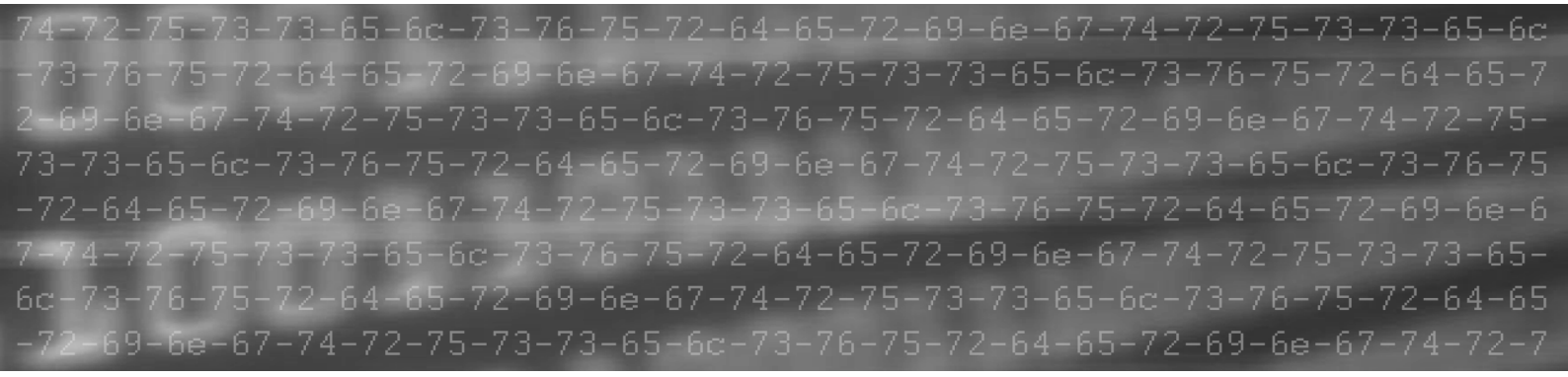
CENTER FOR
CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod Danmark



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Maj 2018

CENTER FOR CYBERSIKKERHED

Cybertruslen mod Danmark 2018

Formålet med denne årlige, nationale trusselsvurdering er at redegøre for den samlede cybertrussel, der møder danske myndigheder og private virksomheder. Truslen er størst fra cyberspionage udført af stater og fra cyberkriminalitet. Truslen er under fortsat udvikling.

Hovedvurdering

- Truslen fra cyberspionage er **MEGET HØJ**. Truslen er især rettet mod danske myndigheder, som har oplysninger, der er strategisk, politisk eller økonomisk værdifulde for fremmede stater. Visse stater udfører også cyberspionage mod danske virksomheder. Stater gør generelt mere for at skjule deres cyberspionage.
- Truslen fra cyberkriminalitet er **MEGET HØJ**. Cyberkriminalitet er et globalt fænomen, der også rammer danske myndigheder, virksomheder og borgere. Der er særligt en betydelig trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra myndigheder, virksomheder og borgere. Der er cyberkriminelle netværk, der arbejder organiseret og langsigtet, og statsstøttede hackere står sandsynligvis også bag cyberkriminalitet.
- Truslen fra cyberaktivisme er **MIDDEL**. Cyberaktivister retter sjældent fokus på danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige evner og ressourcer til at udføre cyberangreb. Det er sandsynligt, at stater også anvender visse cyberaktivistiske grupper som dække i forsøg på at påvirke meningsdannelsen i andre lande.
- Truslen fra cyberterror er **LAV**. Militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb. Selv om de i få tilfælde har ytret interesse for at udføre cyberterror, har de aktuelt ikke kapacitet til dette.
- Visse stater bruger cyberangreb til at styrke deres magtposition. Det gælder bl.a. anvendelsen af destruktive cyberangreb og hack og læk af politisk følsomt materiale. Danske virksomheder og organisationer er udsat for en større risiko for destruktive cyberangreb, hvis de er til stede i visse konfliktområder.

Indledning

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Anden brug af internettet med ondsindet formål, såsom rekruttering til terrorgrupper via sociale medier eller salg af narkotika på internettet, indgår ikke i denne definition af cybertrusler.

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål anvendelsen af cyberangreb har for de aktører, der udgør en cybertrussel. CFCS beskriver og vurderer her aktiviteter, der har til formål at udføre eller begå cyberspionage, cyberkriminalitet, cyberaktivisme eller cyberterror. Desuden beskriver CFCS staters brug af destruktive cyberangreb.

Trusselsniveauerne er baseret på en analyse af aktørernes intention og cyberkapaciteter. CFCS vurderer en aktørs cyberkapacitet ud fra de menneskelige og materielle ressourcer, aktøren har til rådighed. Det kan være teknisk dygtige hackere og udviklere af malware eller viden om mål, der kan bruges til eksempelvis social engineering. Det kan også være it-infrastruktur, tid, penge og adgang til information. Hvor stor en cyberkapacitet, en aktør har, vil derfor afhænge af flere forskellige forhold og aktørens evne til at udnytte dem.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede, som har en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Kapitlet om cyberkriminalitet er afstemt med Nationalt Cybercrime Center ved Rigspolitiet, og kapitlet om cyberterror er afstemt med Center for Terroranalyse ved Politiets Efterretningstjeneste.

Cyberspionage

Truslen fra cyberspionage er **MEGET HØJ**.

Flere lande har væsentlige cyberkapaciteter, som benyttes til at spionere mod andre lande, herunder mod Danmark. Cyberspionage udgør en sikkerhedspolitisk og samfundsøkonomisk trussel mod Danmark og danske interesser. Der er tale om en særdeles aktiv trussel fra enkelte stater, der løbende forsøger at stjæle informationer fra danske myndigheder og virksomheder.

Truslen mod danske myndigheder vil gælde på langt sigt og er dermed et grundvilkår for myndighederne. Sammenlignet med traditionel spionage udført af eksempelvis menneskelige agenter er

cyberspionage en relativt risikofri måde for fremmede stater til at indhente informationer på. Staterne kan potentielt tiltvinge sig adgang til netværk over hele verden, og ofte er deres angreb svære at opdage. Derudover kan staterne med relativt enkle metoder sløre, hvem der står bag, og derved modvirke tilskrivning og sanktioner, hvis angrebene bliver opdaget. Derfor vil stater med evnen og ressourcerne til at udføre cyberspionage fortsætte med at angribe mål af strategisk, sikkerhedspolitisk og økonomisk relevans.

Truslen fra cyberspionage er især rettet mod de danske myndigheder, der ligger inde med oplysninger af strategisk, politisk og økonomisk betydning. Fremmede stater går særligt vedholdende efter myndigheder med betydning for dansk udenrigs-, forsvars- og sikkerhedspolitik. Der er således løbende forsøg på cyberspionage mod Udenrigsministeriet og dets repræsentationer i udlandet. Der er ligeledes vedholdende forsøg mod Forsvarsministeriet og dets myndighedsområde samt danske institutioner og individer, der er tilknyttet Forsvaret og NATO-samarbejdet.

Truslen fra cyberspionage er ikke geografisk afgrænset på samme måde som f.eks. fysiske trusler. Fremmede stater kan eksempelvis udføre cyberspionage mod danske udsendte styrker ved at kompromittere myndigheder og stabe i Danmark. En fremmed stat kan også få vigtige oplysninger om forsvaret i Danmark ved at kompromittere udsendte danske styrker.

Det samme gælder danske diplomatiske repræsentationer i udlandet. Dels kommer truslen mod danske repræsentationer fra stater, der ønsker at spionere mod Danmark og dansk udenrigspolitik. Dels kommer truslen fra stater, der ønsker at bruge danske repræsentationer som et springbræt til at spionere mod det land eller den region, repræsentationen ligger i. Cyberspionagen mod danske repræsentationer kan bl.a. have det formål at finde ud af, hvilke lokale organisationer og personer ambassaden har kontakt med. Nogle danske repræsentationer kan også have fremmede staters interesse, fordi de har en rolle i internationale organisationer.

Danske virksomheder udsættes for økonomisk motiveret cyberspionage

Visse stater udfører også cyberspionage mod danske virksomheder. Industrispionage via internettet er en attraktiv måde for stater at høste fordele af den viden og teknologi, som andre har brugt ressourcer på at udvikle. Fremmede stater vil derfor fortsætte med at indsamle data og stjæle intellektuel ejendom, så længe det kan understøtte staternes økonomiske interesser eller sikre deres virksomheder fordele på det internationale marked. Truslen er derfor særligt rettet mod forskningstunge virksomheder, men kan også være rettet mod virksomheder, der eksempelvis er i kraftig vækst på internationale markeder, aktive i konfliktområder eller som driver virksomhed inden for strategiske ressourcer såsom olie og gas.

De statsstøttede hackergrupper retter desuden deres cyberangreb mod virksomheder og underleverandører, som de kan bruge som springbræt til informationer, der tilhører deres egentlige mål. Den stigende brug af underleverandører og outsourcing af drift eller infrastruktur kan øge danske

myndigheders og virksomheders sårbarhed over for truslen fra cyberspionage. Det skyldes, at underleverandører ofte har direkte adgang til følsomme data hos deres kunder.

Enkelte statsstøttede hackergrupper har i 2017 specifikt rettet deres opmærksomhed mod underleverandører, der tilbyder forskellige cloudløsninger og datalagertjenester til kunder i hele verden. Ved at kompromittere disse underleverandører har staterne haft fjernadgang direkte ind i kundernes netværk, hvorfra de har kunnet stjæle informationer. Fordi staterne misbrugte underleverandørernes betroede netværk og brugte legitime brugernavne og kodeord, har det været vanskeligt for ofret at skelne mellem legitim og illegitim aktivitet. I visse tilfælde har aktørerne også haft adgang til de kundedata, der lå på underleverandørernes egne servere.

Andre statsstøttede hackergrupper er specifikt gået efter større vestlige advokat- og rådgivningsfirmaer inden for investeringsbranchen for derved at få adgang til relevante og ofte følsomme oplysninger fra virksomhederne selv og deres kunder.

Cyberspionage hænger sammen med andre trusler
CFCS vurderer, at andre landes sikkerheds- og efterretningstjenester typisk står bag udførelsen af cyberspionage. Cyberspionage er for disse sikkerheds- og efterretningstjenester ét af flere mulige værktøjer i indhentningen mod myndigheder og virksomheder i Danmark.

Cyberspionage kan derfor være forbundet til mere traditionelle former for spionage. Fremmede tjenester kan i deres cyberangreb eksempelvis misbruge informationer, som er tilgængelige på sociale medier, eller som de indhenter fra menneskelige kontakter. Informationer fra cyberspionage kan også benyttes til at støtte andre former for spionage.

Cyberspionage kan desuden understøtte andre typer cyberangreb og trusler. Cyberspionage kan give en modstander adgang til følsomme oplysninger, der senere kan bruges til afpresning eller lækkes til offentligheden med henblik på at påvirke meningsdannelsen. Cyberspionage kan også anvendes forud for destruktive cyberangreb, særligt hvis cyberspionagen giver adgang til kritiske systemer eller informationer af relevans for det destruktive angreb. En allerede kompromitteret virksomhed eller myndighed er derfor mere sårbar over for denne type trusler.

Ofte udføres cyberspionagen af statsansatte hackere, der arbejder direkte for sikkerheds- og efterretningstjenester. Nogle stater udliciterer dog arbejdet til hackergrupper eller legitime it-sikkerhedsfirmaer, der tilbyder eksempelvis sårbarhedsscanninger og rådgivning om it-sikkerhed. Ved at gøre brug af mellemmænd kan staterne nemmere skjule deres involvering og mere overbevisende benægte at have kendskab til cyberspionagen.

Flere lande har væsentlige cyberkapaciteter

Flere lande har opbygget cyberkapaciteter, der udgør en enten aktiv eller potentiel trussel mod Danmark. De herunder nævnte lande har meget væsentlige cyberkapaciteter, der især anvendes til cyberspionage, men også andre typer politisk og økonomisk motiverede cyberangreb.

Rusland
Rusland er fortsat en førende og yderst aktiv aktør på cyberområdet. Den russiske stat råder over omfattende kapacitet til at udføre cyberspionage og destruktive cyberangreb, der kan understøtte Ruslands strategiske og sikkerhedspolitiske interesser samt landets militære operationer. Rusland bruger betydelige kræfter på at fremme sine interesser i Vesten og anvender også cyberangreb til dette formål.

Kina
Kina råder over avancerede cyberkapaciteter, som landet anvender både defensivt og offensivt. Kina har netop reorganiseret sine militære cyberkapaciteter. Det vil sandsynligvis medføre, at kinesiske aktører vil udføre mere sofistikeret cyberspionage, som er sværere at opdage. Kinesiske efterretningstjenester er flere gange blevet beskyldt for at have stået bag omfattende cyberspionage mod offentlige myndigheder og private virksomheder i hele verden. Efter en kortvarig nedgang i aktivitetsniveau mellem 2016 og 2017 benytter Kina igen aktivt sin cyberkapacitet.

Iran
Iran har de seneste år udviklet sin evne til at gennemføre cyberangreb. Ud over cyberspionage har iranske hackergrupper muligvis stået bag simple destruktive cyberangreb, der slettede data. De pågældende angreb var bl.a. rettet mod kemi-, olie og gasindustrien i Saudi-Arabien og Qatar.

Nordkorea
Nordkorea har gennem flere år udviklet en væsentlig evne til at gennemføre forskellige typer cyberangreb, herunder simple destruktive angreb, der sletter data. Disse angreb har især været rettet mod Sydkorea, men Nordkorea er sandsynligvis også villig og i stand til at udføre større cyberangreb mod mål i andre lande. Der er desuden sandsynligt, at Nordkorea beriger sig via cyberkriminalitet i udlandet.

Andre stater
Også andre lande udvikler evnen til at udføre særligt cyberspionage. Der er i de seneste år dukket nye regionale aktører op i bl.a. Latinamerika, Mellemøsten, Sydasien og Sydøstasien. Mens disse aktører som udgangspunkt fokuserer på lande i deres respektive nærområde, kan truslen også være rettet mod danske virksomheder eller diplomatiske repræsentationer, der er til stede i den pågældende region.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ**.

Cyberkriminalitet er et globalt fænomen, der også rammer danske myndigheder, virksomheder og borgere. Cyberkriminalitet krydser ofte landegrænser, og nogle cyberkriminelle grupper og netværk har ofre verden rundt.

I denne trusselsvurdering dækker begrebet cyberkriminalitet i udgangspunktet tilfælde, hvor personer og netværk bruger cyberangreb til at begå kriminelle handlinger, hvor formålet er berigelse. Det er eksempelvis tyveri af penge eller finansielle og personlige oplysninger, bedrageri og afpresning.

For både danske myndigheder, virksomheder og borgere vil cyberkriminalitet også på langt sigt udgøre en meget høj trussel. Cyberkriminelle er opfindsomme i deres forsøg på at berige sig og anvender mange forskellige typer cyberangreb, hvoraf en del bliver mere avancerede og komplekse.

Der er cyberkriminelle netværk, der arbejder organiseret og langsigtet. Nogle cyberkriminelle grupper kan udføre målrettede og avancerede cyberangreb, hvor de f.eks. stjæler fra eller afpresser myndigheder og virksomheder for meget høje pengebeløb. Andre netværk har specialiseret sig i angreb, der er i stand til at kompromittere et meget stort antal ofre verden over. Mens disse angreb teknisk set ikke er så avancerede, er der tale om velorganiserede, gentagne angreb i næsten industriel skala.

De mere målrettede og avancerede angreb har på verdensplan især ramt finanssektoren og sundhedssektoren. Cyberkriminelles aktiviteter dikteres dog af muligheden for indtjening, og de er ofte tilpasningsdygtige og hurtige til at finde nye metoder, ofre og indtægtskilder. Cyberkriminelle udviser eksempelvis stigende interesse i at stjæle kryptovalutaer, sandsynligvis som konsekvens af den stigende værdi af disse.

Cyberkriminalitet rangerer fra sofistikerede angreb mod f.eks. finansielle systemer til simple cyberangreb og bedrageriforsøg, der i princippet kan udføres af kriminelle med meget begrænsede evner inden for hacking, eksempelvis simple, bedrageriske e-mails rettet mod borgere og medarbejdere i virksomheder.

Der er særligt en betydelig trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra borgere, virksomheder og myndigheder. Denne trussel kommer især til udtryk i form af ransomwareangreb, hvor cyberkriminelle krypterer ofrets data og kræver en løsesum for at gøre data tilgængelige igen. Ud over at have økonomiske konsekvenser for den ramte organisation kan ransomwareangreb have konsekvenser for samfundet, da de kan forstyrre centrale processer på f.eks. hospitaler eller i transportsektoren.

Cyberkriminelle afpresser også deres ofre på andre måder, f.eks. ved hjælp af DDoS-angreb eller ved at true med at offentliggøre data, som de har stjålet ved hjælp af hacking.

Der er store mørketal, når det gælder viden om cyberangreb mod myndigheder og virksomheder. CFCS vurderer, at dette især gælder for cyberkriminalitet. Mørketallene skyldes bl.a., at nogle cyberangreb ikke bliver meldt til politiet eller andre relevante myndigheder, enten fordi organisatio-

nen ønsker mindst mulig opmærksomhed omkring et angrebsforsøg, eller fordi de ikke er klar over, at de har været udsat for angreb.

Cyberkriminelle arbejder sammen i netværk

Det varierer, hvor velorganiserede de cyberkriminelle, der står bag den mere avancerede cyberkriminalitet, er. Her findes der både organiserede kriminelle grupper og netværk samt kriminelle individer med avancerede it-færdigheder. Grupperne varierer i størrelse og organisation fra etablerede kriminelle samarbejder til løse netværk, der finder sammen på ad hoc basis. Nogle af grupperne kan være specialiserede i bestemte typer cyberangreb, eksempelvis ransomwareangreb eller målrettede angreb mod betalingssystemer.

Der findes et økosystem af udviklere, brugere og udbydere af forskellige cyberkriminelle tjenester og værktøjer. Værktøjer anvendt af cyberkriminelle inkluderer forskellige typer malware og værktøjer til udnyttelse af sårbarheder i it-systemer, såkaldte exploit kits. Cyberkriminelle benytter også såkaldte botnet til spredning af malware gennem store mængder phishingmails. Endelig samarbejder nogle cyberkriminelle med andre typer kriminelle, f.eks. til tyveri fra pengeautomater.

En del af cyberkriminelles salg af tjenester og værktøjer foregår via fora på internettet, der kun er tilgængelige via anonymiseringstjenester såsom TOR, og derfor er skjulte for den brede offentlighed. Denne udveksling gør det muligt for kriminelle uden store it-kompetencer at udgøre en trussel. Udvekslingen af tjenester og værktøjer kaldes også for Crime-as-a-Service. Truslen fra de mere organiserede og ressourcestærke netværk, der deler og sælger deres værktøjer, har derfor en betydning for den samlede trussel fra cyberkriminelle.

Både cyberkriminelle og andre kriminelle netværk udnytter den seneste teknologiske udvikling inden for f.eks. kryptovalutaer og anonyme betalingsmetoder, bl.a. til hvidvaskning af penge. Kombineret med alternative bankplatforme giver disse betalingsmetoder muligheder for at flytte store summer uden myndighedernes kendskab.

Politiaktioner mod cyberkriminelle netværk og kriminelle markedspladser er vigtige værktøjer i bekæmpelsen af kriminalitet på internettet. Indgrebene medvirker til kortvarige opbrud i de kriminelle netværks aktiviteter. Desværre afløses kriminelle netværk og markedspladser ofte efter relativt kort tid af nye cyberkriminelle aktører eller markedspladser.

Statsstøttede hackere står sandsynligvis også bag cyberkriminalitet

CFCS vurderer, at det er sandsynligt, at statsstøttede hackere også står bag cyberangreb, der har berigelse som formål. Det globale WannaCry-ransomwareangreb, der inficerede mere end 300.000 computere i maj 2017, er af flere lande, herunder USA, Storbritannien, Canada, Australien og New Zealand officielt tilskrevet Nordkorea. I 2016 stjal hackere næsten 100 mio. dollars fra Bangladeshs nationalbank. Lignende angreb er siden blevet rettet mod banker i andre lande,

bl.a. mod taiwanske Far Eastern International Bank i oktober 2017. Flere sikkerhedsfirmaer har tilskrevet disse angreb til hackergrupper, som CFCS vurderer har tilknytning til Nordkorea.

Det er også sandsynligt, at statslige aktører bruger angreb, der ligner cyberkriminalitet, som dække for andre typer cyberangreb. Det såkaldte NotPetya-angreb er sandsynligvis et eksempel på dette. Angrebet havde karakter af et globalt ransomwareangreb med udgangspunkt i Ukraine, men ofrene havde ikke mulighed for at frikøbe deres systemer ved at betale afpresningsbeløbet til bagmændene.

Angriberne forsøgte sandsynligvis at forklæde angrebet som et ransomwareangreb for at skabe usikkerhed om angrebets karakter og ophav. Det kan have styrket angriberens risikovillighed til at gennemføre et destruktivt cyberangreb, der endte med at have stor skadevirkning både i og uden for Ukraine, herunder i Danmark.

WannaCry- og NotPetya-angrebene

WannaCry
WannaCry-ransomwaren begyndte at sprede sig til computere verden over i maj 2017. Denne ransomwarevariant var i stand til automatisk at kryptere filer på ofrets computer, slette originalerne og opkræve en løsesum for at dekryptere filerne igen. Samtidig installerede ransomwaren en bagdør på ofrets maskine, som gav angriberen mulighed for at installere yderligere malware. WannaCry var i stand til at sprede sig over lokalnetværk og internettet via en sårbarhed i Server Message Block, version 1 (SMBv1)-protokollen.

NotPetya
NotPetya-malwaren gjorde sit indtog i juni 2017, og ramte som WannaCry mange computere på verdensplan. NotPetya udgav sig indledningsvist for, ligesom WannaCry, at være ransomware. Men selv om malwaren afkrævede en løsesum, havde den reelt ikke funktionalitet til at genskabe adgangen til ofrenes filer, som det ellers teoretisk set er tilfældet ved ransomware. NotPetya blev derfor anset som et angreb med destruktive formål og ikke som en ransomwarekampagne.

Eksempler på cyberangreb udført af cyberkriminelle

Her er en gennemgang af typiske angreb udført af cyberkriminelle. Listen er ikke udtømmende.

Ransomwareangreb

Ransomware bliver, som andre typer malware, typisk spredt via phishingmails eller via inficering af hjemmesider, som offeret besøger. Ransomware krypterer offerets data og aftvinger en løsesum typisk i form af kryptovaluta, såsom Bitcoin, for at frigive data igen. Der findes mange varianter af ransomware. Mere målrettede ransomwareangreb forsøger at ramme eksempelvis administrative netværk i specifikke virksomheder og myndigheder. Særligt sundhedssektoren har i udlandet været offer for disse mere målrettede ransomwareangreb, hvor løsesummen har været af ganske betragtelig størrelse.

Inficering med andre typer malware

Cyberkriminelle distribuerer fortsat flittigt andre typer malware. Disse typer malware bruges bl.a. til at stjæle personlige og finansielle oplysninger, der kan sælges eller misbruges af kriminelle. Her er der malware rettet specifikt mod brugere af netbanksystemer, såkaldte banking trojans. Kriminelle er i stigende grad også interesserede i at stjæle kryptovalutaer fra deres ofre. En nyere type malware kaldet mineware inficerer computere med henblik på at misbruge maskinkraft til at tjene kryptovalutaer i såkaldt kryptomining.

Angreb mod finansielle systemer

Nogle cyberkriminelle er specialiseret i målrettede cyberangreb mod banker og betalingssystemer brugt i f.eks. detailhandel. Kompromitteringen af betalingssystemer har til formål at stjæle kreditkortinformationer, der bl.a. sælges videre i stort antal på kriminelle markeder. Kompromitteringer af banker har især været udbredt i Rusland, hvor beløb svarende til hundreder af millioner af kroner er blevet stjålet af cyberkriminelle. Cyberkriminelle går også efter børser, der handler med kryptovalutaer. I januar 2018 blev kryptovaluta til en værdi af mere end 3 mia. danske kroner eksempelvis stjålet fra en japansk valutabørs. Både i Danmark og udlandet har der også været sager, hvor kriminelle bryder ind i betalingsautomater og får hjælp fra hackere til at få maskinen til at frigive store kontantbeløb.

Målrettet afpresning

Som en nyere tendens er der grupper, der specialiserer sig i at stjæle følsomme oplysninger om virksomheders kunder og forretning med henblik på afpresning. Trusler om overbelastningsangreb via internettet, såkaldte DDoS-angreb, benyttes også som afpresning. Ofte kræver de cyberkriminelle meget store pengebeløb af deres ofre. Gruppen Dark Overlord blev bl.a. kendt i medierne for at have lækket afsnit af en tv-serie, Orange is the New Black, efter først af have forsøgt at afpresse producenten bag serien. Et dansk eksempel på denne type trussel er, da cyberkriminelle i februar 2017 forsøgte at afpresse den danske filial af teleselskabet 3 ved at true med at offentliggøre data, som de havde stjålet via hacking.

Bedrageri

Såkaldte BEC (Business Email Compromise) scams har til formål at franarre virksomheder og organisationer penge gennem falske anmodninger om pengeoverførelser. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også for CEO-fraud eller direktørsvindel. De bedrageriske e-mails sendes ofte fra fremmede mailkonti, men i nogle tilfælde kan bedrageriforsøget misbruge kompromitterede mailkonti, der tilhører ledende medarbejdere i virksomheden. Fremsendelse af falske e-mails fra sådanne kompromitterede konti kan øge risikoen for et succesfuldt bedrageriforsøg. I en rundspørge fra Berlingske Business i 2017 svarede mere end halvdelen af de adspurgte virksomheder, at de havde været udsat for forsøg på direktørsvindel.

Cyberaktivisme

Truslen fra cyberaktivisme er **MIDDEL**.

Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver. Cyberaktivister kan fokusere på personer eller organisationer, som de opfatter som modstandere af deres sag.

Cyberaktivister bruger forskellige typer simple cyberangreb. F.eks. gør de hjemmesider utilgængelige ved hjælp af DDoS-angreb. De hacker også hjemmesider eller profiler på sociale medier og indsætter budskaber eller billeder. Nogle cyberaktivister lækker også følsomme oplysninger fra hacking af f.eks. personlige mailkonti for at skabe opmærksomhed om deres sag.

Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige evner og ressourcer til at udføre cyberangreb. Truslen kan derfor pludselig stige, hvis danske myndigheder eller virksomheder kommer i cyberaktivisters søgelys.

Det skete eksempelvis i september 2017, da Statsministeriets, Udenrigsministeriets, Udlændinge og Integrationsministeriets samt Nationalbankens hjemmesider i en kort periode blev gjort utilgængelige af DDoS-angreb, som tyrkiske cyberaktivister sandsynligvis stod bag. Aktivisterne, der kalder sig Aslan Neferler Tim, har flere gange i 2017 taget ansvar for cyberangreb rettet mod europæiske lande, som gruppen hævdede, havde krænket bl.a. Tyrkiets ledere, den nationale stolthed eller islam.

Angrebet illustrerer, at cyberaktivister til tider også angriber myndigheder og virksomheder, som hackerne betragter som symbolske mål, selvom de ikke har været direkte indblandet i den sag, som har fanget hackernes opmærksomhed. Hvor Aslan Neferler Tim fokuserer på en relativt afgrænset mærkesag, så indgår an-

Faketivister – falske aktivister

Der er flere eksempler på aktører på internettet, der udgiver sig for at være cyberaktivister, men hvor tekniske spor indikerer, at der er tale om statsstøttede hackere. Sådanne hackere kaldes i populær tale for faketivister.

Et eksempel er hackere, der kalder sig Anonymous Poland, har lækket oplysninger fra kompromitteringer af bl.a. World Anti-Doping Agency (WADA) og Court of Arbitration for Sport (CAS) i 2016. Anonymous Poland har i 2017 bl.a. lagt kommentarer på internettet om valget i Catalonien og konflikten i Ukraine.

Et sikkerhedsfirma, der undersøgte kompromitteringerne af WADA og CAS, tilskrev imidlertid angrebene til hackergruppen Fancy Bear. Denne gruppe stod ifølge amerikanske myndigheder bag kompromitteringen af den Demokratiske Nationale Komite i 2016. Samme gruppe stod ifølge CFCS bag cyberangreb mod Udenrigsministeriet i 2015 og Forsvarsministeriets myndighedsområde i 2015 og 2016. CFCS vurderer også, at det er sandsynligt, at det var et andet lands efterretningstjeneste, der stod bag disse angreb (Kilde: En aktør, mange angreb. CFCS's hjemmeside).

dre hackere i mere fragmenterede cyberaktivistiske netværk, der retter deres opmærksomhed mod mange forskellige sager og emner. Anonymous er nok det mest kendte eksempel på et sådant fragmenteret netværk af hackere.

I løsere hackernetværk som Anonymous sker der til tider en mobilisering på sociale medier, hvor hackerne varsler kommende angreb. Dette skete f.eks. efter afstemningen om Cataloniens uafhængighed den 1. oktober 2017. Hackere, der hævdede at være knyttet til Anonymous, varslede i oktober 2017 en kampagne mod bl.a. spanske myndigheder. Forskellige hackere og hackergrupper udførte derefter cyberangreb mod hjemmesider, og de lækkede i enkelte tilfælde informationer, som de havde stjålet via hacking. Cyberaktivismen i forbindelse med den catalanske uafhængighedsafstemning er også et eksempel på, hvordan cyberaktivisme kan ledsage mere traditionel politisk aktivisme.

Nogle grupper benytter simple cyberangreb som instrument til spredning af militante ekstremistiske synspunkter. Det gælder bl.a. hackernetværket United Cyber Caliphate (UCC), der sympatiserer med Islamisk Stat. Andre grupper og netværk udfører cyberaktivisme for at bekæmpe militant ekstremisme på eksempelvis sociale medier. På trods af ideologiske forskelle trækker flere af disse modstridende grupper på en vis grad af fælles sprogbrug og grafisk udtryk, eksempelvis bruger mange forskellige grupper de såkaldte Guy Fawkes masker.

Endelig benyttes cyberaktivistiske grupper som dække i forsøg på at påvirke den folkelige meningsdannelse i andre lande. Dette blev især kendt i forbindelse med det amerikanske præsidentvalg i 2016, hvor hack og læk af mails fra den Demokratiske Nationale Komite blev tilskrevet russiske hackere af amerikanske myndigheder.

Cyberterror

Truslen fra cyberterror er **LAV**.

CFCS vurderer, at militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb, og selv om de i få tilfælde har ytret interesse for at udføre cyberterror, har de aktuelt ikke kapacitet til dette. Der er derfor en lav trussel mod Danmark fra cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, f.eks. cyberangreb, der forårsager fysisk skade på mennesker eller materiel eller skaber omfattende forstyrrelser af kritisk infrastruktur.

Flere hackergrupper, der støtter terrororganisationen Islamisk Stat i Irak og Levanten (ISIL), har det seneste år forsøgt at styrke deres cyberkapaciteter ved at slå sig sammen til hackernetværket United Cyber Caliphate (UCC). Det har indtil nu ikke øget deres evner eller ressourcer. De er på nuværende tidspunkt alene i stand til at udføre simple cyberangreb, der især har til formål at skabe opmærksomhed om og sprede propaganda for ISIL. UCC har ikke haft kapacitet til at målrette sine

angreb i særlig høj grad. Netværket er derfor primært gået efter hjemmesider med lav it-sikkerhed tilhørende alt fra danselærere til bilentusiaster.

ISIL's ledelse har indtil nu ikke officielt anerkendt UCC eller andre hackergrupper. Truslen fra hackere, der støtter ISIL eller andre ekstremistiske terrorgrupper, kan stige, hvis grupper som ISIL i fremtiden vælger at støtte UCC eller andre hackergrupper. Det er mindre sandsynligt, at ISIL eller andre sunniekstremistiske terrorgrupper på kort sigt vil støtte udviklingen af cyberkapaciteter i en sådan grad, at det vil øge truslen fra cyberterror.

Militante ekstremister med tilstrækkelig finansiel styrke kan købe sig til mere avancerede kapaciteter end dem, de råder over nu. De værktøjer, de vil kunne købe sig til på nuværende tidspunkt, er dog ikke tilstrækkeligt avancerede til at udføre så alvorlige cyberangreb, at de kan få samme effekt som konventionel terror.

Udviklingstendenser med betydning for cybertruslen

Visse stater bruger cyberangreb til at styrke deres magtposition

Evnen til at kunne gennemføre cyberangreb kan ses som et potentielt magtmiddel. Det gælder bl.a. anvendelsen af destruktive cyberangreb, overbelastningsangreb og hack og læk af politisk følsomt materiale. Hertil kommer evnen til cyberspionage, der i sig selv kan styrke det enkelte land på bekostning af andre.

På kort sigt er det mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark. Det er det dog muligt, at danske virksomheder og myndigheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske virksomheder og myndigheder, der er til stede i konfliktområder, hvor fremmede stater eller organiserede hackergrupper, som har evnen til at udføre alvorlige cyberangreb, har interesser, såsom i dele af Østeuropa, Mellemøsten og Østasien.

Bl.a. Ukraine, Sydkorea og Saudi-Arabien har i de seneste år været udsat for flere destruktive cyberangreb rettet mod bl.a. kritisk infrastruktur og industri. Disse cyberangreb er sandsynligvis blevet udført af statslige aktører som led i regionale konflikter og spændinger.

Effekten af disse angreb har i enkelte tilfælde været markante, men der har ikke været tale om større fysisk skadevirkning eller længerevarende nedbrud af kritisk infrastruktur. Disse

Destruktive cyberangreb
CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt af angrebet er død, personskade, betydelig skade på fysiske objekter eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

cyberangreb har funktion af politisk signalgivning og chikane. For de lande, der står bag disse angreb, er der tale om et magtmiddel, der ligger under tærsklen for krig og krigshandlinger. Grundet usikkerhed forbundet med tilskrivningen af disse angreb til bestemte lande er det samtidigt vanskeligt at gengælde eller afskrække angrebene. Tvivlen er en fordel for angriberen, og det udnytter visse lande.

Landene, der står bag destruktive cyberangreb er derfor generelt sluppet afsted med angrebene uden væsentlige modsvar. NotPetya-angrebet i 2017 viste, at angriberen havde stor villighed, da angrebet havde skadevirkning på flere internationale virksomheder. Stigende risikovillighed og fraværet af konsekvenser for angriberen øger risikoen for nye destruktive cyberangreb, der har skadevirkning uden for de nævnte, typiske konfliktområder.

Der er dog en voksende villighed fra flere lande til at tilskrive cyberangreb til specifikke lande og aktører. Dette kan danne platform for en mere tydelig international normdannelse mod og modsvar på destruktive cyberangreb.

Visse lande benytter også hack og læk af politisk følsomt materiale i forsøg på at påvirke meningsdannelsen. Her er cyberangreb igen et instrument i den politiske dagsorden og magtkamp. Det er bl.a. sket i forbindelse med afholdelse af valg i udlandet, hvor angrebene har haft til formål at påvirke befolkningens holdning og tillid til bestemte politikere samt skabe mistro til den demokratiske proces. Det sker i en grad så vestlige lande i dag generelt forbereder sig på at blive udsat for cyberangreb i forbindelse med afholdelse af valg.

I disse tilfælde har cyberangreb været ét blandt flere virkemidler i bredere informations- og påvirkningskampagner, der også har inkluderet f.eks. falske nyhedshistorier og aktiviteter på sociale medier. Det er muligt, at cyberangreb, såsom hack og læk af følsomme oplysninger, vil blive brugt som virkemiddel i en eventuel påvirkningskampagne i Danmark. Truslen fra sådanne cyberangreb kan stige i forbindelse med politiske sager, hvis udfald fremmede stater har en væsentlig interesse i at påvirke eller i forbindelse med en politisk eller militær konflikt.

Ukraine er en digital slagmark

Ukraine har været udsat for mange cyberangreb, dels i form af omfattende cyberspionage, dels i form af destruktive cyberangreb rettet mod bl.a. strømforsyningen.

Cyberangreb i Ukraine har også haft betydning uden for landet. I forbindelse med det såkaldte NotPetya-angreb i 2017 blev flere ikke-Ukrainske virksomheder, herunder Mærsk, også blev ramt af alvorlige nedbrud med store økonomiske tab til følge. Mærsk har opgjort tabet til mellem 1,6 og 1,9 mia. kr.

For de lande, der benytter disse midler, er cyberangreb et supplement eller alternativ til mere traditionelle magtmidler. For nogle lande kan det være et forsøg på at undergrave den regionale stabilitet og styrke sin position i konflikter, hvor andre midler enten ikke kan anvendes eller er utilstrækkelige.

Stater gør mere for at skjule deres handlinger

Stater forsøger at gøre deres cyberspionage stadigt sværere at opdage. Visse statsstøttede hackergrupper bruger bl.a. betydelige ressourcer på tekniske tiltag, der kan skjule deres aktiviteter. Det kan ses som en reaktion på de offentlige afsløringer af cyberoperationer, hvor navngivne statsansatte hackere er blevet offentligt udstillet og i nogle tilfælde efterlyst.

Stater slører på flere måder, hvor cyberspionagen kommer fra, og hvem der står bag. Eksempelvis benytter nogle statsstøttede hackergrupper sig ikke længere af værktøjer, som tidligere har været karakteristiske for netop deres cyberspionage. Andre statsstøttede hackergrupper forsøger at sikre deres anonymitet ved i højere grad end tidligere at anvende offentligt tilgængelige værktøjer, der også benyttes af cyberkriminelle eller legitime it-sikkerhedsfirmaer og -eksperter. Når stater anvender offentligt tilgængelige værktøjer i stedet for deres egne unikke værktøjer, kan de nemmere så tvivl om deres involvering.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynlighed i analyser: