typer organisationer i samfundsvigtige sektorer, herunder danske universiteter, vil kunne blive udvalgt som mål for eventuelle destruktive cyberangreb.

Hvis Rusland i den nuværende sikkerhedspolitiske situation vælger at rette destruktive cyberangreb mod Danmark, er det sandsynligt, at formålet vil være at påvirke befolkningen og beslutningstagere. Den konkrete fysiske effekt af angrebene vil derfor sandsynligvis være sekundær sammenlignet med, om angrebene skaber opmærksomhed.

Destruktive cyberangreb er ét blandt flere hybride virkemidler, som Rusland kan bruge til at forsøge at presse vestlige befolkninger og beslutningstagere.

Truslen fra destruktive cyberangreb udspringer især fra Rusland
Truslen fra destruktive cyberangreb mod Danmark, herunder mod danske universiteter, kommer især fra Rusland. Det er dog mindre sandsynligt, at Rusland i den nuværende sikkerhedspolitiske situation vil udføre destruktive cyberangreb mod danske universiteter med hensigten om at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.

Selvom disse angreb er mindre sandsynlige, vurderer SAMSIK, at statsstøttede russiske hackergrupper løbende forbereder sig på at kunne udføre den form for destruktive cyberangreb mod Danmark. Sandsynligheden for, at disse angreb finder sted, kan derfor stige med kort eller uden varsel.

Andre aktører udgør også en potentiel trussel
Selvom truslen fra destruktive cyberangreb især kommer fra Rusland, er der også en potentiel trussel fra andre stater. For eksempel er det sandsynligt, at hackergrupper fra Iran har udført destruktive cyberangreb mod vestlige mål.

Derudover kan der også være en trussel fra ikke-statslige hackere. Det skyldes blandt andet, at stater kan forsøge at sløre deres involvering i et destruktivt cyberangreb ved at få kriminelle eller aktivistiske hackere til at udføre angrebene for dem.

Samtidig vurderer SAMSIK som beskrevet, at visse cyberaktivistiske grupper har intentioner om at udføre cyberangreb med destruktiv effekt. For eksempel blev et mindre dansk vandværk i slutningen af 2024 ramt af et destruktivt cyberangreb fra pro-russiske cyberaktivister. Ved angrebet blev vandværkets operationelle systemer manipuleret, hvilket bl.a. medførte, at flere husstande var uden vand i en kortere periode.

Det er dog kun i få tilfælde, at en reel effekt fra et cyberaktivistisk destruktivt angreb er blevet bekræftet, og SAMSIK vurderer generelt, at aktivisternes evne til at udføre den type angreb er begrænset sammenlignet med fremmede staters. De udgør derfor primært en trussel mod organisationer med svage sikkerhedsforanstaltninger.

Cyberterror

Truslen fra cyberterror mod danske universiteter er **INGEN**.

Det er usandsynligt, at den danske universitetssektor vil blive udsat for forsøg på cyberterror på kort sigt.

SAMSIK definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som konventionel terror. Det kan f.eks. være cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

Denne slags cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Samtidig er ekstremisternes hensigt om at udføre denne form for angreb mod Danmark yderst begrænset.

Trusselsniveauer

Styrelsen for Samfundssikkerhed anvender i sine trusselsvurderinger Forsvarets Efterretningstjenestes (FE) trussels- og sandsynlighedsniveauer.

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer:

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, eller en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for SAMSIK's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.

SAMSIK bruger denne skala for sandsynligheder i analyser:

En sandsynlighedsgrad er udtryk for et skøn, ikke en beregnet statistisk sandsynlighed.
"SAMSIK vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.

Andre relevante publikationer

Nedenfor fremgår en række af de publikationer, som kan være relevante for organisationer i den danske universitetssektor. Publikationerne kan tilgås på WWW.SAMSIK.DK.

Cybertruslen mod Danmark 2024
I denne årlige trusselsvurdering beskrives den generelle cybertrussel for hhv. cyberkriminalitet, cyberspionage, cyberaktivisme, destruktive cyberangreb og cyberterror mod Danmark.

Cybertruslen mod IoT-enheder
Trusselsvurderingen beskriver cybertruslen mod IoT-enheder, inkl. netværksudstyr, der ligesom almindelige it-systemer rammes af cyberangreb.

Anatomien af et målrettede ransomware-angreb
Denne rapport kortlægger, hvordan særligt målrettede ransomware-angreb typisk forløber, og giver konkrete anbefalinger til, hvordan myndigheder og virksomheder kan beskytte sig endnu bedre.

Et wiper-angrebs anatomi
Rapporten belyser, hvordan den klart mest udbredte type destruktive cyberangreb, wiper-angreb, fungerer, og hvordan du forsvarer dig imod dem.

Logning – en del af et godt cyberforsvar
Vejledningen giver gode råd til, hvor i netværket man skal logge og hvad man bør logge. Den bygger på erfaringer fra bl.a. it-sikkerhedsfirmaer i forbindelse med bistand ved hændelseshåndtering.

Vejledning om cybersikkerhed i leverandørforhold
Vejledningen "Cybersikkerhed i leverandørforhold" giver gode råd til, hvordan man kan oprette og bibeholde et godt samarbejde mellem kunden og leverandøren af it-driften, gennem hele samarbejdsperioden. Fra valg af leverandør til ophør af samarbejdet.

Vejledning om password-sikkerhed
Vejledningen beskriver nogle af de angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Vejledningen indeholder desuden en række konkrete anbefalinger til, hvordan man – på forskellige niveauer i en organisation – bør arbejde med password-sikkerhed.

Vejledning om at imødegå ransomware-angreb
Vejledningen "Reducér risikoen for ransomware" giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket.

Vejledning om at imødegå phishing-angreb
Vejledningen ”Beskyt din organisation mod phishing-angreb” hjælper organisationer med at imødegå truslen fra phishing-mails.

Vejledning om beskyttelse mod DDoS-angreb
Vejledningen ”Beskyt mod DDoS-angreb” kommer med en række forholdsregler, som en organisation kan tage for at beskytte sig mod DDoS-angreb.