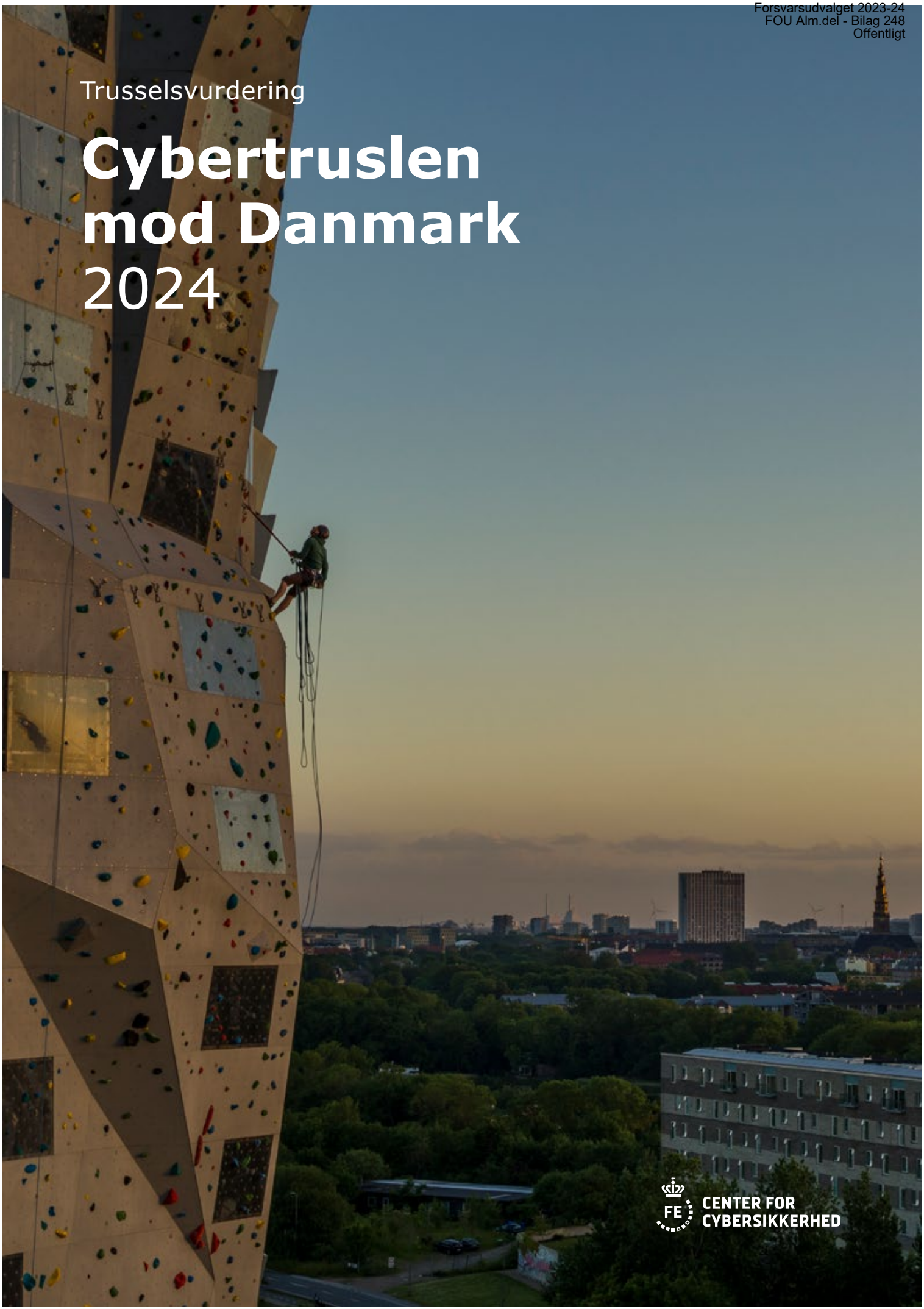
Trusselsvurdering

Cybertruslen mod Danmark 2024



CENTER FOR CYBERSIKKERHED

CENTER FOR CYBERSIKKERHED

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk
www.fe-ddis.dk

Indhold

CYBERTRUSLEN MOD DANMARK 2024

Formålet med vurderingen er at informere beslutningstagere i danske myndigheder og virksomheder om cybertruslen mod Danmark. Trussels-vurderingen redegør for de forskellige typer af cybertrusler, Danmark står over for. Vurderingen kan bl.a. indgå som del af grundlaget for organisationers risikovurderinger.

HOVEDVURDERING

- TRUSLEN FRA CYBERSPIONAGE MOD DANMARK ER **MEGET HØJ**

  Organisationer med viden om dansk udenrigs- og sikkerhedspolitik er særligt udsatte. Også dansk kritisk infrastruktur og Forsvaret er i fremmede staters søgelys, når de udfører cyberspionage.

  Truslen fra cyberspionage mod Danmark kommer primært fra Rusland og Kina. Begge stater har betydelige cyberkapaciteter, som de bl.a. bruger til at udføre cyberspionage mod mål i Danmark og udlandet.

- TRUSLEN FRA CYBERKRIMINALITET MOD DANMARK ER **MEGET HØJ**

  Cyberkriminalitet rammer bredt og alle dele af samfundet.

  CFCS vurderer, at der i 2023 var flere ransomware-tilfælde i Danmark end hidtil, og at det også gælder internationalt.

- TRUSLEN FRA CYBERAKTIVISME MOD DANMARK ER **HØJ**

  Cyberaktivistiske angreb, der løbende har ramt danske mål, understreger, at truslen mod danske virksomheder og myndigheder er blevet en del af normalbilledet.

  Truslen fra cyberaktivisme mod Danmark udspringer primært fra pro-russiske cyberaktivister. CFCS vurderer, at nogle pro-russiske cyberaktivister har forbindelse til den russiske stat.

- TRUSLEN FRA DESTRUKTIVE CYBERANGREB MOD DANMARK ER **MIDDEL**

  Truslen kommer primært fra russiske statslige hackere. Det er dog mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod Danmark, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.

  Flere fremmede stater har kapacitet til at udføre destruktive cyberangreb mod Danmark. Truslen fra destruktive cyberangreb kan stige med kort eller uden varsel, hvis fremmede staters intentioner om at ramme danske mål ændrer sig.

- TRUSLEN FRA CYBERTERROR MOD DANMARK ER **INGEN**

  CFCS har fulgt truslen fra cyberterror siden 2016 med fokus på militante ekstremister og vurderer, at ingen aktører aktuelt har kapacitet til eller intention om at udføre cyberterror mod Danmark.

INDLEDNING

Siden CFCS udgav C*ybertruslen mod Danmark 2023*, har den sikkerhedspolitiske situation i verden fortsat udviklet sig. Der er opstået krig mellem Israel og Hamas i Gaza, og Ruslands invasion af Ukraine har udviklet sig til at være en langvarig krig. Den sikkerhedspolitiske situation og konkurrencen mellem stater smitter også af på cyberdomænet. Det skyldes, at cyberangreb er ét værktøj blandt flere, stater bruger til at understøtte deres interesser.

Cyberspionage, destruktive cyberangreb og cyberaktivisme relaterer sig i høj grad til forholdet mellem stater, mens det står anderledes til med cyberkriminalitet. Her er aktørerne typisk apolitiske og angriber opportunistisk i jagten på et så stort økonomisk afkast som muligt. Cyberangreb kan derfor ramme alle, både myndigheder, virksomheder, tænketanke, NGO'er og individer.

Cybertruslen er med andre ord et grundvilkår, som vi – særligt i et så digitaliseret land som Danmark – er nødt til at leve med. Det er tydeligt i mediebilledet, hvor bl.a. ransomware-angreb og cyberaktivistiske overbelastningsangreb har fået spalteplads.

CFCS opdeler cybertruslen i fem forskellige kategorier: cyberspionage, cyberkriminalitet, cyberaktivisme, destruktive cyberangreb og cyberterror. Det er ikke gjort for at simplificere truslen, men for at understrege, at cybertruslen er en sammensat størrelse, som ikke lader sig beskrive ud fra én vinkel. Hver kategori tager udgangspunkt i formålet med en given angrebstype. Formålet med cyberspionage er at spionere, formålet med cyberterror er at udføre terror via cyberdomænet osv. Det er dog ikke altid ligetil at vurdere formålet med et angreb, da der kan være overlap mellem nogle typer af angreb.

Danmark udgør fortsat et mål for flere cybertrusler

Dette års *Cybertruslen mod Danmark* understreger, at Danmark fortsat udgør et attraktivt mål for ondsindede aktører. I starten af juni hævede CFCS trusselsniveauet for destruktive cyberangreb fra **LAV** til **MIDDEL**. Niveauet blev hævet på baggrund af en udvikling i Ruslands risikovillighed i forhold til at anvende hybride virkemidler, herunder destruktive cyberangreb, mod europæiske NATO-lande. Det understreger, at en ustabil sikkerhedspolitisk situation på globalt plan også smitter af på cyberdomænet.

Trusselslandskabet er hele tiden i udvikling. Nye aktører kommer til, mens andre forsvinder fra trusselsbilledet, og hackere udvikler hele tiden deres angrebsmetoder. Nedenfor følger et oprids af truslen fra de fem typer, CFCS opdeler cybertruslen i.

Truslen fra cyberspionage mod Danmark er **MEGET HØJ**. Fremmede stater udfører løbende forsøg på cyberspionage mod organisationer i Danmark. Det har de gjort i en årrække, og det vil de fortsat forsøge at gøre.

Truslen fra cyberkriminalitet er ligesom cyberspionage **MEGET HØJ**. Truslen er blandt de mest synlige i trusselslandskabet og kan gå ud over både den enkelte borger, myndigheder og virksomheder uanset størrelse og samfundskritiske funktioner. Den type angreb rammer med andre ord bredt, hvilket særligt skyldes cyberkriminelle aktørers opportunisme.

Truslen fra cyberaktivisme mod Danmark er fortsat **HØJ**. Den høje trussel fra cyberaktivisme er siden Ruslands invasion af Ukraine blevet en del af normalbilledet. Krigen i Gaza har været en yderligere drivkraft, der har affødt nye cyberaktivistiske aktører og motiveret aktiviteten hos eksisterende. Truslen fra cyberaktivisme udspringer dog fortsat hovedsageligt fra pro-russiske cyberaktivister.

Truslen fra destruktive cyberangreb mod Danmark er nu **MIDDEL**. Truslen udspringer primært fra russiske statslige hackere, men ikke-statslige hackere med forskellige grader af forbindelser til den russiske stat udgør også en trussel.

Truslen fra cyberterror mod Danmark er **INGEN**. CFCS vurderer, at ingen terrorgrupper aktuelt har kapacitet til eller intention om at udføre cyberterror. Det er derfor usandsynligt, at danske myndigheder og virksomheder inden for de næste to år vil blive udsat for forsøg på cyberterror.

CFCS bruger Forsvarets Efterretningstjenestes trussels- og sandsynlighedsniveauer, der er indsat til sidst i vurderingen. I denne vurdering af cybertruslen mod Danmark beskriver CFCS truslen med en tidshorisont på to år.

God læselyst!

CYBERSPIONAGE

Truslen fra cyberspionage mod Danmark er **MEGET HØJ**. Fremmede stater forsøger løbende at udføre cyberspionage mod organisationer i Danmark, af og til med succes. Det har de gjort i en årrække, og det er meget sandsynligt, at de fortsat vil gøre det de næste mange år.

■ Cyberspionagen er oftest rettet mod Forsvaret og organisationer med viden om dansk udenrigs- og sikkerhedspolitik. Andre organisationer er dog også udsat for en trussel fra cyberspionage. Det skyldes, at fremmede stater udfører cyberspionage med flere formål og mod flere typer mål.

Det er sandsynligt, at statslige russiske hackere udfører cyberspionage mod dansk kritisk infrastruktur for at forberede sig på at kunne udføre destruktive cyberangreb i fremtiden. Det kan blive aktuelt, hvis deres intention om at ramme danske mål ændrer sig. Derudover er det meget sandsynligt, at især Kina udfører cyberspionage mod mål i bl.a. Danmark for at tilegne sig viden og overføre teknologi.

Truslen fra cyberspionage kommer primært fra Rusland og Kina
Truslen fra cyberspionage mod Danmark kommer især fra Rusland. CFCS vurderer desuden, at cyberspionage fra Kina også udgør en vedvarende trussel. Begge stater har betydelige cyberkapaciteter, som de bl.a. bruger til at udføre cyberspionage mod mål i Danmark og udlandet.

Andre stater, herunder Nordkorea og Iran, har også kapacitet til at udføre cyberspionage. De bruger dog primært deres kapacitet til at udføre cyberspionage i deres nærområde. Det er mindre sandsynligt, at disse stater aktuelt prioriterer at udføre cyberspionage mod Danmark. Det er dog fortsat muligt, at organisationer i Danmark bliver ramt af cyberspionage fra andre lande end Rusland og Kina. Det skyldes, at nogle aktører arbejder opportunistisk, når de udfører cyberspionage. Deres angreb er således ikke altid målrettede, men kan i stedet være drevet af, hvilke systemer de relativt ukompliceret kan tilgå. Derudover kan truslen fra disse stater hurtigt ændre sig, hvis f.eks. internationale begivenheder gør Danmark til et interessant spionagemål.

Fremmede stater forsøger at stjæle viden om udenrigs- og sikkerhedspolitik
Det er meget sandsynligt, at både Rusland og Kina bl.a. bruger cyberspionage til at få adgang til viden om dansk udenrigs- og sikkerhedspolitik. Den viden kan staterne bruge til at udfordre vestlige normer og styrke deres internationale indflydelse. Det kan potentielt ske på bekostning af Danmarks interesser.

CFCS vurderer, at Danmark udgør et mål for denne type cyberspionage på linje med andre NATO- og EU-lande. Det skyldes, at Rusland og Kina er bredt interesserede i Vestens udenrigs- og sikkerhedspolitik og syn på internationale dagsordener, konflikter og begivenheder. Et eksempel på et emne af særlig interesse for Rusland er Vestens støtte til Ukraine.

Der er dog også forhold, som bidrager til en mere specifik interesse for Danmarks udenrigs- og sikkerhedspolitik fra fremmede stater. Eksempelvis er det sandsynligt, at Danmarks geografiske placering i Østersøen bidrager til truslen fra cyberspionage fra især Rusland. Samtidig er det meget sandsynligt, at Rusland og Kinas cyberspionage mod Danmark også er drevet af Kongerigets geografiske placering og rolle i Arktis.

Cyberspionage kan både have en generel og konkret værdi for staterne. De kan f.eks. bruge cyberspionage til at opbygge en generel viden om Danmarks udenrigs- og sikkerhedspolitiske prioriteter og Danmark som strategisk aktør. Cyberspionage kan dog også give dem adgang til konkret viden om danske positioner i en international forhandlingssituation.

Rusland udfører cyberspionage for at forberede sig på en militær konflikt
Det er meget sandsynligt, at særligt Rusland også udfører cyberspionage mod Danmark for at forberede sig på en eventuel militær konflikt med NATO. På den måde kan Rusland, i kombination med andre former for spionage, stille sig selv bedst muligt, hvis en militær konflikt skulle opstå.

Denne cyberspionage er drevet af en bred russisk interesse for NATO-lande. Det skyldes de enkelte landes rolle i en eventuel militær konflikt mellem Rusland og NATO. Denne cyberspionage er ligeledes drevet af en specifik interesse for Danmark. Det skyldes bl.a. Kongerigets placering i Østersøen og Arktis, hvor Rusland har militære interesser.

Truslen fra cyberspionage, der skal bidrage til forberedelsen af en eventuel konflikt med NATO, er særligt rettet mod Forsvaret. Der er dog også en trussel mod Forsvarets leverandører og øvrige organisationer, som ifølge Ruslands forventning understøtter Forsvaret eller andre NATO-landes militære organisationer. Det er meget sandsynligt, at Rusland bl.a. er interesseret i at få adgang til viden om Forsvarets og NATO's kapaciteter, organisering, planer og personel.

Truslen er også rettet mod organisationer inden for den kritiske infrastruktur i Danmark. Det skyldes bl.a., at statslige russiske hackere sandsynligvis udfører cyberspionage mod disse for at forberede sig på at kunne udføre destruktive cyberangreb. Gennem cyberspionage kan hackere få indsigt i organisationerne, opbygge viden om deres systemer og netværk samt etablere bagdøre. På den måde kan hackerne udføre destruktive cyberangreb mod disse mål med kort eller uden varsel i tilfælde af f.eks. en eskalerende krise eller krig.

Kina anvender også cyberspionage til at få adgang til viden og teknologi
Det er meget sandsynligt, at særligt Kina også udfører cyberspionage for at fremme landets økonomiske interesser og teknologiske udviklingsmål. Det gør de ved at tilegne sig viden og overføre teknologi fra udlandet.

Truslen fra cyberspionage med dette formål retter sig bredt mod organisationer verden over, herunder også organisationer i Danmark.

CYBERSPIONAGE TRUER SAMFUNDET OG DEN ENKELTE ORGANISATION

Cyberspionage kan både have store konsekvenser for samfundet som helhed og den enkelte organisation. Nogle konsekvenser er tydelige, mens andre lettere overses, fordi de er uhåndgribelige eller først indtræffer på længere sigt.

Fra et nationalt perspektiv kan cyberspionage bl.a. have konsekvenser for Danmarks sikkerhed og interesser. Det gælder f.eks., hvis stater får adgang til viden, de kan udnytte i en militær konflikt eller internationale forhandlinger. Tyveri af intellektuel ejendom kan også svække Danmarks handelspositioner og dermed den danske økonomi.

For den enkelte organsation kan konsekvenserne ved cyberspionage bl.a. være økonomiske tab og tab af omdømme, tillid og konkurrenceevne. Samtidig kan cyberspionage medføre bødestraf, hvis følsomme personoplysninger kompromitteres.

Flere danske virksomheder og forskningsinstitutioner er førende inden for deres felt og har derfor en viden, der gør dem til potentielle mål for cyberspionage. Det gælder særligt organisationer med viden på de områder, som er strategisk vigtige for Kinas økonomiske og teknologiske udvikling. Områderne omfatter bl.a. informations- og kommunikationsteknologi, kunstig intelligens, lægemidler samt kvante- og luftfartsteknologi.

Virksomheder i den danske forsvarsindustri er desuden interessante mål for cyberspionage for både Kina og Rusland. Viden og teknologi, de kan bruge til at opbygge deres egne militære kapaciteter, har værdi for begge stater. Derudover kan viden fra forsvarsindustrien give indsigt i vestlige landes militære kapaciteter.

Opportunistisk cyberspionage truer alle dele af samfundet

CFCS vurderer, at alle organisationer i Danmark er udsat for en generel trussel for at blive kompromitteret af fremmede stater. Det skyldes, at nogle statslige hackere løbende forsøger at kompromittere et stort antal ofre på opportunistisk vis. Alle organisationer risikerer dermed at blive ramt, også selvom de ikke udgør et oplagt spionagemål.

Det er f.eks. meget sandsynligt, at nogle statslige hackere forsøger at få adgang til mange systemer og netværk ved at udnytte en udbredt sårbarhed eller udsende et stort antal phishing-mails. CFCS vurderer, at formålet bl.a. er at udføre cyberspionage mod de kompromitterede ofre, der er interessante. Alternativt kan hackerne udnytte de kompromitterede enheder som del af deres infrastruktur til at udføre yderligere cyberangreb mod andre organisationer.

STATER BRUGER BÅDE SIMPLE OG AVANCEREDE METODER

Statslige hackere har ofte kapacitet til at udføre avancerede former for cyberspionage. Det omfatter bl.a. udnyttelse af zero day-sårbarheder, som er sårbarheder, der endnu ikke er lukket via en opdatering, og som derfor kan være svære at imødegå. I december 2023 blev det eksempelvis beskrevet i åbne kilder, at russiske statslige hackere udnyttede en zero day-sårbarhed i Microsoft Outlook til at spionere mod energi-, transport-, tele- og forsvarssektoren i en række NATO-lande.

Statslige hackere bruger dog også mere simple metoder ved cyberspionage. De kan f.eks. snyde medarbejdere til at klikke på et link eller en vedhæftet fil i en phishing-mail og derved give dem adgang til organisationernes systemer. Desuden kan de få adgang til systemer via kendte sårbarheder eller brute force-angreb.

Det er sandsynligt, at statslige hackere primært bruger deres avancerede metoder, hvis simple angreb er utilstrækkelige, og angrebets udbytte vurderes at blive højt. Det kan f.eks. være tilfældet i forbindelse med cyberspionage mod højt prioriterede mål.

Det er sandsynligt, at statslige hackere primært bruger deres avancerede metoder, hvis simple angreb er utilstrækkelige, og angrebets udbytte vurderes at blive højt. Det kan f.eks. være tilfældet i forbindelse med cyberspionage mod højt prioriterede mål.

Nogle statslige hackere forsøger også at kompromittere et stort antal ofre via en fælles leverandør. Det kan f.eks. ske ved et software supply chain-angreb. Her kompromitterer hackere en software-leverandør for at gemme malware i en legitim opdatering. Når opdateringen udgives, risikerer softwarens brugere dermed at blive kompromitteret. I nogle tilfælde kan der være tale om tusindvis af brugere.

Et andet eksempel på et supply chain-angreb kan være, hvis hackerne kompromitterer en cloud-udbyder. I sådan et tilfælde kan hackerne potentielt få adgang til det data eller de systemer, som cloud-udbyderen lagrer for deres kunder. Desuden kan hackerne i nogle tilfælde udnytte integrationen mellem cloud-udbyderen og kundernes netværk til at kompromittere og stjæle data fra de kunder, der udgør interessante spionagemål.

Cyberspionage er et alsidigt og bredt anvendt værktøj

Fremmede stater udfører også cyberspionage med andre formål end dem, der er beskrevet ovenfor.

Fremmede stater foretager f.eks. også cyberspionage til at spionere mod befolkningsgrupper og dissidenter, der opholder sig i udlandet. Kina forsøger f.eks. gennem cyberspionage at kontrollere og undertrykke den kinesiske diaspora generelt og især dissidenter, herunder fra mindretal som uighurer og tibetanere.

Derudover vurderer CFCS, at fremmede stater bl.a. bruger cyberspionage til at understøtte påvirkningskampagner. Det kan f.eks. ske gennem hack og læk-angreb, hvor formålet er at påvirke vestlige landes befolkning. Her stjæler og lækker hackerne interne dokumenter eller data for at sende et bestemt budskab eller skade en person, organisation eller et lands omdømme. I hack og læk-angreb kan de lækkede informationer være blevet redigeret eller manipuleret for at understøtte et bestemt budskab.

CFCS vurderer dog, at cyberspionage med disse formål primært har været rettet mod mål i udlandet. Det er mindre sandsynligt, at Danmark udgør et prioriteret mål for cyberspionage med den slags formål.

LÆS MERE

Se flere trusselsvurderinger på **cfcs.dk**

CYBERKRIMINALITET

Truslen fra cyberkriminalitet mod danske myndigheder, virksomheder og borgere er **MEGET HØJ**. Det er meget sandsynligt, at danske myndigheder og virksomheder vil blive ramt af cyberkriminalitet inden for de næste to år.

■ De cyberkriminelle udnytter deres data- og systemadgange til at berige sig selv økonomisk. Cyberkriminalitet er blandt de mest synlige cybertrusler i det danske samfund, og truslen kan have mærkbare konsekvenser for både borgere og organisationer. Det er bl.a. tydeligt, når personoplysninger bliver lækket, når virksomheder må afbryde driften, eller når de i yderste konsekvens må lukke som følge af et angreb.

Ransomware rammer alle dele af samfundet

Truslen fra ransomware-angreb er ikke blevet mindre. CFCS vurderer, at der i 2023 var flere ransomware-tilfælde i Danmark end hidtil, og at det også gælder internationalt.

I ransomware-angreb forsøger kriminelle at afpresse myndigheder og virksomheder 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.

Ransomware-angreb rammer bredt, fordi cyberkriminelle er opportunistiske. Alle typer organisationer uanset branche og størrelse kan blive ramt. Hackere går efter små og mellemstore virksomheder, hvis de nemt kan bryde deres sikkerhed. De går samtidig efter store virksomheder i forventningen om at kunne få et stort udbytte. Eksempelvis er produktionsvirksomheder attraktive mål for ransomware-aktører, der stræber efter et højt udbytte. Produktionsvirksomheder har typisk en relativt høj omsætning og kan derfor potentielt betale en høj løsesum til hackerne. De kan derudover yderligere presses, hvis ransomwaren medfører nedetid i produktionen.

Nogle af de kriminelle aktører, der typisk har udført ransomware-angreb, har også benyttet sig af andre afpresningsteknikker. Der er eksempler på grupper, der stjæler data fra et offer, men ikke krypterer offerets data. Herefter truer de kriminelle med at lække eller sælge det stjålne data, hvis offeret ikke betaler løsesummen. Det kan få stor betydning for de virksomheder og myndigheder, der bliver ramt, men også for samarbejdspartnere, kunder, borgere osv., hvis deres data lækkes. De kriminelle lækker ofte data på såkaldte dedicated leak sites (DLS) på det mørke internet.

I løbet af 2023 har der i Danmark været eksempler på, at cyberkriminelle forsøger at afpresse organisationer ved at true med at offentliggøre stjålne personoplysninger. Flere medier beskriver f.eks., at kriminelle hackere fik adgang til en række personoplysninger og dokumenter i et angreb, der ramte ejendomsmæglerkæden EDC. Efterfølgende forsøgte hackerne at afpresse EDC. Da de ikke betalte, blev oplysningerne lagt ud på det mørke internet.

Man er som offer aldrig garanteret, at de cyberkriminelle dekrypterer låste filer eller systemer eller sletter data, de har stjålet. Det kom eksempelvis frem i februar 2024, at ransomware-gruppen LockBit havde beholdt data fra ofre, der ellers havde betalt løsesum til gruppen.

Cyberkriminelle udfører også andre typer af cyberkriminalitet

Cyberkriminelle forsøger at berige sig økonomisk på forskellig vis, og cyberkriminalitet er således ikke begrænset til afpresnings- og ransomware-angreb. De beriger sig eksempelvis ved salg af data og systemadgange samt ved at svindle deres ofre til at overføre penge til dem.

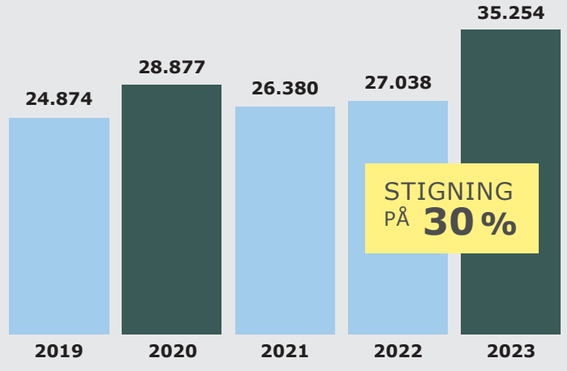
Der er bl.a. veletablerede undergrundsmarkeder for cyberkriminelle, der stjæler data eller skaber adgange til organisationers systemer og videresælger disse til andre cyberkriminelle. Hackere, der specialiserer sig i at skaffe og videresælge disse adgange, kaldes Initial Access Brokers (IAB).

ANGREBET MOD AZEROCLOUD

Ransomware-angreb kan også påvirke andre virksomheder end den, der bliver ramt direkte. Hvis man f.eks. opbevarer sine data hos en ekstern leverandør, kan ransomware-angreb mod leverandøren få alvorlige konsekvenser.

I august 2023 blev den danske hosting-virksomhed AzeroCloud ramt af et ransomware-angreb. Ifølge AzeroCloud lykkedes det de kriminelle at kryptere al data inklusive backups. Det resulterede i, at størstedelen af deres kunder mistede al deres data hos AzeroCloud. AzeroCloud meldte i marts 2024 ud, at virksomheden går konkurs.

ANMELDELSER OM IT-KRIMINALITET I DANMARK VAR REKORDHØJ I 2023



- Figuren viser udviklingen i antal anmeldelser om it-relateret økonomisk kriminalitet fra 2019-2023
- Fra 2022 til 2023 var der en stigning i antallet på 30 procent (svarende til 8.220 anmeldelser)

It-relateret økonomisk kriminalitet omhandler økonomisk kriminalitet, der foregår på internettet med brug af it-systemer og telefoner til at opnå økonomisk vinding. Denne type kriminalitet indbefatter bl.a. Business E-mail Compromise-svindel (BEC-svindel), misbrug af kortoplysninger, ransomware, masseafpresning og samhandelsbedrageri, hvor køber overfører penge for en vare, som aldrig bliver afsendt. Tallene er fra Nationalt Center for IT-kriminalitets årsrapport for 2023, som kan findes på Politiets hjemmeside.

BERYGTEDE RANSOMWARE-GRUPPER PRESSER DANSKE OFRE

Danske organisationer går ikke fri af afpresning fra cyberkriminelle. Forskellige ransomware-grupper, der forvolder stor skade verden over, hævder løbende også at have ramt danske mål. I løbet af 2023 havde mindst fem berygtede ransomware-grupper danske ofre på deres respektive DLS'er. Når grupperne nævner organisationer med navn på deres DLS, er det et forsøg på at presse dem og fremtidige ofre til at betale en løsesum.

Grupperne kræver hvert år mange millioner dollars i løsesum i deres angreb. For eksempel har ransomware-gruppen LockBit ifølge amerikanske og britiske myndigheder modtaget mere end 120 millioner dollars i løsesum og ramt over 2.000 ofre.

Udover at kunne købe og sælge systemadgange udbyder kriminelle også salg af malware og tjenester af hinanden. Den form for platformsøkonomi bidrager til at øge både omfanget og udbyttet af cyberkriminelle angreb. Hackernes mulighed for at købe sig til specialiserede ydelser sænker adgangsbarrieren for at kunne udføre et vellykket cyberangreb. Derudover understøtter samarbejdet og handlen de cyberkriminelles kapaciteter. Det skyldes, at hackere kan specialisere og dygtiggøre sig i enkelte led i angrebskæden.

Svindel er en anden udbredt form for cyberkriminalitet. Mod myndigheder og virksomheder kommer det primært til udtryk i form af BEC-svindel. Ved BEC-svindel forsøger de kriminelle at franarre organisationer penge gennem falske anmodninger om pengeoverførsler. I nogle tilfælde kompromitterer hackerne f.eks. en legitim mailkonto hos en virksomhed eller hos en virksomheds samarbejdspartnere for derefter at manipulere medarbejdere til at overføre penge til de kriminelle. Globalt er BEC-svindel blandt de mest lukrative former for cyberkriminalitet. Også i Danmark fører svindlen til tab. For eksempel blev en dansk kommune ramt af BEC-svindel i 2023, hvor de betalte falske fakturaer for knap halvanden million kroner.

Mod enkeltindivider kommer svindlen bl.a. til udtryk som phishing, der leder til betalingskortmisbrug og netbankindbrud. Cyberkriminelle bruger eksempelvis malware til at opsnappe loginoplysninger, men mange forsøg på svindel mod individer udføres dog også uden brug af cyberangreb. Betalingskort- og netbanksvindel med og uden brug af cyberangreb medfører hvert år betydelige økonomiske tab.

Cyberkriminalitet rammer generelt bredt, og alt fra større organisationer til enkeltindivider kan blive ofre. Det er derfor relevant at beskrive de typiske angrebsmetoder, som cyberkriminelle bruger. Metoderne er dog ikke begrænset til kun at blive brugt til cyberkriminalitet. Også stater udnytter angrebsmetoderne til at opnå deres mål.

Cyberkriminelle udnytter sårbarheder

Cyberkriminelle angriber ofte via kendte sårbarheder i software. En sårbarhed er i denne sammenhæng en svaghed i et stykke software, hackere potentielt kan udnytte til at kompromittere informationssikkerheden. Når en sårbarhed er kendt, vil der typisk komme en opdatering til softwaren, som lukker muligheden for at kompromittere et system via sårbarheden. Gamle sårbarheder bliver dog fortsat udnyttet i høj grad, fordi nogle virksomheder og myndigheder ikke får implementeret opdateringer. CFCS vurderer, at de cyberkriminelle generelt er hurtige til at udnytte nye sårbarheder.

Cyberkriminelle udnytter også sårbarheder, som endnu ikke kan lukkes via en opdatering, altså zero day-sårbarheder. Der var i 2023 adskillige cyberangreb via zero day-sårbarheder. Det er sandsynligt, at nogle kriminelle hackere enten selv opdager zero day-sårbarheder eller køber sig til dem. Kriminelle køber og sælger desuden zero day-sårbarheder for betragtelige summer på undergrundsmarkeder.

Cyberkriminelle kan også finde sårbarheder at udnytte i nye digitale enheder, der fortsat kobles til internettet hos både private og på arbejdspladser. Enhederne går ofte under betegnelsen Internet of Things-enheder (IoT-enheder).

Eksempler er biler, fjernsyn, printere og netværksudstyr. Udbredelsen af enheder tilsluttet internettet medfører en betydelig sikkerhedsrisiko, da IoT-enheder typisk er mere eksponerede og dårligere beskyttede end almindelige computere. Dermed udgør de en relativ direkte indgang til et netværk. Samtidig betyder det øgede antal enheder, at der er flere potentielle angrebsvinkler for de cyberkriminelle.

Kriminelle hackere udnytter også forsyningskæden

Hackere kan gennem leverandører og software-udbydere forsøge at få adgang til kundernes netværk eller systemer. På den måde kan en leverandør eller software-løsning bruges som trædesten for videre cyberangreb. Bliver en leverandør først kompromitteret, kan det potentielt få alvorlige direkte eller indirekte konsekvenser i forsyningskæden. Angreb via forsyningskæden er effektive, fordi hackerne ved at kompromittere ét led potentielt kan få adgang til mange mål.

Udbydere af cloud-løsninger er også attraktive mål for cyberangreb, fordi nogle organisationer i dag flytter deres data til disse løsninger. Cloud-tjenester kan i mange tilfælde være attraktive for virksomheder og myndigheder, da de kan understøtte driften og udviklingen af en organisations it-løsninger. Angreb gennem cloud-udbydere kan derfor have stor rækkevidde, da udbyderen ofte helt eller delvist dækker it-behovene for adskillige kunder.

Phishing

CFCS vurderer, at phishing-mails fortsat er blandt hackeres foretrukne værktøjer. Phishing bliver brugt af alle typer hackere, fordi det virker og er nemt at udføre. Ved phishing forsøger afsenderen at narre mailmodtagere til i god tro at videregive personlige eller andre beskyttelsesværdige oplysninger eller give uretmæssig adgang til bl.a. it-systemer. Det kan blive den indledende adgang for f.eks. en ransomware-aktør.

De kriminelle har brugt phishing længe, men metoden udvikler sig hele tiden. CFCS har tidligere beskrevet, hvordan chatrobotter giver hackere mulighed for at effektivisere produktionen af phishing-mails. Det kan man læse mere om i CFCS' trusselsvurdering "Hackere misbruger generativ AI" på CFCS' hjemmeside.

Udnyttelse af svage eller genbrugte passwords

En anden simpel og effektiv angrebsmetode, cyberkriminelle bruger, er brute force-angreb. Betegnelsen dækker over forskellige typer af angreb, hvor hackere forsøger at gætte kombinationer af brugernavne og passwords. Det kan f.eks. ske ved at udnytte passwords fra tidligere datalæk eller via systematisk gæt af kombinationer fordelt på mange forskellige brugerkonti.

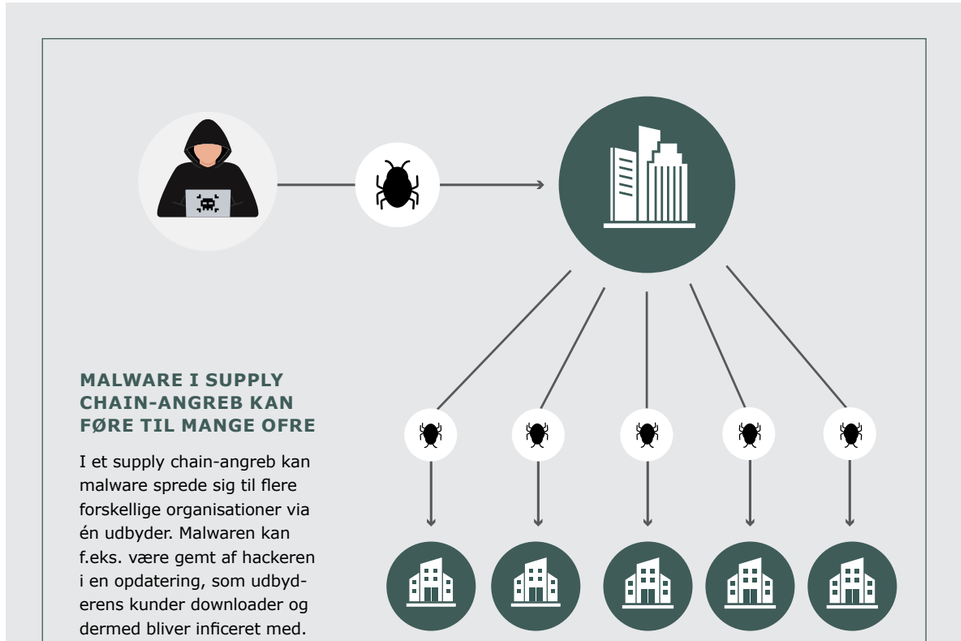
KRIMINELLE HACKERE KOMPROMITTERER VIRKSOMHEDER VERDEN OVER

Flere virksomheder blev i 2023 kompromitteret gennem en hidtil ukendt sårbarhed. Sårbarheden befandt sig i et software-program ved navn MOVEit, som bruges til overførsel af filer. Ved at angribe et udbredt software-program kunne hackerne efterfølgende ramme mange virksomheder. Hackerne misbrugte deres adgang til virksomhedernes systemer til at trække data ud.

Kampagnen er blevet tilskrevet den kriminelle hackergruppe CL0p. CL0p har løbende afpresset ofre ved at offentliggøre offeret ved navn på deres DLS. Danske virksomheder har også været ramt af Cl0ps kampagne.

RANSOMWARE-ANGREB MOD FINSK CLOUD-UDBYDER RAMMER SVENSKE ORGANISATIONER

I januar 2024 blev den finske virksomhed Tietoevry ramt af et ransomware-angreb. Tietoevry leverer bl.a. cloud-hosting til en lang række svenske organisationer. Ransomware-angrebet ramte ifølge udbyderen et af deres svenske datacentre, hvilket påvirkede en række svenske virksomheder. Angrebet satte også en lang række myndigheders fælles lønsystem ud af drift. Ifølge åbne kilder påvirkede angrebet desuden flere kommuner og regioners it-systemer, herunder sundhedsjournalsystemet i Uppsala.



MALWARE I SUPPLY CHAIN-ANGREB KAN FØRE TIL MANGE OFRE

I et supply chain-angreb kan malware sprede sig til flere forskellige organisationer via én udbyder. Malwaren kan f.eks. være gemt af hackeren i en opdatering, som udbyderens kunder downloader og dermed bliver inficeret med.

CYBERAKTIVISME

Truslen fra cyberaktivisme mod Danmark er **HØJ**. Truslen udspringer primært fra pro-russiske cyberaktivister og rammer bredt på tværs af sektorer. De er dog ofte rettet mod finans- og transportsektoren samt Forsvarsministeriets myndighedsområde. Det er meget sandsynligt, at cyberaktivister vil udføre cyberaktivistiske angreb mod danske myndigheder og virksomheder inden for de næste to år.

■ Cyberaktivisme er cyberangreb begået af grupper eller individer med det formål at skabe opmærksomhed omkring deres dagsorden eller budskab. Det er typisk drevet af ideologiske eller politiske motiver. Cyberaktivister kan fokusere på enkeltsager, personer eller organisationer, som de opfatter som modstandere af deres sag.

Cyberaktivisme mod danske mål er blevet en del af normalbilledet

Den høje trussel fra cyberaktivisme mod danske virksomheder og myndigheder er blevet en del af normalbilledet efter Ruslands invasion af Ukraine. Truslen skal både ses i kontekst af Danmarks rolle som bidragsyder af militær støtte til Ukraine og som medlemsland i EU og NATO. Pro-russiske aktivister angriber løbende virksomheder og organisationer i Europa og NATO, som de ser som symbolske for vestlig støtte til Ukraine.

De pro-russiske grupper er et godt eksempel på, hvordan cyberaktivister kan understøtte staters interesser. Det er dog ikke ensbetydende med, at de arbejder direkte for staten. CFCS vurderer, at nogle pro-russiske cyberaktivistiske grupper har forbindelse til den russiske stat.

Den typiske cyberaktivisme er som nævnt drevet af ideologiske eller politiske motiver og bliver som udgangspunkt udført uafhængigt af stater. Det kan dog være vanskeligt at vurdere en cyberaktivistisk aktørs tilhørsforhold til fremmede stater. I nogle tilfælde er det derfor ikke entydigt, om cyberaktivister handler overvejende på eget eller på en stats initiativ.

En gruppe, der har taget ansvar for angreb mod danske mål, er den pro-russiske cyberaktivistiske gruppe NoName057(16). For eksempel hævdede de i februar at have ramt en række danske hjemmesider med overbelastningsangreb.

Selvom truslen fra cyberaktivisme mod Danmark primært udspringer fra pro-russiske aktivister, kan truslen også opstå uden varsel fra andre cyberaktivistiske miljøer. Det var eksempelvis tilfældet ved den internationale opmærksomhed omkring koranafbrændingerne i Danmark og Sverige i starten af 2023. Som reaktion på afbrændingerne iværksatte flere cyberaktivistiske grupper såkaldte Distributed Denial of Service-angreb (DDoS-angreb), som er en type overbelastningsangreb, mod danske og svenske hjemmesider. Samtidig opfordrede de også andre aktivister til at begå cyberangreb mod danske og svenske mål. Overbelastningsangrebene ramte både større og mindre virksomheder og myndigheder i samfundskritiske sektorer. For eksempel blev Nationalbankens hjemmeside ramt og hjemmesider for flere danske hospitaler, herunder Rigshospitalet.

CYBERAKTIVISTERNES VÆRKTØJSKASSE

DDoS

DDoS står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller netværk. Målet er at gøre hjemmesiden eller netværket utilgængelig for legitim trafik, mens angrebet står på. Hvis serveren, der angribes, f.eks. hoster offerets brugervendte hjemmeside, kan et DDoS-angreb gøre hjemmesiden utilgængelig for brugere.

Defacement

Defacement af en hjemmeside er et angreb, der ændrer hjemmesidens visuelle udtryk. Angriberen kan f.eks. indsætte tekst eller et billede på hjemmesidens forside med et særligt budskab.

Hack og læk

Et mål eller delmål med hack og læk-angreb kan være at skade den ramte organisations omdømme. Det kan ske ved at offentliggøre interne dokumenter eller data, der er skaffet fra et kompromitteret system eller netværk.

Angrebene er forstyrrende, men ikke ødelæggende

Cyberaktivister anvender i overvejende grad DDoS- og defacement-angreb mod danske virksomheder og myndigheder. De retter typisk angrebene mod ofrenes brugervendte hjemmesider. Både DDoS-og defacement-angreb kan gøre ofrenes hjemmesider midlertidigt utilgængelige. Ved DDoS-angreb sker det ved, at hjemmesiderne overbelastes med ondsindet trafik, så de ikke kan tilgås. Effekten af defacement-angreb er typisk, at hjemmesidens visuelle udtryk udskiftes med et, aktivisterne indsætter. Begge angrebstyper har en forstyrrende effekt, men er ikke ødelæggende for ofrenes systemer. Nedetiden på ofrenes hjemmesider er med til at skabe omtale af aktivisternes dagsorden.

Begge angrebsformer er relativt simple, og aktivisterne behøver derfor ikke udvikle komplicerede tekniske færdigheder for at gennemføre dem.

Aktivister kan også anvende hack og læk-angreb mod deres ofre. Her lækker aktivisterne dokumenter eller data, som de har skaffet gennem en kompromittering af et system eller netværk. Hack og læk-angreb kan skabe utryghed eller bekymring hos ofrene i forhold til de eventuelle konsekvenser af, at deres data er lækket. Det kan f.eks. have en negativ effekt på tilliden til den ramte organisation fra kunderne. Selve angrebet er dog ikke ødelæggende for offerets systemer.

Cyberaktivister påstår at stå bag destruktive cyberangreb

CFCS vurderer, at visse cyberaktivistiske grupper har intention om at udføre cyberangreb med destruktiv effekt, men at deres kapacitet er begrænset.

CYBERAKTIVISTER VARSLER VOLDSOMT ANGREB – DOG UDEN REEL EFFEKT

Et eksempel på, at cyberaktivister giver misvisende indtryk af deres angreb, er fra sommeren 2023. To pro-russiske grupper varslede, at de i samarbejde med en kendt cyberkriminel gruppe ville rette verdenshistoriens største cyberangreb mod europæiske banker.

Målet var ifølge gruppernes kommunikation på sociale medier at standse vestlig hjælp til Ukraine. Grupperne understregede, at der ikke kun ville være tale om DDoS-angreb. Der blev i den efterfølgende periode kun registreret et fåtal af DDoS-angreb mod europæiske banker. Ingen af angrebene havde betydelig effekt.

Cyberaktivister udgør primært en trussel mod organisationer med svage sikkerhedsforanstaltninger. Svage sikkerhedsforanstaltninger betyder, at selv cyberaktivister med begrænset kapacitet kan kompromittere systemerne. Nogle cyberaktivistiske grupper har påstået at have udført destruktive cyberangreb i forbindelse med konflikter, f.eks. konflikten mellem Israel og Hamas og Ruslands invasion af Ukraine. Det er dog de færreste af angrebene, hvor der er blevet bekræftet en reel effekt.

Flere både bekræftede og ubekræftede angreb har været rettet mod internetvendt operationel teknologi (OT). OT er teknologi brugt til realtidsstyring, monitorering og indsamling af data i fysiske miljøer. Det anvendes primært i industrien, men er også anvendt i mange andre sektorer, f.eks. forsvaret og hospitalsvæsenet. Hvis cyberaktivister kompromitterer OT i organisationer, der forvalter kritisk infrastruktur, kan det få betydelige konsekvenser. Det kan bl.a. påvirke mange mennesker, og kritiske samfundsfunktioner kan blive lukket ned. CFCS følger løbende udviklingen i det cyberaktivistiske trusselsbillede.

CFCS vurderer, at både reelle destruktive cyberangreb og falske påstande om angreb af destruktiv karakter har til hensigt at skabe offentlig opmærksomhed omkring aktivisternes dagsorden. Gennem falske påstande om destruktive angreb opnår aktivisterne opmærksomhed omkring deres sag uden at skulle udvikle kapaciteten til reelt at udføre angrebene.

Cyberaktivisternes kommunikation kan give misvisende trusselsbillede

Cyberaktivisters primære mål er typisk at skabe opmærksomhed omkring deres sag. Derfor spiller omtalen af deres angreb en næsten lige så stor rolle som angrebene i sig selv. Ofte er aktivisternes omtale af deres angreb dog misvisende og overdreven. Den misvisende kommunikation er et redskab, som cyberaktivisterne bruger til at forstærke deres politiske fortælling og den psykologiske effekt af deres cyberangreb.

Cyberaktivisterne bruger bl.a. deres platforme på sociale medier til at overdrive effekten af deres angreb. Her beskriver de f.eks. simple overbelastningsangreb mod brugervendte hjemmesider som hændelser, der giver driftsforstyrrelser i kritisk infrastruktur, selvom dette ikke er tilfældet i praksis.

FØLG OS PÅ

X@Cybersikkerhed

LinkedIn@Centre for Cyber Security

DESTRUKTIVE CYBERANGREB

Truslen fra destruktive cyberangreb mod Danmark er **MIDDEL**. CFCS hævede i juni 2024 niveauet fra **LAV** til **MIDDEL**. Niveauet blev hævet, fordi det er sandsynligt, at Rusland er blevet mere risikovillig i forhold til at bruge hybride virkemidler med destruktive effekter i europæiske NATO-lande. CFCS vurderer, at denne risikovillighed også omfatter destruktive cyberangreb.

■ Det er dog mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod Danmark, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.

Det er primært mindre omfattende destruktive cyberangreb, trusselsniveauet relaterer sig til. Det kan f.eks. være angreb, der påvirker samfundsvigtige funktioner i begrænset omfang. Den type angreb kan dog stadig få betydelige konsekvenser for offeret og for samfundet. Selv hvis destruktive cyberangreb ingen konsekvenser har for samfundsvigtige funktioner, kan de skabe utryghed og påvirke samfundet.

Selvom det er mindre sandsynligt, at Rusland vil gennemføre destruktive cyberangreb med alvorlige og omfattende konsekvenser, vurderer CFCS alligevel, at hackergrupper knyttet til Rusland løbende forbereder sig på at kunne udføre den angrebstype mod Danmark. Sandsynligheden for, at disse angreb finder sted, kan derfor stige med kort eller uden varsel – særligt hvis konflikten mellem Rusland og Vesten eskalerer eller ændrer karakter.

I det tilfælde kan mål være systemer i kritisk infrastruktur. Hvis disse ikke fungerer, kan det påvirke f.eks. Forsvarets evne til at løse opgaver eller på anden måde påvirke befolkningens og det politiske systems modstandskraft i forbindelse med en eskalerende konflikt med Rusland.

CFCS' DEFINITION AF DESTRUKTIVE CYBERANGREB

CFCS 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.

Truslen kommer primært fra Rusland

Hvis Danmark i den nuværende situation bliver ramt af et destruktivt cyberangreb, er det mest sandsynligt, at Rusland vil stå bag angrebet. Truslen fra destruktive cyberangreb kommer særligt fra russiske statslige hackere, men også ikke-statslige hackere med forskellige grader af forbindelser til den russiske stat udgør en trussel.

Destruktive cyberangreb er ét blandt flere hybride virkemidler, Rusland kan bruge til at opnå strategiske fordele. Ruslands overordnede formål med at bruge hybride virkemidler mod Vesten er at stresse beslutningstagere og befolkninger. Det kan de bl.a. gøre ved at skabe forvirring og usikkerhed.

CFCS vurderer, at Rusland i den nuværende situation vil forsøge at sløre, at de står bag destruktive cyberangreb. Dermed vil Rusland forsøge at gøre det vanskeligt for lande, der rammes af Ruslands hybride aktiviteter, at reagere med et modsvar. Modsvar kan blive mere komplicerede, hvis Ruslands involvering ikke er tydelig. Rusland kan eksempelvis sløre sine angreb ved at udføre ransomware-angreb, der ligner kriminelle angreb, hvor data bliver krypteret, men efterfølgende ikke kan dekrypteres. Der har tidligere været eksempler på sådanne falske ransomware-angreb.

Det er dog meget sandsynligt, at de ransomware-angreb, der har ramt danske organisationer inden for de seneste år, har været udført af kriminelle hackere, hvis formål var at tjene penge og ikke at ødelægge data eller infrastruktur. CFCS forventer, at ransomware-angreb også fremover i langt de fleste tilfælde vil blive udført af økonomisk motiverede kriminelle hackere.

Statslige hackere kan også forsøge at skjule deres forbindelse til destruktive angreb ved at udgive sig for at være aktivistiske hackere. Det kan de gøre ved f.eks. at oprette hjemmesider eller konti på forskellige platforme under dække af at være cyberaktivister, hvor de tager ansvar for destruktive cyberangreb.

En anden måde, Rusland kan sløre sin involvering i destruktive cyberangreb, er ved at forsøge at få andre aktører til at udføre angrebene for dem. Derfor er der også en potentiel trussel fra ikke-statslige hackere.

Som nævnt i kapitlet om cyberaktivisme vurderer CFCS, at visse cyberaktivister har intention om at udføre destruktive cyberangreb, men at de primært udgør en trussel mod systemer med svage sikkerhedsforanstaltninger.

FREMMEDE STATER KAN UDFØRE BÅDE SIMPLE OG AVANCEREDE DESTRUKTIVE CYBERANGREB

Destruktive cyberangreb kan blive udført med mere eller mindre avancerede kapaciteter. Hackere kan f.eks. udnytte udbredte sårbarheder til at udføre simple wiper-angreb mod dårligt beskyttede mål. Denne type angreb kræver ikke nødvendigvis lang tids forberedelelse.

Mere avancerede og målrettede destruktive cyberangreb kræver typisk længere tids forberedelse.

Formålet med angreb er sandsynligvis at påvirke befolkningen
Det er sandsynligt, at eventuelle russiske destruktive cyberangreb primært vil have til formål at påvirke befolkningen og beslutningstagere, herunder at svække den danske støtte til Ukraine.

Fordi formålet med angreb vil være påvirkning, vurderer CFCS, at mange typer af organisationer i samfundsvigtige sektorer vil kunne blive valgt som mål for eventuelle destruktive cyberangreb. I Ukraine i tiden efter Ruslands invasion i 2022 blev alt fra supermarkeder til statslige myndigheder udsat for hyppige destruktive cyberangreb. Formålet med de fleste af angrebene var sandsynligvis at stresse og belaste det ukrainske samfund.

Selvom destruktive cyberangreb umiddelbart har til formål at destruere noget, kan angrebene også være et værktøj til at opnå andre større strategiske mål, hvor den destruktive effekt er sekundær. I den nuværende situation er det sandsynligt, at den konkrete fysiske effekt af eventuelle angreb mod Danmark netop vil være sekundær for hackerne, der udfører det. I stedet vil det primære mål være, at angrebene skaber bred opmærksomhed.

Andre stater har også kapacitet til at udføre destruktive cyberangreb
Flere fremmede stater har kapacitet til at udføre destruktive cyberangreb. Selvom truslen primært kommer fra Rusland, udgør Iran også en potentiel trussel. Det er sandsynligt, at Iran tidligere har udført destruktive cyberangreb mod vestlige mål.

Eksempelvis har en gruppe under navnet CyberAv3ngers taget ansvar for en række destruktive cyberangreb mod dårligt beskyttet OT-udstyr i vestlige lande. Her udpegede gruppen alt udstyr produceret i Israel som legitime mål i forbindelse med konflikten mellem Israel og Hamas.

Den amerikanske myndighed Cybersecurity and Infrastructure Security Agency (CISA) har offentligt knyttet CyberAv3ngers til Irans Revolutionsgarde (IRGC). USA har desuden sanktioneret seks personer fra IRGC grundet gruppens destruktive cyberangreb mod amerikanske mål. Angrebene er eksempler på, at statslige hackere slører deres angreb som aktivisme.

Kina anvender primært landets omfattende cyberkapaciteter til at udføre cyberspionage. Det er meget sandsynligt, at Kina også har kapacitet til at udføre destruktive cyberangreb. Det er dog usandsynligt, at Kina aktuelt har intentioner om at udføre destruktive cyberangreb mod danske mål. I en mere tilspidset konflikt kan sandsynligheden for, at Kina vil bruge destruktive cyberangreb, ændre sig. I sådan et tilfælde vil Kina sandsynligvis rette angreb mod lande, der ventes at være modstandere i forbindelse med en eventuel fremtidig konflikt. Det kunne f.eks. være lande i nærområdet eller lande, der med stor sandsynlighed vil støtte Taiwan i en eventuel krig mellem Kina og Taiwan.

DESTRUKTIVT CYBERANGREB HAVDE BEGRÆNSEDE EFFEKTER

Destruktive cyberangreb kan have meget forskellige effekter alt efter, hvilket mål de rettes mod, og hvordan de udføres. Som nævnt er det mindre sandsynligt, at Rusland i den nuværende situation vil gennemføre destruktive cyberangreb mod Danmark, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner. Mindre omfattende angreb kan dog også påvirke samfundsvigtige funktioner.

Et eksempel på et destruktivt cyberangreb, hvor påvirkningen af samfundsvigtige funktioner var relativt begrænset, fandt sted i Irland i december 2023. Angrebet var mod et vandværk, og ifølge medierne forstyrrede det knap 200 irske husstandes vandforsyning i to dage. I angrebet blev vandværkets computere også defacet med en anti-israelsk besked.

VOLT TYPHOON HAR UDFØRT CYBERSPIONAGE MOD MÅL I KRITISK INFRASTRUKTUR I USA

I februar og senere i marts 2024 udsendte CISA, NSA, FBI og en række andre amerikanske myndigheder og internationale partnere i fællesskab varsler mod hackergruppen Volt Typhoon. Ifølge varslerne er gruppen en kinesisk statsstøttet gruppe, der har gået efter mål i kritisk infrastruktur.

Flere medier skriver, at gruppen har været aktiv siden midten af 2021 og muligvis længere, hvor de løbende har kompromitteret systemer og forsøgt at bibeholde adgang. Blandt andet har de gået efter mål i transport-, spildevands- og energisektoren i USA og Guam, som er en del af amerikansk territorie.

Amerikanske myndigheder vurderer, at Volt Typhoon har kompromitteret målene med henblik på senere at kunne bevæge sig fra it-systemer videre til OT-systemer for efterfølgende at udføre angreb af destruktiv karakter. Myndighederne vurderer, at gruppen vil gøre brug af destruktive cyberangreb i tilfælde af geopolitiske spændinger og militære konflikter mellem USA eller dets allierede og Kina.

LÆS MERE
Se flere trusselsvurderinger på
cfcs.dk

CYBERTERROR

Truslen fra cyberterror mod Danmark er **INGEN**. CFCS vurderer, at ingen aktører aktuelt har kapacitet til eller intention om at udføre cyberterror. Det er derfor usandsynligt, at danske myndigheder og virksomheder inden for de næste to år vil blive udsat for forsøg på cyberterror.

■ CFCS har ikke kendskab til eksempler på cyberterror. CFCS har fulgt truslen fra cyberterror siden 2016 med fokus på militante ekstremister. Det sker med fokus på eventuelle ændringer i både kapacitet og intention med henblik på, at disse aktører vil kunne udføre cyberterror.

CFCS definerer cyberterror som alvorlige politisk motiverede cyberangreb, der har til hensigt at skabe samme effekt som mere konventionel terror. Cyberterror kan f.eks. komme til udtryk i form af cyberangreb, der forårsager fysisk skade på mennesker eller materiel.

Center for Terroranalyse (CTA) ved PET vurderer for nuværende, at truslen fra konventionel terror mod Danmark og danske interesser er i niveauet alvorlig, som er niveau 4 ud af 5.

CTA vurderer, at den konventionelle terrortrussel mod Danmark særligt udspringer fra militante islamister og i mindre grad højreekstremister, antimyndighedsekstremister og venstreekstremister. CTA vurderer desuden, at et terrorangreb mest sandsynligt vil komme fra soloterrorister eller mindre grupper af personer, der benytter lettilgængelige midler.

CFCS vurderer, at sådanne personer og grupper hverken besidder kapacitet til eller intention om at udføre alvorlige cyberangreb for at opnå samme effekt som konventionel terror.

FØLG OS PÅ

X@Cybersikkerhed

LinkedIn@Centre for Cyber Security

PERSPEKTIV:

FRA CYBERTRUSSEL TIL CYBERSIKKERHED – DET EVIGE KAPLØB MOD HACKERNE

De forudgående kapitler understreger, at Danmark er udsat for en trussel fra flere forskellige typer af cyberangreb. Det følgende kapitel giver derfor en overordnet introduktion til, hvordan fokus på cybersikkerhed kan være med til at bremse hackerne, når de forsøger at kompromittere systemer.

Kapitlet berører nogle generelle tiltag og tematikker, som kan gøre en forskel på cybersikkerhedsområdet. Cybersikkerhed er dog et løbende arbejde, der bør være tilpasset den enkelte organisation og udvikle sig i takt med truslen.

Simple angrebsmetoder skal gøres ineffektive

Viden om cybertruslen kan hjælpe organisationer med at prioritere sikkerhedstiltag. Simple angrebsmetoder er desværre stadig effektive værktøjer for både stater og cyberkriminelle. Mange organisationer er udfordret af, at nogle basale sikkerhedsforanstaltninger enten ikke er på plads eller er svære at vedligeholde. Så længe disse foranstaltninger ikke er implementeret, kommer hackerne til at udnytte sikkerhedshullerne.

Cybersikkerhed er dog kommet på dagsordenen, og der foregår vigtigt og nødvendigt arbejde med sikkerhed i mange danske organisationer. Flere initiativer er på vej, og bl.a. implementeringen af NIS2-direktivet vil bidrage til arbejdet med cybersikkerhed i en bred del af samfundet, ikke bare i Danmark, men i hele EU.

Medarbejdere under angreb skal trænes og hjælpes

Uanset hvilke sikkerhedstiltag der bliver implementeret, kan medarbejdere fortsat udgøre en potentiel vej ind i enhver organisation. Medarbejdere, og særligt deres interaktion med hackere via phishing-mails, spiller en central rolle i langt de fleste cyberangreb.

Organisationer bør derfor løbende oplyse og træne medarbejdere i cybersikkerhed, lige fra de starter. Arbejdet skal understøttes af politikker og tiltag, som it-sikkerhedsorganisationen og ledelsen har ansvaret for. Det gælder både organisatoriske, teknologiske, adfærdsmæssige og fysiske tiltag. Ledelsen bør også fremme en sikkerhedskultur, hvor medarbejdere tør sige, hvis de har begået fejl, og bl.a. ved, hvem de skal orientere.

Understøt stærke passwords

Passwords illustrerer samspillet mellem oplysning og teknisk understøttelse af medarbejdere. På den ene side er det ofte medarbejderens ansvar at lave et stærkt og unikt password, som kun de kender til. På den anden side bør organisationen oplyse medarbejderen om password-sikkerhed og sætte tekniske krav til passwords, der understøtter medarbejderen i at lave et stærkt password. Organisationen kan også understøtte medarbejderne ved at gøre brug af en godkendt password-manager. En password-manager er software, der på sikker vis kan opbevare brugerens mange unikke og stærke passwords. Dermed skal brugeren kun huske ét meget stærkt password: det til password-manageren.

Brug flerfaktor-autentifikation

Flerfaktor-autentifikation er et eksempel på et andet effektivt sikkerhedstiltag, der kan hjælpe medarbejdere og organisationer. Når virksomheder, myndigheder og individer bruger flerfaktor-autentifikation på deres mailkonti eller i kritiske systemer, besværliggør de nogle af hackernes foretrukne angrebsmetoder. De fjerner bl.a. hackernes mulighed for at udnytte brute force-angreb, hvor hackerne forsøger automatiseret at gætte eller bryde svage eller genbrugte passwords. Flerfaktor-autentifikation gør det også sværere for hackerne at misbruge login-oplysninger, som de har fået adgang til via phishing- eller spear phishing-mails.

Flerfaktor-autentifikation kunne have forhindret mange succesfulde cyberangreb. Det er bl.a. cyberangreb, der efterfølgende har haft alvorlige konsekvenser for de berørte organisationer og i visse tilfælde for Danmark bredere set.

Opdater software

Et andet sted, virksomheder, myndigheder og individer kan sætte ind, er ved at opdatere software i videst muligt omfang, når leverandøren frigiver nye versioner eller sikkerhedsopdateringer. Det inkluderer bl.a. at opdatere operativsystemer, applikationer og firmware på f.eks. mobile enheder, IoT-enheder og servere. Software bør opdateres snarest muligt efter frigivelse af nye opdateringer, da hackerne hurtigt kan udnytte kendte sårbarheder.

Hvis det er muligt, bør automatiske opdateringer desuden være slået til. I de tilfælde, hvor det ikke kan lade sig gøre, er det vigtigt at orientere sig om, hvilke alvorlige sårbarheder hackere aktivt udnytter. Organisationen bør også sikre en procedure for at mindske risikoen for, at en sårbarhed kan udnyttes, indtil det er muligt at opdatere. Det kan eksempelvis være ved at adskille den sårbare enhed fra organisationens øvrige systemer eller afkoble enheden fra internettet. Denne tilgang kan også være relevant, når hackere udnytter zero day-sårbarheder.

Når hackerne alligevel overhaler os

Det er ikke altid et spørgsmål om, *hvorvidt* en myndighed eller virksomhed bliver ramt, men et spørgsmål om, *hvornår* de bliver ramt. Med den rette forberedelse vil organisationer øge chancerne for, at de kan nå at

FLERFAKTOR-AUTENTIFIKATION KUNNE HAVE STOPPET ALVORLIGT RANSOMWARE-ANGREB

Den amerikanske virksomhed Colonial Pipeline blev i 2021 ramt af et ransomware-angreb. Angrebet startede ved, at hackerne brugte et stjålet password til at logge ind på en af virksomhedens VPN-konti, hvor der ikke var tilknyttet flerfaktor-autentifikation.

På grund af angrebet lukkede virksomheden midlertidigt ned for store dele af en rørledning, der transporterede brændstof langs den amerikanske østkyst. Det fik store konsekvenser, da nedlukningen af rørledningen bl.a. påvirkede oliepriser og førte til mangel på benzin i området.

opdage hackerne og inddæmme skaden. I bedste fald vil organisationerne helt kunne forhindre hackerne i at opnå deres mål.

Det er vigtigt, at ledelsen understøtter, at organisationen kan håndtere kompromitteringer. Det kan de bl.a. gøre ved at få udarbejdet og løbende øvet en beredskabsplan og plan for, hvordan virksomheden drives videre i en krisesituation. Andre tiltag er mere tekniske, men kræver også ledelsens opbakning. Det er tekniske tiltag som f.eks. en velfungerende backup. Langt de fleste kender til dette tiltag, fordi ransomware-angreb gentagne gange har understreget værdien af en velfungerende backup. Ved at have backup offline eller offsite vil det være betydeligt vanskeligere for ransomware-aktører at kryptere selve backuppen.

Andre tekniske tiltag som monitorering, segmentering og rettigheds- og adgangsstyring fortjener dog også større bevågenhed, da de vil kunne stoppe mange ransomware-aktører og statslige aktører i at nå deres mål.

CFCS og it-sikkerhedsfirmaer oplever desuden ofte at mangle de logs, der er nødvendige for at kunne afdække hændelsesforløbet i en konkret sag. Logning er en del af et godt cyberforsvar. Det er logs, der bl.a. gør det muligt at undersøge, hvor, hvornår og hvordan hackerne er kommet ind og har bevæget sig rundt i en organisations systemer.

Fra cybertrussel til risikovurdering

Det er den enkelte organisations ansvar at vurdere, hvordan den vil prioritere og håndtere sikkerhed inden for lovens rammer og øvrige krav samt organisationens mål og ønsker. Sikkerhed er nemlig ikke gratis og kan også ske på bekostning af f.eks. tilgængelighed. Viden om cybertruslen er ét aspekt i en sådan risikovurdering, som hjælper organisationen med at prioritere ressourcer og sikkerhedstiltag. Viden om organisationens drift og prioriteter er den anden del.

Selvom alle kan blive udsat for cyberangreb, særligt fra cyberkriminelle, er truslen større for visse myndigheder og virksomheder. Statslige hackere har traditionelt et særligt fokus på organisationer, der arbejder med udenrigs-, sikkerheds- og forsvarspolitik. De avancerede cyberkriminelle, som CFCS har særligt fokus på, opererer mere opportunistisk. Blandt andet spiller organisationernes omsætning en rolle i forhold til, hvor attraktive mål de udgør for afpresning og svindel.

Denne vurdering giver den overordnede status på cybertruslen mod Danmark. Derudover findes der flere trusselsvurderinger på CFCS' hjemmeside, som dykker ned i delelementer af trusselsbilledet. CFCS udgiver desuden løbende nye trusselsvurderinger.

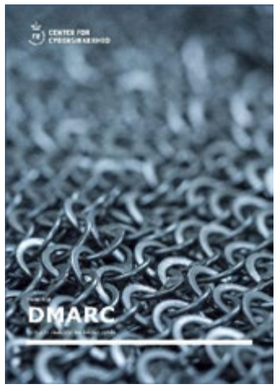
På CFCS' hjemmeside ligger også vejledninger til at højne cybersikkerheden. Det er bl.a. "Cyberforsvar der virker", som går i dybden med sikkerhedstiltag nævnt i dette kapitel. Vejledningen indeholder desuden anbefalinger i forhold til håndtering af de risici, der opstår som følge af de cybertrusler, en organisation står over for.

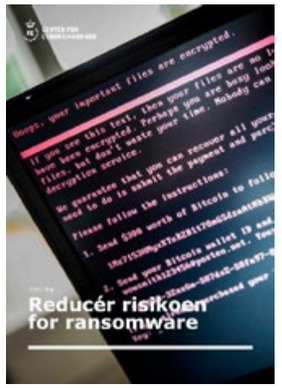
OUTSOURCING AF SIKKERHED, MEN IKKE ANSVAR

Mange organisationer outsourcer driften af deres it, herunder it-sikkerhedsopgaver. Det fritager dog ikke organisationen for ansvaret for sikkerheden. Det er organisationen selv, der skal stille de relevante krav til deres leverandører af it-drift og eventuel it-sikkerhed. De skal desuden selv løbende følge op på, om kravene er opfyldt og stadig er effektive og tilstrækkelige.

Læs flere råd i CFCS' vejledning "Cybersikkerhed i leverandørforhold" på CFCS' hjemmeside.

LÆS OGSÅ CFCS' ØVRIGE VEJLEDNINGER





FØLG OS PÅ

X@Cybersikkerhed

LinkedIn@Centre for Cyber Security

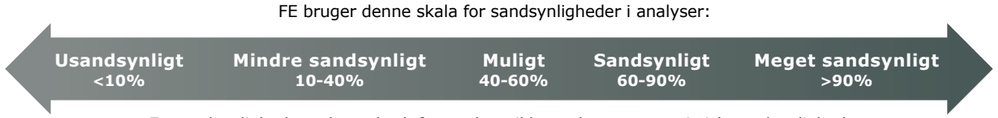
TRUSSELSNIVEAUER

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 waktivitet.
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 FE's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.

FE bruger denne skala for sandsynligheder i analyser:



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

CYBERTRUSLEN MOD DANMARK 2024

Udgivelse
August 2024

Foto
Forside, DRONERUNE
Side 10 og 29, SCANPIX

CENTER FOR CYBERSIKKERHED

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
www.cfcs.dk
www.fe-ddis.dk