CENTER FOR CYBERSIKKERHED

30. januar 2013

Center for Cybersikkerhed: Truslen i cyberspace

Hovedvurdering
De alvorligste cybertrusler mod Danmark kommer fra statslige aktører, som bl.a. ved brug af deres nationale efterretningstjenester udnytter cyberspace til spionage og tyveri af intellektuel ejendom, som eksempelvis informationer om udvikling, forskning eller forretningshemmeligheder.

Ikke-statslige aktører i form af hacktivister og cyberkriminelle udgør ligeledes en trussel mod Danmark. Center for Cybersikkerhed vurderer, at disse grupper har en kapacitet til at forstyrre eller forårsage mindre skade på dansk informations- og kommunikationsteknologisk infrastruktur samt indhente og offentliggøre følsomme data.

En alvorlig og stigende trussel er de såkaldte "Supply chain threats", hvor der allerede i produktionen af hard- og software bliver installeret malware eller teknisk styrbare komponenter, som en aktør skjult kan fjernstyre over internettet.

Den såkaldte 'insider- trussel' er et andet væsentligt aspekt af truslen fra cyberspace. Truslen kommer fra personer i en organisation eller virksomhed, der bevidst bryder sikkerheden og herved medvirker til tyveri af data eller overfører skadelig software til informations- og kommunikationsteknologiske systemer. En variant heraf er den situation, hvor personer ved en målrettet indsats fra en tredjepart ubevidst foretager sig en handling, der bryder sikkerheden.

Det er meget sandsynligt, at udenlandske efterretningstjenester på kort- og mellemlangt sigt fortsat vil indsamle dansk intellektuel ejendom og strategisk viden om Danmarks politiske, militære, økonomiske og samfundsmæssige forhold. Det er ikke sandsynligt, at en statslig aktør inden for denne tidshorisont vil have til hensigt at udføre ødelæggende cyberangreb mod dansk informations- og kommunikationsteknologisk infrastruktur. Det er heller ikke sandsynligt, at ikke-statslige aktører opnår evnen til at gennemføre sådanne angreb.

Selvom netværk og systemer bliver udviklet gennem implementering af styrkede sikkerheds-foranstaltninger, er der en risiko for, at der samtidig implementeres nye sårbarheder, der kan udnyttes til cyberspionage. Det medfører, at systemer og netværk kontinuerligt bør overvåges for at fastholde en acceptabel sikkerhed.

Detaljeret redegørelse
Danmark er regelmæssigt udsat for forsøg på indtrængen i den danske informations- og kommunikationsteknologisk infrastruktur, men der er endnu ikke set ødelæggende cyberangreb i Danmark.

Aktører

Nationalstater

Flere stater har i det seneste årti styrket deres kapaciteter med henblik på at indhente informationer fra computere og netværk. Denne kapacitet bliver normalt opbygget inden for militæret og efterretnings- og sikkerhedstjenesterne.

Ud over indhentning af intellektuel ejendom samt økonomiske og politiske oplysninger fra vestlige firmaer og myndigheder har staterne ofte fokus på indhentning af oplysninger om aktiviteter, personer og organisationer, som de betragter som en trussel, f.eks. systemkritiske personer eller organisationer.

Med den stadig stigende brug af informations og kommunikationsteknologi, og ikke mindst internettet, vurderer CFCS, at tyveri af intellektuel ejendom og egentlig cyberspionage er stigende. Handlingerne kan ske over store afstande og via tredjelande. Det gør, at det er meget vanskeligt at afdække, hvem der står bag, og indhentningen kan gennemføres som målrettede angreb mod enkeltpersoner eller organisationer, der besidder sensitive informationer. Ligeledes kan indhentningen målrettes mod firmaer for at indhente informationer om patenter, budgetter eller fremtidsplaner. En udbredt fremgangsmåde er såkaldt spear phishing, hvor eksempelvis en tilsyneladende troværdig e-mail sendes til centrale personer i en virksomhed eller organisation for at stjæle oplysninger.

Der er tegn på, at nogle stater anvender ikke-statslige grupperinger og enkeltpersoner til at gennemføre cyberangreb for at undgå, at cyberangreb mod og kompromittering af andre nationers informations- og kommunikationsteknologiske systemer bliver tilskrevet de pågældende stater. Det er set, at nogle stater anvender egne studerende på universiteter enten hjemme eller i den nation, man ønsker at angribe eller kompromittere, til at gennemføre sådanne aktiviteter.

Det er sandsynligt, at stater vil fortsætte med at anvende betragtelige ressourcer på at udvikle offensive og defensive cyberkapaciteter.

CFCS vurderer, at der fortsat vil være stater, der vil kompromittere netværk og servere for at skaffe sig informationer, der kan understøtte deres økonomiske, militære og samfundsmæssige udvikling. Det vurderes ikke sandsynligt, at der er stater, der på kort eller mellemlangt sigt vil udføre et ødelæggende cyberangreb mod den danske informations- og kommunikationsteknologiske infrastruktur.
Det er sandsynligt, at cyberspace i stigende grad vil blive anvendt til spionageformål.

Ikke-statslige aktører

Hacktivister
Truslen fra cyberspace kommer i stigende grad fra forskellige grupper af hackere, hvis cyberaktiviteter ofte er politisk eller ideologisk motiverede. Den politisk motiverede hacking bliver ofte kaldt for hacktivisme, som er en sammentrækning af hacking og aktivisme.
En af de mest aktive hackergrupper er Anonymous, som er et løst sammenhængende hackerkollektiv, hvor associerede personer kan udføre angreb i gruppens navn. Anonymous ønsker gennem sine hackeraktiviteter at gøre opmærksom på sociale og politiske forhold og kæmper mod tiltag, som den betragter som censur af internettet.

Adskillige offentlige svenske hjemmesider tilhørende institutioner, så som Nationalbanken og Rigspolitiet blev i efteråret 2012 udsat for DDOS-angreb, der strakte sig over et par dage. Personer der hævdede at komme fra Anonmyous erklærede, at DDOS-angrebet var en protest mod de svenske myndigheders udleveringsbegæring af Wikileaks-stifteren Assange.

Også i Danmark eksisterer der aktive hackergrupper. En gruppering ved navn UN1M4TR1X0 (Unimatrix Zero) med selverklæret tilknytning til Anonymous tog i begyndelse af 2012 ansvaret at have hacket nyhedsbureauet Ritzau, interesseorganisationen IT-Branchen samt Statsforvaltningens hjemmeside. En anden dansk hackergruppering, der går under navnet Unorthodox, tog i april 2012 ansvaret for at gøre PET's hjemmeside utilgængelig med et DDOS-angreb. Dette skete som en protest mod brugen af aflytningssoftware, der kan installeres på en mistænkts computer. I juli 2012 var fagforeningen 3F's hjemmeside i perioder utilgængelig som følge af DDOS-angreb. En person med selverklæret tilknytning til Anonymous anførte, at angrebet skete i protest mod blokaden af Vejlegården. Senere i november 2012 blev Det Centrale Personregisters hjemmeside cpr.dk angrebet af Anonymous, der også hævdede at have adgang til oplysninger fra en IT-virksomhed og et vandværk.

CFCS vurderer, at hacktivister har evnen til at udføre angreb, der kan forstyrre eller forårsage mindre skade på danske myndigheders informations- og kommunikationsteknologiske systemer. Hacktivisterne kan endvidere skaffe sig adgang til personfølsomme og forretningskritiske informationer, hvis net og systemer ikke har en tilstrækkelig sikring.

Angrebsmetoder
Trusler i cyberspace er en kombination af mennesker og maskiner. Truslerne kan opdeles i to kategorier. De lavteknologiske og ikke målrettede angreb, som hverken kræver store tekniske færdigheder eller solid økonomi at realisere, og de højt specialiserede målrettede angreb, som bliver udført af eksperter og muligvis understøttes af statslige aktører.

Den første kategori udgør især et problem på grund af kvantiteten, og kan generelt set betragtes som værende "baggrundsstøj" på internettet, eksempelvis simple netværksscanninger og spam-mail til brug for phishing. Dette kan i vid udstrækning bortfiltreres ved brug af passende sikkerhedsforanstaltninger.

Målrettede angreb
Den anden kategori adresserer særlige forhold typisk fokuseret mod veldefinerede mål – heraf betegnelsen målrettede angreb. Et avanceret eksempel er Stuxnet, der er en såkaldt computerorm, der i 2010 inficerede Siemens Programmable Logic Controllers (PLC) i Iran. Stuxnet var udarbejdet med indgående kendskab til og viden om sårbarheder i den konkrete infrastruktur og de tilhørende anvendte komponenter.

Fakta om Advanced Persistent Threats (APT)
APT betegner truslen fra hackere, der forsøger at opnå uautoriseret adgang til en udvalgt myndighed eller virksomheds netværk. Angrebet gennemføres som regel med spionage for øje og forberedes normalt grundigt. Det kan strække sig over meget lang tid, eksempelvis flere år. Angriberen søger ved brug af forskelligt malware at opretholde adgang til netværket og løbende udtrække data herfra. Den anvendte malware vil blive løbende opdateret for at undgå opdagelse og der vil normalt blive brugt flere forskellige typer malware samtidigt for at kunne bevare adgang til netværket, selvom angrebet måtte blive opdaget.

Også danske virksomheder og myndigheder har været udsat for målrettede angreb. I 2012 har CFCS i flere tilfælde bistået berørte institutioner med at bekæmpe målrettede angreb. Højteknologiske virksomheder har været særligt udsat, da de ligge inde med forretningshemmeligheder, som kan være interessant for andre aktører. Denne type angreb er foretaget af aktører, som har store ressourcer til rådighed, og som arbejder gennem lang tid for at opnå et resultat. CFCS vurderer, at sådanne angreb enten udføres af statslige eller statssponsorerede aktører.

Målrettede angreb er meget effektive. Som eksempel blev der sendt en mail, der angiveligt kom fra ledelsen til et begrænset antal chefer med en vedhæftet fil, der skulle omhandle medarbejderrokader. Otte ud af ti modtagere klikkede på den vedhæftede fil, hvorved systemet blev infiltreret. CFCS må formode, at store mængder data kan være stjålet fra disse virksomheder. I et andet eksempel har angriberen haft fodfæste i virksomhedens net i adskillige år. Dette er moderne industrispionage, som kan sikre konkurrenter et forskningsmæssigt forspring uden at være nødt til at anvende store summer på en selvstændig udviklingsindsats.

Insider truslen
'Insider- trusler' er et andet væsentligt aspekt af truslen fra cyberspace. Begrebet dækker over personer i en organisation eller en virksomhed med fysisk adgang til informations- og kommunikationsteknologisk infrastruktur, som bevidst eller ubevidst medvirker til tyveri af data eller overfører malware til informations- og kommunikationsteknologiske systemer. Insider truslen kan opdeles i en bevidst- og en ubevidst trussel.

Den bevidste trussel kommer fra personer, der eksempelvis af ideologiske grunde eller for økonomisk

vindings skyld uberettiget fjerner information fra en organisation eller en virksomhed, og overdrager det til en tredjepart. Et eksempel på den bevidste trussel er en amerikanske soldat, som er anklaget for at have lækket fortrolige dokumenter fra krigene i Afghanistan og Irak til internetsiden WikiLeaks. Den bevidste trussel kan også bestå i, at en person installerer skadelig malware, der enten videresender informationer til en tredjepart, eller giver tredjeparten adgang til eller kontrollen over et system.

Den ubevidste trussel kommer fra personer, der bryder sikkerheden ved f.eks. at anvende private eller ikke godkendte USB-medier, der kan indeholde skadelig malware, som automatisk bliver aktiveret, når mediet bliver sat i computeren. Derved udsætter brugeren utilsigtet en computer eller et netværk for en betydelig sikkerhedsrisiko. Den ubevidste trussel kommer også fra personer, der offentliggør sensitiv information på internettet, faglige chatfora eller sociale medier som Facebook og Twitter.
CFCS har ved flere episoder konstateret, at samme USB-medie er blevet anvendt mellem lukkede sikrede systemer og åbne systemer med adgang til internettet. Derved opstår risikoen for, at eksempelvis malware sender klassificerede informationer fra et lukket system via internettet til udenforstående aktører.

Supply chain threat
En alvorlig og stigende trussel er den såkaldte "Supply chain threat", hvor der allerede i produktionen af hard- og software bliver installeret malware eller teknisk styrbare komponenter, som en aktør kan fjernstyre over internettet. "Supply chain threats" kan forekomme i flere led i produktionskæden, og soft – og hardwaren er ofte så kompleks eller utilgængelig, at selv store internationale infrastrukturvirksomheder som slutbrugere ikke opdager den.

Et eksempel på en utilsigtet, men potentielt yderst alvorlig "Supply chain threat" er uautoriseret adgang til den testfunktionalitet, som en producent af en FPGA - Field Programmable Gate Array (avanceret mikrochip) normalt indsætter i sit FPGA-design til eget brug. Den pågældende testfunktionalitet giver ubegrænsede muligheder for at tilføje usynligt funktionalitet, indlæse hemmelige krypteringsnøgler og centrale opsætningsparametre i FPGA'en mm. Af sikkerhedsmæssige årsager bliver adgangen til testfunktionaliteten derfor blokeret af FPGA-producenten, således at uvedkommende ikke kan få adgang til denne yderst sikkerhedskritiske funktionalitet.

I marts måned 2012 kunne to engelske forskere imidlertid dokumentere, at de ved brug af nyudviklet metode, enkelt laboratorieudstyr og en dags test havde fået adgang til testfunktionaliteten i en af markedets mest sikre FPGA fra den amerikanske virksomhed Actel/Mircrosemi, der bl.a. producerer mikrochips til militære formål. Som dokumentation kunne de to forskere i løbet af få sekunder udlæse den hemmelige AES-nøgle i et kryptoudstyr, der benyttede den pågældende FPGA.

CFCS vurderer, at det er sandsynligt, at angrebsmetoder i cyberspace på kort og mellemlangt sigt vil blive mere sofistikerede og professionelle. Der vil dog fortsat være risiko for, at mindre professionelle aktører kan udnytte svagheder i software eller informations- og kommunikationsteknologiske systemer.

Teknologisk udvikling påvirker trusselsbilledet
Den teknologiske udvikling i cyberspace medfører bl.a. at antallet af maskiner og udstyr, der opkobles til Internettet stiger hastigt og forventes at være flerdoblet inden for få år. I fremtiden vil flere systemer og netværk af vital betydning for samfundet være integreret via nettet. Ansatte i virksomheder og i offentlige myndigheder vil i stigende omfang kunne få adgang til informationer i firmaernes eller organisationernes

netværk fra mobile enheder. Ofte har de mobile enheder ikke den samme grad af sikkerhed som stationære eller bærbare computere. Det medfører en øget risiko for, at data, der bliver sendt mellem disse medier, bliver kompromitteret, eller at selve enheden bliver brugt til at få direkte adgang til et netværk.

Bedre bekæmpelse af malware

Den teknologiske udvikling betyder dog også, at der er øget fokus på sikkerheden i kommende informations- og kommunikationsteknologiske systemer. Det medfører, at det vil være stadig sværere for ikke-professionelle at udvikle værktøjer, der kan ødelægge, inficere eller overtage kontrollen med computere og informations- og kommunikationsteknologiske systemer. Omvendt stilles disse værktøjer ofte til rådighed som en serviceydelse via internettet, såkaldt "crime-as-a-service". Flere institutioner og firmaer er endvidere begyndt at beskytte sensitive og fortrolige informationer gennem fysisk adskillelse af deres netværk fra internettet eller ved at sikre deres netværk gennem sektionering og rettighedsstyret adgangskontrol.

Malware

Malware, som ifølge åbne kilder, er programmer, der gør skade eller udfører uønskede handlinger på en computer, er blevet mere sofistikeret og har fået indbygget flere angrebsmetoder. Kompleksiteten i kodningen af visse typer af malware tyder på, at de er udviklet af cyberaktører med en stor teknisk indsigt og mange ressourcer. Noget malware er skabt med henblik på at udføre meget målrettede handlinger, mens andet malware rammer mere bredt.

"Stuxnet" er ligeledes et eksempel på yderst kompliceret malware, der fra begyndelsen har været målrettet til at ramme bestemte systemer, som bruges i industrien. Ifølge åbne kilder er "Stuxnet" udviklet i et samarbejde mellem USA og Israel, og virussen satte ligeledes ifølge åbne kilder i 2010 centrifuger på uranberigelsesanlægget i Natanz i Iran ud af kraft.

"Flame": I 2012 blev en computervirus ved navn Flame fundet på internettet. Virussen ser ud til at være en kompleks og avanceret malware. Iran, Israel, Sudan, Libanon, Saudi-Arabien og Egypten er blandt de lande, der målrettet er blevet angrebet af virussen, og flere eksperter mener, at virussen, der er i stand indsamle store mængder information fra inficerede computere, er udviklet af en eller flere statslige aktører. It-sikkerhedsfirmaet Kaspersky Lab har fundet ligheder i kodning af "Flame" og "Stuxnet".

"Red October": I januar 2013 blev der opdaget malware, der gik målrettet efter statslige myndigheder og diplomatiske repræsentationer. Malwaren havde været aktivt i mere end fem år, og kunne blandt andet indsamle krypterede filer og data fra mobiltelefoner tilsluttet inficerede pc'er.

CFCS vurderer, at det er sandsynligt, at angrebsmetoder i cyberspace på kort og mellemlangt sigt vil blive mere sofistikerede og professionelle. Der vil dog fortsat være risiko for, at mindre professionelle aktører

kan udnytte svagheder i software eller informations- og kommunikationsteknologiske systemer.

Fremtiden vil byde på flere og flere systemer og netværk, som vil blive integreret og være af vital betydning for samfundets virke. Selvom de foreliggende sikkerhedsforanstaltninger styrkes, og der implementeres nye sikkerhedsfunktionaliteter, vil udviklingen gøre, at der også vil implementeres nye sårbarheder, så systemer og netværk kontinuerligt bør overvåges.