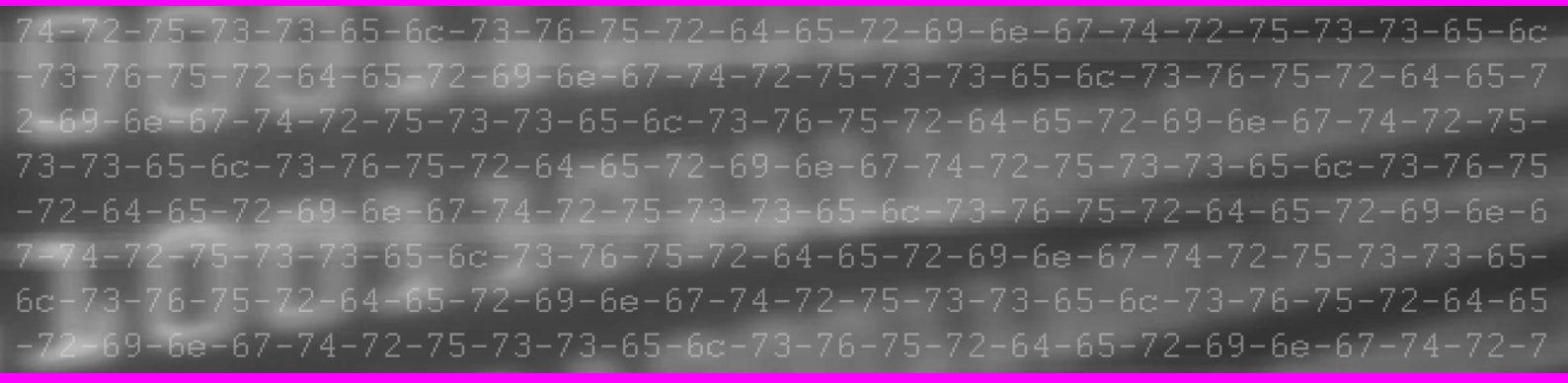
CENTER FOR
CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod Danmark



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Februar 2017

CENTER FOR CYBERSIKKERHED

Februar 2017

Cybertruslen mod Danmark

Vurderingen gør rede for den samlede cybertrussel, der møder danske myndigheder og private virksomheder. Truslen er størst fra cyberspionage udført af stater og fra cyberkriminalitet. Både statslige og kriminelle hackere udvikler deres kompetencer, og angrebsmetoderne bliver fortsat mere avancerede.

Hovedvurdering

Cyberspionage mod offentlige og private mål udgør fortsat den alvorligste cybertrussel mod Danmark. Der er tale om en meget aktiv trussel mod danske interesser. Truslen kommer især fra fremmede stater.

Truslen fra cyberspionage mod danske myndigheder og private virksomheder er **MEGET HØJ**.

Truslen fra cyberkriminalitet er stigende i omfang og kompleksitet, bl.a. fra organiserede kriminelle. Cyberkriminelle ydelser sælges også via internettet. Ransomware og DDoS er blandt de mest benyttede angrebsmetoder.

Truslen fra cyberkriminalitet mod danske myndigheder og private virksomheder er **MEGET HØJ**.

Selvom kapaciteten er til stede, er der ikke mange eksempler på cyberaktivisme mod danske myndigheder og virksomheder. Dog kan truslen fra cyberaktivisme ændre sig pludseligt for en virksomhed, myndighed eller person, der kommer i aktivisters søgelys af politiske eller ideologiske årsager.

Truslen fra cyberaktivisme mod danske myndigheder og private virksomheder er **MIDDEL**.

Kendte terrorgrupper har på nuværende tidspunkt ikke den fornødne kapacitet til at gennemføre egentlige terrorangreb via internettet med død eller voldsom ødelæggelse til følge.

Truslen fra cyberterror mod danske myndigheder og private virksomheder er **LAV**.

Indledning: cybertruslen udvikler sig konstant

Avancerede økonomier har typisk en højere grad af afhængighed af internettet end udviklingslande. Det gør dem til oplagte mål for fremmede stater og kriminelle, der vil udnytte cyberdomænet til ondsindede formål.

Danske myndigheder og private virksomheder er i høj grad afhængige af internettet i deres arbejde. Det samme gælder i stigende grad for samfundsvigtig infrastruktur. Digitaliseringen skaber nye og innovative muligheder, men gør også brugere og samfund sårbare overfor cyberangreb. It-teknologiens dynamiske natur gør, at truslerne er i konstant forandring. Det stiller krav til myndigheder og virksomheder om hele tiden at udvikle deres cybersikkerhed og beredskab. Denne trusselsvurdering beskriver og vurderer hovedtyperne af cybertrusler mod danske digitale netværk.

Der er store mørketal, når det gælder viden om cyberangreb mod myndigheder og virksomheder. Det skyldes i nogle tilfælde, at organisationer ønsker mindst mulig opmærksomhed omkring et angrebsforsøg, eller at de ikke er klar over, at de har været udsat for angreb.

For mange private virksomheder gælder det, at cyberangreb kun anmeldes eller rapporteres, hvis angrebet er lykkedes og har ført til erkendte tab for virksomheden. Derfor mangler der samlet statistisk materiale om angrebsforsøg, hvor hackere ikke har haft held til deres foretagende. Alle angreb, uanset succes, er relevante for at forstå det komplette trusselsbillede. Center for Cybersikkerhed samarbejder med myndigheder og private virksomheder og beskriver cybertruslen på baggrund af den samlede viden.

Trusselsbilledet

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål aktøren bag den enkelte trussel har, og hvor alvorlige konsekvenserne af en trussel kan være for en myndighed eller virksomhed, der rammes.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som ondsindede aktiviteter, hvor et digitalt system eller netværk udsættes for et cyberangreb, der giver angriberne mulighed for at få uautoriseret adgang til systemer og data. Almindelig brug af internettet med ondsindet formål, såsom rekruttering til terrorgrupper via sociale medier indgår ikke i denne definition af cybertrusler. CFCS beskriver og vurderer her aktiviteter, der har til formål at:

- Udføre spionage via internettet
- Begå berigelseskriminalitet via internettet
- Udføre aktivistiske aktioner via internettet
- Udføre terrorhandlinger via internettet

Desuden beskriver CFCS staters brug af destruktive angreb via internettet.

Trusselsniveauerne afhænger 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 social engineering. Det kan også være it-infrastruktur, tid, penge og adgang til information. Graden af cyberkapacitet vil derfor afhænge af flere forskellige ressourcer og evnen til at kombinere dem. Det betyder, at en aktør med store tekniske evner, men uden den fornødne infrastruktur eller viden om et mål, kan blive vurderet til at have en lav cyberkapacitet. Det samme gælder for en aktør med stor viden om et mål, men uden de tekniske kompetencer til at udnytte sin viden.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede, som har en varslingshorisont på 0-2 år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed.

I slutningen af trusselsvurderingen findes en oversigt, der forklarer forskellige begreber og cyber-termer, som bruges løbende i teksten. Forsvarets Efterretningstjenestes trusselsniveauer og sand-synlighedsgrader er også forklaret i slutningen af vurderingen.

Cyberspionage

CFCS vurderer, at truslen fra cyberspionage mod danske myndigheder og private virksomheder er **MEGET HØJ** og især kommer fra fremmede stater. CFCS har gennem de seneste år konstateret en stigning i angreb fra stater og kontinuerlige forsøg på at kompromittere danske myndigheder og virksomheder.

Staternes interesse i at spionere mod Danmark kan være både strategisk, politisk og kommerciel. Formålet med cyberspionage kan f.eks. være at få indsigt i den politiske forberedelse forud for vigtige forhandlinger eller at kopiere en virksomheds produkter og intellektuelle ejendom for at opnå en konkurrencemæssig fordel.

Det kan have store konsekvenser for Danmark, hvis fremmede stater får uønsket adgang til værdi-fulde oplysninger, f.eks. på det sikkerhedspolitiske område eller inden for politiske fokusområder såsom Arktis. Det kan også skade danske myndigheders og virksomheders ry og påvirke den tillid, som borgere, kunder og samarbejdspartnere har til dem.

Flere statslige eller statsstøttede hackere har både evner og ressourcer til at udføre avancerede cyberangreb, hvor kompromittering kan være svær at opdage. De er dygtige til at tilpasse sig nye teknologier, og de bliver fortsat bedre til at skjule deres aktiviteter og identitet.

Rusland er en førende aktør på cyberområdet

Rusland har gennem en længere periode investeret intensivt i sine cyberkapaciteter og har avancerede kapaciteter til at udføre omfattende cyberspionage mod politiske og militære mål i Vesten. Samtidig har Rusland adgang til cyberkapaciteter, som kan understøtte landets konventionelle militære operationer, eksempelvis målrettede operationer mod kritisk infrastruktur.

Kinas cyberspionage

Kina råder over omfattende muligheder for at udføre cyberspionage. Flere kinesiske myndigheder, herunder det kinesiske militær, er i Vesten blevet offentligt kritiseret for at stå bag omfattende spionage via internettet mod en lang række mål i udlandet. Kina bruger sine cyberkapaciteter til at indhente informationer af økonomisk, politisk og militær betydning.

Fremmede stater interesserer sig for udenrigs- og sikkerhedsforhold

Truslen fra cyberspionage er rettet mod hele det danske statslige område, men det er i særlig høj grad myndigheder af betydning for dansk udenrigs- og sikkerhedspolitik, der er udsat for forsøg på cyberspionage. CFCS har kendskab til gentagne forsøg på cyberspionage mod Udenrigsministeriet og Forsvarsministeriets myndighedsområde.

Statssponsoreret hackergruppe angriber danske ministerier

I 2015 og 2016 har den samme udenlandske aktør gentagne gange forsøgt at få adgang til informationer fra Udenrigsministeriet og Forsvarsministeriets områder via forskellige typer cyberangreb. Det er bl.a. sket via spear phishing-kampagner, der har forsøgt at lokke målpersoner til at afgive deres maillogin-oplysninger. Der er også set forsøg på adgang til e-mailkontoer ved automatiseret at afprøve tusindvis af kodeord. CFCS vurderer, at en udenlandsk statssponsoreret hackergruppe står bag angrebsforsøgene, og at truslen er vedvarende.

Truslen mod private virksomheder er især rettet mod forskningstunge og højteknologiske industrier samt firmaer med aktivitet i udvalgte geografiske områder. Statslige aktører er gået målrettet efter sådanne danske virksomheder de seneste år. Underleverandører og servicevirksomheder, der er knyttet til disse industrier, bliver ligeledes angrebet, da de ofte har adgang til sensitive informationer.

CFCS har i 2016 bl.a. udgivet sektorspecifikke vurderinger af truslen fra cyberspionage mod forsvars- og aerospaceindustrien og dansk offentlig forskning. Konsekvenserne af cyberspionage for virksomheder eller forskningsinstitutioner kan være ringere konkurrencevilkår og tab af intellektuel ejendom.

På nogle forskningsområder kan fremmede stater få indsigt i den forskning og rådgivning, som regering og Folketing baserer vigtige beslutninger på. På andre områder kan stater søge at opnå konkurrencemæssig og kommerciel fordel ved at kende til forskernes arbejde og danske forskningsresultater, før de er offentliggjort.

I takt med at flere stater øger deres cyberkapacitet, er det sandsynligt, at flere af disse aktører vil forsøge med angreb, da industrispionage og tyveri af intellektuel ejendom er en måde at styrke økonomisk udvikling uden store omkostninger eller risici. Ligeledes kan truslen fra regionale trusselsaktører mod danske repræsentationer i udlandet stige i takt med øget cyberkapacitet i flere stater.

Stater bruger hack og læk til at påvirke forhold i andre lande

Erfaringer fra udlandet viser en stigning i fremmede staters brug af cyberspionage til at forsøge at påvirke politiske og demokratiske processer og folkestemninger i det offentlige rum. Påvirkningskampagner mellem stater er ikke i sig selv nyt, men det er en ny udvikling at bruge cyberkapaciteter. I en såkaldt hack og læk-operation skaffer aktørerne sig adgang til informationer, som de efterfølgende, ofte selektivt, lækker. Det kan f.eks. være private e-mails og fortrolige dokumenter, der sætter politikere i et dårligt lys op til et valg.

Ønsket om at påvirke interne forhold i andre lande kan også være økonomisk motiveret eller forsøg på at modgå, hvad nogle stater regner for vestlige angreb på deres værdier og kultur. Der er stater, der mener, at de er i en informationskrig mod Vesten, og at Vesten optrapper konflikter via sine medier og brug af soft power.

Både USA og Tyskland har i 2016 offentligt udpeget statslige aktører som ansvarlige for hack mod partier og politikere og efterfølgende læk af informationer. Det gælder f.eks. lækken i kølvandet på hacket af Demokraternes Nationale Komité i USA og en stigning i antallet af spear-phishing-angreb mod tyske partier, som den tyske sikkerhedstjeneste ser som et forsøg på at påvirke det kommende forbundsdagsvalg.

Det er dog ikke kun politiske partier eller myndigheder, der er mål for hack-og-læk-operationer. Det såkaldte Sony-hack fra 2014 er et eksempel på et cyberangreb, hvor flere strategier blev taget i brug, herunder også hack og læk.

Hackere angreb filmselskab og lækkede persondata og e-mails

I 2014 blev filmselskabet Sony Pictures Entertainment hacket. Selskabets computere blev inficeret med destruktiv malware, der ødelagde data og systemer, og hackerne fik adgang til intellektuel ejendom og fortrolige informationer. Efterfølgende lækkede hackerne e-mails, der belastede afsenderne, personføl-

somme og medicinske oplysninger om ansatte, cheflønninger, kopier af film, der endnu ikke var udkommet og andre informationer. Hacket resulterede i en række retssager mod Sony Pictures fra tidligere ansatte og stor kritik af selskabet for deres håndtering af sagen. I Sony-sagen pegede USA på en statslig aktør med et politisk motiv

I andre sammenhænge kan forsøg på påvirkning og den slet skjulte brug af informationer fremskaffet ved cyberspionage være en reaktion på sanktioner eller for at vise styrke. Ud fra et "del og hersk-princip" kan staterne også forsøge at påvirke samarbejdsforhold mellem andre lande og destabilisere alliancer som f.eks. EU eller NATO. De kan også forsøge at påvirke folkestemninger, der vedrører debatter om regioners løsrivelse fra nationalstater. Her står cyberspionage ikke alene, da stater også i høj grad benytter sig af klassisk propaganda og misinformation via f.eks. sociale medier.

Hack-og-læk-operationer er et potentielt meget stærkt værktøj til at påvirke meningsdannelsen i andre lande. CFCS vurderer, at der er en risiko for, at fremmede stater også vil anvende selektiv offentliggørelse af informationer fra cyberspionage til at påvirke meningsdannelse og beslutninger i Danmark. Det meget høje aktivitetsniveau med cyberspinonage gør, at værktøjet kan komme i anvendelse uden varsel, hvis en sag er vigtig nok for aktøren.

Cyberkriminalitet

I denne trusselsvurdering dækker begrebet cyberkriminalitet tilfælde, hvor gerningsmænd bruger it til at begå kriminelle handlinger, hvor formålet er berigelse. Det er eksempelvis tyveri af penge eller finansielle oplysninger, bedrageri og afpresning. Fokus er her på kriminalitet mod myndigheder og virksomheder eller handlinger mod større grupper af individer med konsekvenser for virksomheder, såsom når en banks kunder rammes. CFCS baserer sin vurdering bl.a. på informationer fra Rigspolitiets Nationale Cyber Crime Center (NC3) og vurderer, at truslen fra cyberkriminalitet mod danske myndigheder og private virksomheder fortsat er **MEGET HØJ**.

Organiserede kriminelle lokker penge ud af danske virksomheder

NC3 oplyser, at der i 2016 har været en kraftig stigning i sager om såkaldte BEC (Business Email Compromise) scams, hvor aktører ved hjælp af social engineering narrer medarbejdere i virksomheder til at overføre penge eller uforvarende give adgang til systemer i den tro, at de agerer på en ordre fra ledelsen.

Der er i stigende grad tale om organiseret kriminalitet, hvor hackerne bag BEC-scams i sig selv har dannet "firmaer", som specialiserer sig i denne form for svindel. De kriminelle firmaer har bl.a. medarbejdere, som er specialiserede i udvalgte sprogområder eller som står for profilering af målvirksomhedernes ansatte for at finde ud af, hvilke ansatte der har hvilke adgange eller vil være

mest tilbøjelig til at tro på en falsk e-mail. Firmaerne har også underleverandører til f.eks. hvidvaskning af penge.

CFCS har fra NC3 kendskab til, at en række af disse firmaer målrettet har angrebet danske virksomheder på tværs af brancher i 2016.

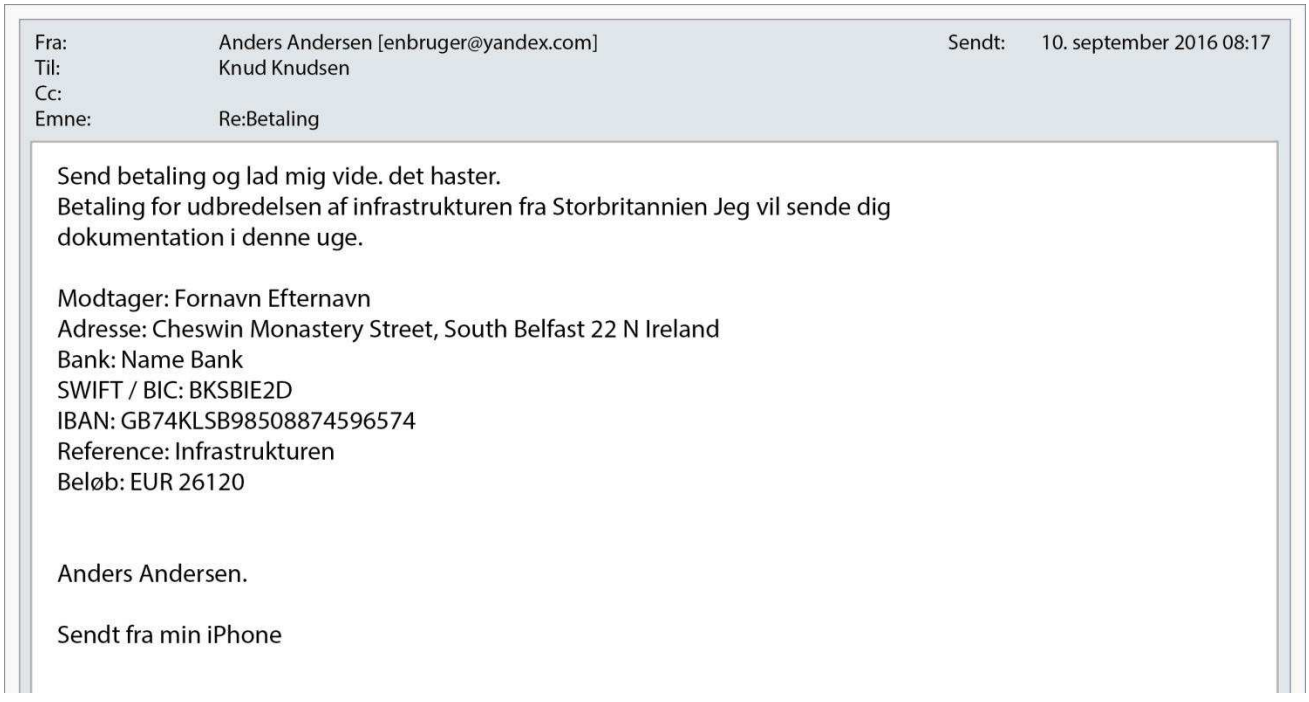
Især i sidste halvdel af 2016 har de udset sig danske virksomheder som mål. Alene i sager anmeldt til politiet i denne periode har danske virksomheder lidt tab for over 180 mio. kr. De økonomiske tab har naturligvis store konsekvenser for de ramte virksomheder og kan også få store personlige konsekvenser for de medarbejdere, der er gået i fælden.

Emne: betaling

Hej Klaus,

Vi er nødt til at sende en betaling på £ 14,075.15 GBP til England i dag. Hvilke oplysninger har du brug for at få det gjort nu?

Tak
Thomas



Fra: Anders Andersen [enbruger@yandex.com] Sendt: 10. september 2016 08:17
Til: Knud Knudsen
Cc:
Emne: Re:Betaling

Send betaling og lad mig vide. det haster.
Betaling for udbredelsen af infrastrukturen fra Storbritannien Jeg vil sende dig dokumentation i denne uge.

Modtager: Fornavn Efternavn
Adresse: Cheswin Monastery Street, South Belfast 22 N Ireland
Bank: Name Bank
SWIFT / BIC: BKSBIE2D
IBAN: GB74KLSB98508874596574
Reference: Infrastrukturen
Beløb: EUR 26120

Anders Andersen.

Sendt fra min iPhone

Eksempler på falske e-mails fra forsøg på BEC-scams i Danmark. Alle navne, adresser og e-mails er ændret.

Det sker også, at hackere skaffer sig direkte adgang til banker og betalingssystemer og selv laver overførsler. Det var tilfældet i en sag fra Bangladesh i 2016, som er blevet kaldt det største internet-bankrøveri nogensinde.

Centralbank mister 100 millioner dollars som konsekvens af cyberangreb
I februar 2016 trængte hackere ind i systemer hos centralbanken i Bangladesh og forsøgte at få overført 951 millioner dollars til falske bankkonti forskellige steder i verden via det internationale banksystem SWIFT. Hackerne havde succes til at få ca. 100 millioner dollars overført, før angrebet blev opdaget og stoppet. Angrebet er af sikkerhedsfirmaer blevet forbundet med lignende angrebsforsøg på banker i andre lande.

Cyberkriminelle sælger også deres ydelser via internettets sorte markeder. Ydelserne kan være værktøjer til overbelastningsangreb (DDoS) og malware til ransomware-angreb. Konceptet kaldes "crime as a service", og grænsefladerne mellem statsstøttede hackere, cyberkriminelle og andre aktører med ondsindede intentioner er blevet mere flydende. Crime as a service gør det muligt for kriminelle uden store it-kompetencer at begå cyberkriminalitet. Bitcoin og andre digitale valutaer er de foretrukne betalingsformer, når cyberkriminelle tager penge for en service eller kræver løsepenge ved ransomware-angreb.

Ransomware er et stigende problem
Ransomware er en af de mest fremtrædende trusler inden for cyberkriminalitet. Udover privatpersoner, retter hackere ransomware-angreb mod især virksomheder, men også myndigheder og offentlige institutioner. Hvis angrebet lykkes, bliver der installeret malware, der krypterer data og kræver løsepenge for igen at give ofret adgang til sine data. Løsepenge kræves som regel i form af Bitcoins. Hackerne bruger meget ofte phishing og social engineering til at få folk til at klikke på links i e-mails, sms'er eller på reklamebannere, der installerer malware. Den menneskelige faktor er derfor af stor betydning, hvis man vil undgå at blive offer for ransomware. For en virksomhed eller organisation vil et ransomware-angreb ofte betyde, at der er opgaver og funktioner, de ikke kan udføre, mens angrebet står på.

I Danmark har man især set brede ransomware-kampagner, hvor hackerne går efter flere mål ad gangen og ikke raffinerer eller målretter teksten i e-mails eller sms'er. Det er dog meget sandsynligt, at hackerne ofte vurderer et måls værdi og villighed til at betale forud for et angreb og sætter løsesummen derefter.

Ransomware-angreb mod udenlandske hospitaler
I USA, England og Tyskland har flere hospitaler været udsat for ransomware-angreb. Hackerne har i flere tilfælde krypteret e-mails og patientjournaler og efterladt beskeder på personalets computere om, at de

skulle betale løsepenge for at få dekrypteret data. I mindst to tilfælde i 2016 har cyberangreb haft direkte konsekvenser for patientbehandlingen på hospitaler i USA. Og i England måtte et hospital udskyde transplantationer og operationer pga. et ransomware-angreb. I andre tilfælde har hospitaler valgt at betale løsepengesummen.

Tekst fra britisk hospitals hjemmeside efter et cyberangreb, der bl.a. fik hospitalet til at udskyde operationer

Overbelastningsangreb bliver mere avancerede

Overbelastningsangreb, også kaldet DDoS-angreb, er en af de metoder, cyberkriminelle benytter sig af. Det ses bl.a. i finanssektoren og online detailhandel. DDoS udgør ikke alene en trussel for angrebets egentlige mål, men også for den teleinfrastruktur, som overfører angrebene. Det kan betyde, at andre end det direkte offer også oplever afbrudte eller langsomme teletjenester. CFCS vurderer, at truslen fra DDoS-angreb udgør den væsentligste trussel mod tilgængeligheden af de danske teletjenester. De danske teletjenester er fortsat dygtige til at beskytte sig mod og afværge disse angreb.

De alvorligste DDoS-angreb bliver løbende kraftigere og mere avancerede, ligesom der er en stigning i brug af "booters/stressers". Det er værktøjer, der er tilgængelige via internettet, og som er udviklet til at stressteste servere med DDoS-angreb, men som også kan bruges ondsindet. DDoS kan også bruges til at forsøge at fjerne opmærksomheden fra andre alvorlige cyberangreb.

Organisationer, der besidder medicinske data, persondata og intellektuel ejendom, udsættes også for DDoS med det formål at afpresse dem til at betale for at få stoppet angrebet og genvinde adgang til egne data.

Hacks mod bankkonti og betalingskort rammer både kunder og virksomheder
Den finansielle sektor er et naturligt mål for cyberkriminalitet. For virksomheder i sektoren er det ikke kun cyberangreb rettet mod virksomhedens systemer og infrastruktur, som er problematiske, men også kriminelle handlinger rettet mod deres kunder. Det gælder f.eks. for de danske banker i sager om kriminelle, som forsøger at få adgang til kunders bankkonti eller lave betalingskortsvindel. Eller for legitime webbutikker, hvor hackere udnytter en sårbarhed i en butiks betalingssystem til at omdirigere betalingen eller stjæle betalingskortinformation fra køberen. Grundlaget for cyberkriminelle er stort, da 77 % af den danske befolkning mellem 16 og 89 år har anvendt e-handel til f.eks. køb af tøj, rejser, oplevelser og dagligvarer, og tendensen er stigende.

Nets anbefaler, at danske banker udskifter 100.000 betalingskort pga. onlinesvindel
Nets, som udbyder betalingskort i Danmark, så i september og oktober 2016, at betalingskort udstedt i Danmark, og som blev brugt online, i stigende grad blev udnyttet. Nets meddelte offentligt, at kilden til udnyttelsen var en udenlandsk webbutik, og at en stor mængde personlig kortinformation var blevet kompromitteret. Nets anbefalede danske banker, som står for at udstede betalingskort, at udskifte først 15.000 kort, siden 100.000 kort præventivt. Der er tale om en af de største potentielle kompromitteringer af betalingskort, man har set i Danmark.

I løbet af de første tre kvartaler i 2016 indrapporterede danske banker 970 tilfælde til FinansDanmark, hvor cyberkriminelle havde forsøgt at få adgang til danske netbanker ved at lokke oplysningerne fra bankkunder. FinansDanmark har endnu ikke offentliggjort tallene fra fjerde kvartal, men oplyser om en kraftig stigning i dette kvartal. Via phishing, smishing og social engineering lokker de kriminelle bankkunder til at afgive deres personlige kontooplysninger enten direkte eller ved at lokke dem ind på falske sider, der ligner deres netbank til forveksling.

Cyberaktivisme

Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver. Cyberaktivister kan fokusere på enkeltsager, personer eller organisationer, som de opfatter som modstandere af deres sag. På trods af kapacitet i aktivistiske cybermiljøer, har CFCS ikke kendskab til mange eksempler på cyberaktivisme rettet mod danske myndigheder og virksomheder og vurderer, at den generelle trussel er **MIDDEL**.

Der er dog eksempler på varsler om og opfordringer til cyberaktivisme, som ikke har ledt til egentlige hændelser.

Billede fra #OpIcarus-kampagnen lagt på Opicarus-blog

Eksempelvis har en aktør, som hævder at tilhøre hackerkollektivet Anonymous, i 2016 på sociale medier opfordret til og varslet hackerangreb mod større finansielle institutioner i verden, herunder Danmarks Nationalbank. Aktøren henviste til en kampagne, som Anonymous allerede havde lanceret i 2011, kaldet #OpIcarus, som også er blevet knyttet til den fysiske manifestation "Occupy Wall Street". 2016-varslet førte imidlertid ikke til konkret angreb i Danmark.

Cyberaktivismens sagsorienterede natur gør, at truslen pludseligt kan stige for en konkret myndighed, virksomhed eller person, som kommer i aktivisters søgelys. Udover DDoS-angreb og defacement af hjemmesider eller anden chikane benytter cyberaktivister også læk af følsomme oplysninger erhvervet gennem hacking af f.eks. personlige mailkonti.

Danske hackere blev dømt for at lække politikeres personlige oplysninger
I 2016 blev to danske mænd dømt for politisk motiveret hacking af 101 firmaer og organisationers hjemmesider. De to hackede sig i 2014 bl.a. ind i partiet SF's systemer og fik adgang til partimedlemmers personlige oplysninger. Hackerne offentliggjorde navn, adresse og cpr-nummer på 22 SF-politikere og i alt 91 medlemmer af det danske Folketing. Hackernes motiv var angiveligt at ramme alle politikere, der havde stemt for en lov om Center for Cybersikkerhed, som hackerne opfattede som et overgreb på retten til privatliv.

Statslige aktører anvender også cyberaktivisme som dække i lokale konflikter og i den politiske meningsdannelse. Det kaldes falsk flag og beskrives senere i trusselsvurderingen.

Cyberterror

I denne trusselsvurdering dækker cyberterror alene over terrorhandlinger via internettet med det formål at forårsage død eller voldsom ødelæggelse. Terrorgruppers øvrige brug af internettet til ondsindede formål betragtes derfor ikke som cyberterror. Det gælder cyberhændelser, der chikanerer eller generer, såsom defacement af hjemmesider. Eller kriminelle handlinger med henblik på terrorfinansiering. Kendte terrorgruppers brug af sociale medier til rekruttering eller propaganda defineres heller ikke som cyberterror. CFCS vurderer, at truslen fra cyberterror mod Danmark er **LAV**.

CFCS vurderer, at aktører, som er kendt for forsøg på eller har udtrykt intention om at begå konventionel terror, såsom militante islamistiske grupper, ikke på nuværende tidspunkt har den fornødne kapacitet til at begå cyberterror. Det er sandsynligt, at militante islamistiske grupper ønsker at opbygge en cyberkapacitet, men det er ikke højt prioriteret på kort sigt.

Truslen vil stige, hvis det lykkes terrorgrupper at tiltrække medlemmer med tilstrækkelige tekniske færdigheder, eller hvis etablerede hackere bliver radikaliseret. Trusselsbilledet kan også forandre sig, hvis terrorister køber sig til services via internettets sorte markeder.

Lykkes terrorgrupper med at tilegne sig de fornødne tekniske færdigheder, vil en række scenarier være tænkelige. Terrorister kunne f.eks. bruge cyberkapaciteter i forbindelse med et konventionelt terrorangreb for at forstærke effekten eller få assistance fra statsaktører, der har en interesse i at udføre destruktive cyberangreb uden selv at stå som afsender.

Destruktive cyberangreb

Destruktive cyberangreb defineres i denne trusselsvurdering som et værktøj, der kan anvendes af forskellige aktører med forskellige formål. Det er altså den ønskede effekt af et cyberangreb, som er afgørende for, om det er destruktivt. Destruktive cyberangreb er derfor ikke en selvstændig trusselskategori på linje med cyberspionage eller cyberterror. Men det er meningsfuldt at beskrive og vurdere truslen fra især staters brug heraf, da visse stater har cyberkapaciteter til at kunne gennemføre destruktive cyberangreb.

Der er tale om et destruktivt cyberangreb, når 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 længere kan anvendes.

Der findes flere eksempler på, at fremmede stater har rettet cyberangreb mod industrielle kontrolsystemer i udlandet. Cyberangrebene kan indgå i en hybrid med mere konventionelle angreb og fysiske virkemidler, f.eks. brug af insidere. Ofte benytter hackerne spear phishing til at sprede malware og opsnappe brugernavne og adgangskoder til selve kontrolsystemet, som de så kan styre. Hidtil har stater primært lavet angreb i en grad, der har været generende, haft en politisk signalværdi eller haft karakter af gengældelse, men uden at forårsage voldsom ødelæggelse eller tab af liv.

CFCS vurderer, at det er mindre sandsynligt, at fremmede stater med kapacitet dertil vil rette et egentligt destruktivt cyberangreb mod et industrielt system eller kritisk infrastruktur i Danmark. Men hvis en politisk eller militær konflikt opstår mellem Danmark og en sådan fremmed stat kan infrastruktur og systemer blive mål for denne type cyberangreb.

Cyberangreb forårsagede strømafbrydelser i Ukraine
I december 2015 blev flere elselskaber i det vestlige Ukraine ramt af cyberangreb. Hackerne fik adgang til elselskabernes kontrolsystemer og lukkede for strømmen i den ramte region. Halvdelen af boligerne i regionen var uden strøm i op til 6 timer. Det er beskrevet i åbne kilder, at en fremmed stat stod bag angrebet, og at der har været flere formodede forsøg på at kompromittere ukrainske elselskaber og andre mål i landet i 2016.

I Saudi-Arabien har virksomheder og myndigheder inden for energi, luftfart og andre sektorer gentagne gange været ramt af de såkaldte Shamoon-angreb, hvor malware overskriver eller sletter data på en computers harddisk. Det føromtalte Sony-hack og angrebet mod TV5 Monde omtalt senere i vurderingen er også eksempler på destruktive cyberangreb.

Udviklingstrends og metoder går på tværs af trusler og aktører

Uanset om formålet er spionage, kriminalitet, aktivisme eller terror, er der metoder som går på tværs af typen af cybertrusler. Brugen af f.eks. DDoS-angreb, phishing-kampagner og social engineering er ikke unikt for ét formål. Forskellige hackere vil også udnytte de samme sårbarheder eller udvikling i teknologi, og den samme hacker eller hackergruppe kan i forskellige sammenhænge bære forskellige kasketter og udføre sine ulovlige handlinger med forskellige formål.

Avancerede værktøjer til cyberangreb er i stigende grad tilgængelige i en bredere kreds. Cyberkapaciteter, der tidligere primært var forbundet med statslige aktører, ser man derfor i nogen grad også blandt grupper, der primært udfører cyberkriminalitet eller cyberaktivisme.

Det kan for efterforskere være svært at skelne mellem aktører, hvis hackerne køber infrastruktur på det sorte marked. Desuden er de fysiske aktører til en vis grad skjult i cyberdomænet. Så efterforskere må ud fra IP-adresser, mønstre i aktivitet, metoder og motiv drage konklusioner om hackergrupper og cyberpersonaer, der kan dække over konkrete individuelle hackere.

Fordi metoderne går på tværs af de forskellige formål, kan det altså være vanskeligt at udpege, hvem der står bag en given hændelse. Denne udfordring udnytter forskellige aktører også til at angribe under det man kalder falsk flag. I en falsk flag-operation forsøger aktøren at give indtryk af, at en anden aktør står bag angrebet. Formålet kan f.eks. være at bevare anonymitet, at trække opmærksomhed væk fra et angrebs egentlige formål eller at give sit budskab en anden afsender. Det kan f.eks. være en statslig aktør, der udgiver sig for at være politiske aktivister eller terrorister.

Cyberaktivisme mod TV5 Monde lignede angreb fra en terroristgruppe
Om aftenen den 8. april 2015 holdt alle den franske tv-station TV5 Mondes 12 kanaler ufrivilligt op med at sende. Stationen var blevet udsat for et avanceret cyberangreb. På sociale medier tog en gruppe, der kaldte sig for "the Cyber Caliphate" ansvar for angrebet, og medier spekulerede i, om Islamisk Stat (IS) stod bag angrebet. Efterforskere har siden sået alvorligt tvivl herom og har linket angrebet og de avancerede metoder til en statsstøttet hackergruppe.

På tværs af formål gælder det, at hackeres arbejde ikke kun handler om tekniske evner eller systemers sårbarheder, men i høj grad også om den menneskelige faktor. Phishing-kampagner og social engineering er udbredte virkemidler til at gennemtrænge de første barrierer hos organisationer og kan omgå selv opdaterede og avancerede systemer. Aktører udvikler altså ikke kun deres malware, men forbedrer også kvaliteten af phishing-mails eller laver falske domæner, der er næsten identiske med de ægte.

Der er flere nyere eksempler fra både Danmark og udlandet, hvor hackere har sendt troværdige spear phishing-mails til myndigheder eller forsøgt at få medarbejdere til at logge på falske, men vellignende login-sider. Ligeledes udvikler flere aktører evner til at udnytte legitime hjemmesider til at lave watering holes og inficere hjemmesidens besøgere med malware.

Nogle aktører bruger i stigende grad malware målrettet telefoner. I takt med at mobiltelefoner i stigende grad bruges som små computere, stiger også kompleksiteten af den malware, der bruges til at angribe mobile enheder. Angrebsmetoderne begynder mere og mere at ligne metoder brugt mod egentlige computere. Også her bruger aktørerne social engineering, f.eks. ved at sende falske sms'er med links, der indeholder malware, såkaldt smishing.

Hackerne kan udnytte, at flere og flere anvender cloud computing til at opbevare data eller tilgå services via sociale medier, webmails eller ved back-up af data på mobiltelefoner. Det åbner yderligere muligheder for social engineering. Akører kan f.eks. lave falske beskeder om, at passwords til mailkonti eller profiler på sociale medier er udløbet og lokke brugere til at følge links for at forny deres passwords, som så kan aflures. Virksomheder kan lagre data i fjerne datacentre, som de ikke selv har kontrol med, og tilgå deres data via internettet. Cloud-leverandørens infrastruktur og virksomhedernes data er derfor sårbare for cybertrusler fra internettet.

Stigningen i brugen af Internet of Things (IoT) åbner nye muligheder for trusselsaktørerne. Fremskrivninger fra internationale it- og televirksomheder estimerer, at der i 2020 vil være ca. 26 milliarder enheder, der er koblet til internettet. Flere mennesker benytter sådanne enheder f.eks. køleskabe, lamper, kameraer eller virtuelle assistenter. Hvis gode sikkerhedsvaner ikke følger med, opstår der nye åbninger for kompromittering. Det er ikke nødvendigvis den enkelte bruger, der er

målet. Men det øgede antal internetforbundne enheder giver flere veje ind i et mål. Angrebsveje, som brugerne ikke nødvendigvis selv er opmærksomme på, såsom et smart-tv med en mikrofon i et mødelokale. Samtidig opstår der mulighed for at knytte de mange enheder sammen i såkaldte botnet, der kan bruges til f.eks. overbelastningsangreb og cyberangreb mod andre og større mål.

Angreb via babyalarmer og dvd-afspillere ramte Netflix, Paypal og Twitter
I oktober 2016 blev en amerikansk domæneudbyder ramt af et DDoS-angreb fra et botnet. Angrebet skabte store problemer med tilgængeligheden for kendte internetsider som Amazon, BBC, Fox News, the Guardian, Netflix, Paypal, Spotify og Twitter. En række statslige hjemmesider i Europa blev også påvirket. Hackerne brugte kompromitterede smart-enheder til angrebet som f.eks. kameraer, printere, dvd-afspillere og babyalarmer. De fleste enheder var ejet af privatpersoner eller små virksomheder.

Det er også muligt, at cyberkriminelle i fremtiden vil udnytte den øgede brug af smart-enheder til f.eks. afpresning af brugere, hvis enheder ikke virker som følge af et hack. Eller at hackere kan gå efter større enkeltmål, som f.eks. fremtidige smart-biler, smart-containerskibe eller smart-byer.

Flere aktører gennemfører kampagner, hvor de scanner it-netværk bredt og systematisk for at finde kendte sårbarheder i it-systemer. I 2015-16 har CFCS set flere angreb mod sårbarheder i et specifikt it-system, som benyttes af flere danske organisationer.

CFCS vurderer, at der ikke altid er tale om direkte forsøg på spionage eller kriminalitet mod den enkelte organisation, men at hackerne undersøger muligheden for at installere bagdøre i systemerne eller opbygge botnet for at teste angrebsscenarier eller til senere angreb mod andre prioriterede mål.

Anbefalinger

Center for Cybersikkerhed anbefaler, at ledelser i både myndigheder og private virksomheder gør sig bevidst om cybertruslen og søger råd i følgende publikationer for at imødegå cybertruslerne:

- Cyberforsvar der virker
- Spear-phishing – et voksende problem
- Reducér risikoen fra ransomware (se også nomoreransom.org)
- Sådan kan du imødegå DDoS-angreb

Myndigheder og private virksomheder bør arbejde målrettet med både processer, teknik og adfærd. Processer er bl.a. regelmæssigt at lave risikoanalyser og finde ud af, hvilke data en organisation vurderer vigtig at beskytte, og hvilke konsekvenser det har, hvis beskyttelsen fejler. Teknik handler bl.a. om at kende egen infrastruktur og løbende identificere og udbedre dens sårbarheder. Adfærd involverer tiltag, der skal øge bevidstheden om cybertruslen hos medarbejdere og

uddanne dem til at begå sig hensigtsmæssigt og sikkert i cyberspace. Desuden bør virksomheder og myndigheder implementere beredskabsplaner, der kan håndtere mulige angreb.

CFCS anbefaler, at myndigheder og virksomheder følger ISO27000-standarderne, som er beskrevet af Digitaliseringsstyrelsens Videnscenter for implementering af ISO27000.

Det er desuden vigtigt at ansætte eller have adgang til personer med de rette kompetencer til at håndtere cybersikkerhed, inden et angreb sker.

CFCS anbefaler, at myndigheder og virksomheder desuden orienterer sig på siden nomore-ransom.org – et internationalt samarbejde som Rigspolitiet er partner i.

Center for Cybersikkerhed
Februar 2017

FE bruger denne skala for sandsynlighed i analyser:

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.

Ordliste

- BEC scams: BEC står for Business Email Compromise og er også kendt som ”CEO Fraud”. I stedet for at sende e-mails til en stor gruppe tilfældige medarbejdere i en virksomhed, laver hackerne grundig research. Det gør dem i stand til at lave troværdige, målrettede e-mails, hvor de f.eks. udgiver sig for at være en direktør, økonomichef eller konsulent i tæt kontakt med den øverste ledelse og lokke ansatte til at agere i den tro, at det er efter ordre fra ledelsen.

- Botnet: Et botnet er et netværk af kompromitterede computere, der styres af en tredjepart. Et botnet bliver skabt ved at computere med internetadgang bliver inficerede med malware, hvorefter den, der kontrollerer botnettet, kan anvende det til f.eks. at lave DDoS-angreb.
- Cloud computing: Begrebet er også kendt som "skyen" og dækker over levering af software, service og tjenesteydelser via internettet. Sociale medier og webmails som f.eks. hotmail eller yahoomail er eksempler på tjenester, hvor applikationen ligger i skyen frem for at være installeret på en lokal computer. Datalagring og back-up kan også foregå via skyen. Skyen adskiller sig fra traditionel hosting, der kun har én server, ved at flere servere eller datacentre kan give brugeren adgang til sine data.
- DDoS-angreb: 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 et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.
- Defacement: Defacement af en hjemmeside er et angreb, der ændrer hjemmesidens visuelle udtryk. F.eks. kan angriberen indsætte en tekst eller et billede på hjemmesidens forside.
- Falsk flag: Falsk flag dækker over angreb, der forsøger at fremstå som om en anden end den egentlige aktør står bag. I samme kategori taler man om faketivists, som er fiktive personaer, der er skabt for at imitere aktivister og fungere som det offentlige talerør, så den egentlige aktør kan benægte at stå bag et hack eller læk af informationer.
- Internet of Things: Internet of things, forkortet IoT, er et udtryk for hverdagsobjekter, som f.eks. køleskabe eller kameraer, der er koblet til internettet. Det gør, at objekterne kan sende og modtage data.
- Kryptering: Kryptering er kodeteknikker, der får information til at fremstå uforståelig for tredjepart. Kryptering bruges ofte til at sikre, at information, der skal sendes via ikke-sikre kommunikationskanaler som f.eks. internettet, ikke kan blive opsnappet og læst af uvedkommende. Men kryptering kan også bruges af hackere, der vil gøre data utilgængelig for dataejeren, f.eks. for at opkræve løsepenge for at dekryptere data.
- Malware: Malware betyder malicious software og er en betegnelse for computerprogrammer, der gør ondsindede, skadelige eller uønskede ting der, hvor de er installeret.
- Phishing: Phishing er forsøg på via social engineering at manipulere en person til i god tro at videregive følsomme oplysninger eller klikke på inficerede filer eller links til falske hjemmesider. Phishing-mails sendes ofte bredt ud til mange modtagere.
- Ransomware-angreb: Hackere forsøger at installere ondsindede værktøjer, der krypterer data på offerets computer eller system. Hackerne kræver løsepenge for igen at give ofret adgang til sine data. Som regel vil hackerne installere malware ved hjælp af phishing, evt. målrettet med social engineering. De fleste ransomware-angreb lykkes, fordi brugere har klikket på noget i en e-mail, sms eller på et reklamebanner på nettet.
- Social engineering: Social engineering er en angrebsteknik, hvor offeret manipuleres til at udføre bestemte handlinger eller til at videregive klassificeret information uden selv at

være klar over det. I forbindelse med it-sikkerhed bruges termen til at beskrive konstruktionen af f.eks. e-mails eller hjemmesider, så de på overfladen ser legitime ud, men i virkeligheden rummer malware. Social engineering kræver et vist kendskab til offeret for at være effektivt.

- Smishing: Smishing er phishing via sms.
- Spear phishing: Spear phishing adskiller sig fra phishing ved i højere grad at være målrettet den enkelte modtager. Forsøg på spear phishing er ofte rettet mod enkeltpersoner, og e-mails er typisk udformet, så de virker særligt relevante, overbevisende og troværdige for modtageren.
- Watering hole: Et watering hole dækker over en angrebsteknik, hvor en ellers legitim hjemmeside, f.eks. en webshop, inficeres med malware. Brugere, der normalt benytter hjemmesiden uden problemer, risikerer at blive inficeret med malware.