CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod telesektoren

Trusselsvurderingen redegør for de cybertrusler, som er rettet imod telesektoren i Danmark. Telesektoren i Danmark er af kritisk betydning for samfundets funktion, stabilitet og sikkerhed. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen for virksomheder i sektoren.

Trusselsvurderingen er opdateret med ændringer i kapitlerne om cyberaktivisme og cyberterror som følge af ændrede trusselsniveauer i den nationale trusselsvurdering "Cybertruslen mod Danmark" udgivet juni 2020. Ligesom i den nationale vurdering er der tilføjet et trusselsniveau for destruktive cyberangreb

Dato: Oktober 2019
Opdateret juni 2020

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf. 33 32 55 80
E-mail cfcs@cfcs.dk
www.cfcs.dk

Hovedvurdering

- Truslen fra cyberkriminalitet mod telesektoren er **MEGET HØJ**. Cyberkriminelle truer primært teleudbyderens forretning, men kan også kompromittere teleinfrastruktur i forsøg på at ramme telesektorens kunder. Cyberkriminalitet kan påvirke tilgængeligheden af teletjenester.
- Truslen fra cyberspionage mod telesektoren er **HØJ**. Formålet er at indhente oplysninger om teleudbyderen og teleinfrastruktur samt teleudbyderens kunder og deres kommunikation. Det er mindre sandsynligt, at cyberspionage vil påvirke tilgængeligheden af teletjenesterne.
- Truslen fra destruktive cyberangreb mod telesektoren i Danmark er **LAV**. Det er dog muligt, at sektoren kan blive ramt af følgevirkningerne af et destruktivt cyberangreb mod mål udenfor Danmark.
- Truslen fra cyberaktivisme mod telesektoren er **LAV**. Telerelaterede emner i den offentlige debat kan tiltrække sig opmærksomhed fra cyberaktivister, men det er mindre sandsynligt, at det vil føre til cyberaktivisme mod telesektoren.
- Truslen fra cyberterror mod telesektoren er **INGEN**. Denne type angreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.
- DDoS-angreb udgør fortsat en alvorlig trussel mod tilgængeligheden af teletjenester.

Indledning

Denne trusselsvurdering beskriver cybertruslerne mod telesektoren i Danmark. Vurderingen er udarbejdet af Trusselsvurderingsenheden ved Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS). Trusselsvurderingen erstatter den tidligere trusselsvurdering fra februar 2017.

Trusselsvurderingen behandler cybertrusler, som kan påvirke tilgængeligheden, integriteten eller fortroligheden af teletjenesterne eller som kan skade teleudbydernes virksomhed. Set fra et samfundsmæssigt perspektiv er truslerne mod tilgængeligheden af teletjenesterne de mest alvorlige.

I denne vurdering defineres telesektoren som de erhvervsmæssige teleudbydere, der offentligt udbyder de tjenester og den teleinfrastruktur, som gør det muligt for myndigheder, virksomheder og borgere at kommunikere elektronisk over faste eller mobile forbindelser.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede og 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.

Hvad er cybertrusler
Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør ved hjælp af it forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester.

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering beskriver og vurderer CFCS truslen ud fra cyberaktørens formål med angrebet, ligesom der fokuseres på enkelte angrebsmetoder.

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. Det kan også være it-infrastruktur, tid, penge og adgang til information.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod telesektoren i Danmark er **MEGET HØJ**. Det er således meget sandsynligt, at virksomheder i sektoren vil blive udsat for forsøg på cyberkriminalitet.

Cyberkriminalitet er drevet af ønsket om økonomisk vinding. Hovedparten af den cyberkriminalitet som rammer telesektoren er ikke entydigt rettet mod sektoren, men er forårsaget af cyberkriminelle, som går bredt efter virksomheder på tværs af samfundet.

Truslen er kompleks, og virksomheder i telesektoren er blandt andet udsat for den vedvarende trussel fra cyberkriminalitet, som forsøger at skabe en profit ved at ramme så mange ofre som muligt. Sektoren er også udsat for den mere målrettede trussel fra hackergrupper, som

udfører målrettede og avancerede hackerangreb mod få udvalgte ofre, herunder i telesektoren.

Telesektoren er derudover udsat for truslen fra avancerede hackergrupper, som forsøger at kompromittere teleinfrastruktur for at ramme kunder og andre brugere af mobil- og internettet. Den type kompromittering kan påvirke tilgængelighed, fortrolighed eller integritet af teletjenester.

Cyberkriminelle udnytter i stort omfang velkendte metoder og sårbarheder, men er også hurtige til at omstille sig for at udnytte nye sårbarheder, metoder og exploits.

Cyberkriminelle kompromitterer kundekonti og selvbetjeningsløsninger

Teleudbydere har ofte selvbetjeningsløsninger, hvor private kunder kan administrere deres internet- eller mobil-abonnement samt tjenester som e-mail og streaming af film og musik. Til erhvervskunder findes der også selvbetjeningsløsninger, hvor det eksempelvis er muligt at administrere virksomhedens mobilabonnementer.

Sådanne løsninger og tjenester er attraktive mål for cyberkriminelle, og det er sandsynligt, at cyberkriminelle vil forsøge at skaffe sig adgang til dem for at videresælge adgangen til streamingtjenester eller for at udnytte kundedata, brugernavne, kodeord eller e-mail-konti i andre cyberangreb.

Stofa kundekonti kompromitteret

I september 2018 lukkede danske Stofa midlertidigt for kundernes adgang til selvbetjeningsløsningen "Mine Sider", fordi udefrakommende havde skaffet sig adgang til cirka 2.000 kunders konti.

I udlandet er der eksempler på, at en teleudbyders kundekonti kompromitteres, fordi cyberkriminelle ønsker at overtage specifikke kunders mobilnumre. Ved at overtage en kundes mobilnummer kan de kriminelle få adgang til sms-beskeder med to-faktor kodeord, der giver adgang til online tjenester såsom netbank eller webmail, hvor de kriminelle allerede har fået kendskab til brugernavn og kodeord. Ved hjælp af adgangen til selvbetjeningsløsningen kan de kriminelle forsøge at narre udbyderen til at sende kunden et nyt simkort, som så opsnappes af de kriminelle. I 2017 lykkedes det cyberkriminelle at få adgang til hundreder af kundekonti hos T-Mobile i USA netop med det formål at overtage kunders mobilnummer. Det er sandsynligt, at cyberkriminelle også i Danmark vil forsøge at omgå teleudbydernes sikkerhedsmekanismer med det formål at overtage udvalgte kunders mobilnummer.

Fysiske simkort vil over de kommende år gradvist blive erstattet med digitale simkort, også kaldet eSIM, som kunderne downloader fra teleudbyderen og installerer på en chip på den mobile enhed. I Danmark tilbyder visse teleudbydere allerede eSIM til kunder, som benytter mobile enheder, der understøtter teknologien. CFCS vurderer, at cyberkriminelle vil forsøge at bryde sikkerheden ved eSIM, samt de procedurer som teleudbyderne anvender ved bestilling og levering af eSIM til kunderne, blandt andet med det formål at overtage mobilnumre.

Cyberkriminelle forsøger at udnytte svagheder i SS7-netværket
En avanceret metode til at opsnappe sms-beskeder er at kompromittere det såkaldte SS7-netværk, som forbinder alle verdens mobilnet, og omdirigere bestemte personers sms-beskeder til de kriminelle. Metoden er i 2018 blevet anvendt mod kunder hos den engelske Metro Bank, ligesom også enkelte kunder hos teleudbyderen O2-telefonica i Tyskland i april 2017 fik opsnappet sms'er med to-faktor kodeord til deres bankkonti.

Det kræver en særlig viden at få adgang til, og ikke mindst kompromittere, SS7-netværket, og CFCS vurderer, at kun få cyberkriminelle grupper er i stand til det. Der er dog en risiko for, at kriminelle, som potentielt opnår denne adgang, vælger at stille den til rådighed for andre kriminelle mod betaling.

Teleinfrastruktur kan blive kompromitteret for at omdirigere brugernes internettrafik til kriminelle
Der er avancerede hackergrupper, som forsøger at omdirigere internettrafik til falske hjemmesider for at opsnappe adgangskoder til digitale tjenester, sprede malware, eller vise reklamer, som genererer en indtægt til de kriminelle. Selvom det endelige offer er brugerne af internettet, så foregår angrebet ved at kompromittere teleinfrastruktur eller centrale internetservices i telesektoren.

Såkaldte BGP-hijacks kan bruges til at omdirigere store mængder internettrafik til cyberkriminelle. Hjemmesiden BGPStream.com, som overvåger BGP-routing på internettet, har siden 2016 registreret omkring 200 mulige BGP-hijack hver måned. I april 2018 lykkedes det udenlandske cyberkriminelle at stjæle kryptovaluta ved hjælp af et BGP-hijack, som omdirigerede brugere af tjenesten MyEtherWallet.com til en falsk login-side.

BGP-hijack
Betegner en ondsindet ændring af routingdata i en såkaldt Border Gateway Protocol router. BGP-routere anvendes til at forbinde de mange netværk, der tilsammen udgør internettet. Routeren fortæller nabonetværk hvilke IP-adresser, som kan nås fra netværket.

Kun få cyberkriminelle har kapacitet til at udføre et BGP-hijack, men på grund af internettets opbygning, kan et BGP-hijack påvirke danske internetbrugere, uanset hvor i verden det sker. Konsekvenserne af et BGP-hijack kan være særligt alvorlige, hvis det ikke lykkes en dansk teleudbyder at bortfiltrere falske BGP routinginformationer, som er opstået i, eller har spredt sig til, tilstødende netværk. Udover at omdirigere internettrafik kan et BGP-hijack medføre, at dele af internettrafikken bliver langsom eller afbrudt. Uden effektiv overvågning af ændringer i BGP-routning kan et BGP-hijack, som ikke giver trafikforstyrrelser, potentielt være effektivt i dage eller uger.

DNS-server

En DNS-server indeholder oplysninger om, hvilken IP-adresse en hjemmeside befinder sig på. Internetbrowsere anvender oplysningerne, når en bruger ønsker at besøge en hjemmeside.

Kompromittering af en internetudbyders DNS-server kan omdirigere udbyderens kunder til falske hjemmesider. Det kan ske ved, at cyberkriminelle opnår uautoriseret adgang til serveren, eller ved at cyberkriminelle ændrer eller forfalsker de data, som udbyderens DNS-server modtager og gemmer fra andre DNS-servere på internettet.

Truslen har medført, at et stigende antal hjemmesider benytter DNSSEC, som kan sikre integriteten af DNS-meddelelser. Globalt set er det dog under 2.5 % af hjemmesiderne, som benytter DNSSEC.

Der er også cyberkriminelle, som forsøger at omdirigere internetbrugere til falske hjemmesider ved at hacke hjemmeroutere og konfigurere dem til at benytte DNS-servere, som kontrolleres af de kriminelle. I sommeren 2018 ramte et sådan angreb mere end 100.000 hjemmeroutere i Brasilien. Formålet var at sende brugerne til en falsk hjemmeside, som efterlignede den brasilianske bank Banco de Brazil.

Kundeudstyr som hjemmeroutere, der forbinder brugernes hjemmenetværk med teleinfrastrukturen, anses normalt ikke som en del af udbydernes teleinfrastruktur. Især for privatkunder gælder det dog, at udstyret ofte er leveret og administreret af teleudbyderen.

Ransomware kan true teletjenesterne
Ransomwareangreb er stadig et udbredt fænomen, og det er sandsynligt, at virksomheder i telesektoren i Danmark vil blive forsøgt ramt med ransomware. Der er tegn på, at antallet af simple angreb falder, mens andelen af målrettede og avancerede angreb stiger. Det kan betyde, at risikoen for at blive ramt af ransomware er blevet mindre, men at det til gengæld kræver en bedre beskyttelse at forsvare sig mod angrebene.

Ransomware kan være særdeles skadelig, fordi det i flere tilfælde har lammet hele eller dele af en virksomheds administrative netværk og påvirket virksomhedens evne til at fungere effektivt. Det skete for eksempel for det norske selskab Hydro i marts 2019. I 2017 ramte det omfattende Wannacry ransomwareangreb den spanske teleudbyder Telefónica, som fik lammet computere i deres administrative netværk.

Angrebet mod Telefónica påvirkede ikke teletjenesterne. Det kunne dog være sket, hvis centrale netværksfunktioner som Domain Controller og Active Directory, der styrer computere og medarbejderes adgang til netværket, var blevet ramt. Det kunne have låst alle medarbejdere ude af netværket, og vanskeliggjort adgang, herunder fjernadgang, til teleinfrastrukturen og de værktøjer, som styrer den.

Teletjenesterne kan også blive påvirket, hvis ransomware i det administrative netværk rammer it-systemer eller databaser, som understøtter teletjenesterne, eller hvis ransomware spreder sig til det managementnetværk, som anvendes til at konfigurere og kontrollere teleinfrastrukturen, eller til selve teleinfrastrukturen. Den ransomware, som ramte Hydro, var blandt andet programmeret til at kryptere databasefiler.

Malware, der krypterer data, kan under dække af at være ransomware også benyttes destruktivt. Det oplevede blandt andre Mærsk i 2017, da det såkaldte NotPetya angreb ramte flere virksomheder, som var til stede i Ukraine. Denne hændelse viste også, at et cyberangreb kan sprede sig i en virksomhed på tværs af landegrænser.

Datatyveri, cryptomining malware og BEC-scams rammer også telesektoren

Tyveri af data via internettet er et udbredt problem, som også rammer telesektoren. Cyberkriminelle er på udkig efter data og personoplysninger, som kan videresælge eller misbruges. Stjålet data kan også bruges til at afpresse teleudbyderen til at betale en løsesum, mod at dataene ikke bliver offentliggjort. Modsat ransomware kan datatyveri være vanskeligt at opdage, medmindre de cyberkriminelle selv gør opmærksom på, at de har stjålet dataene, f.eks. i tilfælde af afpresning.

Datatyveri mod telesektoren

I 2017 blev teleselskabet "3" udsat for forsøg på afpresning af cyberkriminelle, som truede med at offentliggøre stjålne kundedata. Selskabet løste dog sagen uden at betale de cyberkriminelle.

I 2017 fik Swisscom i Schweitz stjålet kundedata via en kompromittering af en salgspartners adgang til kundedataene. Det understreger, at cyberkriminalitet kan ske via en underleverandør.

Selvom kryptovalutaerne er faldet i værdi siden toppen i 2018, er de stadig et populært mål for cyberkriminelle, som ønsker at udvinde kryptovaluta uden selv at skulle investere i den nødvendige hardware. Det kan medføre, at en teleudbyders hjemmeside eller enheder i kontornetværket bliver inficeret med cryptomining malware. Hvis malwaren finder vej til udstyr i managementnetværket eller teleinfrastrukturen, kan det potentielt stjæle processorkraft fra kritiske netværkskomponenter. CFCS vurderer dog, at det er mindre sandsynligt, at malware, som udvinder kryptovaluta, vil påvirke teletjenesterne.

BEC-scams er fortsat en trussel, også mod telesektoren. Formålet er at franarre virksomheder og myndigheder penge via e-mails, der indeholder instrukser om at gennemføre pengeoverførsler til aktøren. Metoden er attraktiv, fordi den ikke nødvendigvis kræver avancerede it-færdigheder. Et BEC-scam påvirker ikke teletjenesterne direkte.

Et stigende antal virksomheder i telesektoren benytter kontorværktøjer og e-mail, der leveres som en cloudløsning via internettet. Fordi det er attraktivt for cyberkriminelle at få adgang til e-mail-konti for at misbruge indholdet, sende troværdige phishing-mails eller misbruge adgangen i et BEC-scam, er det meget sandsynligt, at cyberkriminelle vil forsøge at kompromittere sådanne løsninger ved hjælp af phishing-mails med links til falske login-sider, eller ved at gætte det korrekte brugernavn og kodeord. Løsninger uden to-faktor login er særligt sårbare over for den type angreb.

Cyberspionage

Truslen fra cyberspionage mod telesektoren i Danmark er **HØJ**. Det er således sandsynligt, at der er virksomheder i telesektoren, som vil blive mål for forsøg på cyberspionage.
Det generelle niveau for cyberspionage mod Danmark er **MEGET HØJ**. CFCS vurderer, at fremmede stater også har intention og kapacitet til at udføre cyberspionage mod telesektoren i Danmark, men vurderer samtidig, at aktivitetsniveauet ikke er ligeså højt mod telesektoren.

CFCS opdager jævnligt forsøg på cyberspionage mod myndigheder og virksomheder i Danmark. Formålet med cyberspionage er at indhente information, som har strategisk, sikkerhedspolitisk eller økonomisk betydning for aktøren. Truslen retter sig især mod myndigheder og institutioner, der beskæftiger sig med udenrigs- og forsvarspolitik, samt samfundsvigtige og forskningstunge virksomheder.

Telesektoren kan blive mål for cyberspionage, blandt andet fordi den leverer teleinfrastruktur og teletjenester til de ovenfor nævnte organisationer. Der er i udlandet eksempler på at statslige aktører har kompromitteret teleudbydere for at få adgang til opkaldsdata og sms-beskeder, eller for at aflytte kommunikation. De værktøjer og netværksenheder i teleinfrastrukturen, hvor der er adgang til kommunikationen, er særlig interessante for en angriber.

Cyberspionage mod telesektoren kan have til formål at afdække detaljer om den anvendte it- eller teleinfrastruktur. For at kunne kompromittere et netværk er det værdifuldt at vide, hvilken hardware og software ofret anvender. Med den viden er det muligt for en avanceret aktør at anskaffe og analysere identisk udstyr for hidtil ukendte sårbarheder, som kan udnyttes i et cyberangreb.

Teleinfrastruktur og kundeudstyr kan misbruges til cyberspionage mod telesektorens kunder

Nedenfor er der beskrevet eksempler på metoder, som CFCS vurderer, at stater har anvendt mod telesektoren i udlandet, med det formål at spionere mod brugere af teletjenester.

De BGP-hijack og cyberangreb på DNS-servere, som er omtalt i afsnittet om cyberkriminalitet, kan også anvendes til cyberspionage. Ved at omdirigere internettrafik til et netværk, eller en server, hvor angriberen har adgang, kan kommunikationen aflyttes, inden den sendes videre til den oprindelige destination. Der detekteres jævnligt mistænkelige BGP-ændringer, som omdirigerer internettrafik til netværk i lande, som CFCS vurderer har kapacitet til at udføre cyberspionage, og det er muligt, at statslige aktører forsøger at udføre cyberspionage ved hjælp af BGP-hijacks og kompromittering af DNS-servere.

Det kan være attraktivt for en statslig aktør, at få adgang til indholdet i specifikke personers sms-beskeder. CFCS vurderer, at det er meget sandsynligt, at der er stater, som har kapacitet til at kompromittere teleinfrastruktur med malware, som kan opsamle og videresende indholdet i sms-beskeder til og fra udvalgte mobilnumre.

Der er også stater, som forsøger at spionere mod brugere af mobiltelefoni ved at kompromittere det tidligere omtalte SS7-netværk. Svagheder i designet af SS7-netværket kan udnyttes af statslige aktører til at følge og aflytte brugere af mobilnettet i ind- og udland. CFCS vurderer,

at det er meget sandsynligt, at der er fremmede stater, som forsøger at udnytte SS7-netværket til at udføre spionage.

De tidligere omtalte hjemmeroutere, som forbinder teleudbyderens infrastruktur med kundens eget netværk, kan ligeledes udnyttes til at spionere mod en teleudbyders kunder. Som eksempel udsendte de amerikanske myndigheder i maj 2018 et varsel om, at tusindevis af sårbare hjemmeroutere verden over var blevet inficeret med malwaren VPNFilter. Malwaren, som også ramte hjemmeroutere i Danmark, kan blandt andet aflytte kommunikationen, som flyder igennem enheden og truer derved fortroligheden af internetkommunikationen.

Cyberspionage kan ske via en teleudbyders underleverandører
Telesektoren i Danmark anvender underleverandører og outsourcer opgaver, og er derfor udsat for truslen fra cyberangreb på deres forsyningskæde. Leverandører er attraktive mål, fordi de kan give adgang til mange mål på en gang, og måske har en lavere sikkerhed end det endelige mål. I april 2017 udsendte US-CERT varslet TA17-117A om en omfattende kompromittering af leverandører af it-drift i blandt andet Norge, Sverige og Finland. Målet var at spionere mod leverandørernes kunder, som også omfattede teleudbydere. CFCS er ikke bekendt med, at danske teleudbydere har været ramt af dette cyberangreb.

Hvis en aktør kompromitterer hardware eller software fra en underleverandør, kan udbyderen ubevidst selv komme til at installere malware i sit netværk. I marts 2019 blev det afsløret, at ukendte aktører havde kompromitteret servere hos ASUS, som indeholdt softwareopdateringer til deres bærbare computere, og i 2017 blev inficeret CCleaner-software fra firmaet Piriform downloadet mere end 2 millioner gange, inden kompromitteringen blev opdaget. En analyse af denne hændelse viste, at blandt andet telesektoren var mål for angrebet. CCleaner anvendes bredt i Danmark herunder også i dele af telesektoren.

Praktisk taget al software indeholder sårbarheder, som potentielt kan udnyttes af en angriber. Derfor er det vigtigt at sikre sig, at underleverandører løbende vedligeholder deres produkter og udsender sikkerhedsopdateringer, samt at disse opdateringer installeres. Hvis en angriber opnår kendskab til sårbarhederne, inden underleverandøren har udsendt en sikkerhedsopdatering, eller hvis underleverandøren ikke er i stand til at udsende sikkerhedsopdateringer, så vil det pågældende produkt over tid udgøre en stadig større sårbarhed. Som eksempel har det amerikanske Bureau of Industry and Security (BIS) i maj 2019 udsendt en liste over selskaber, som amerikanske virksomheder efter en given dato ikke må eksportere til uden en særlig tilladelse. For telesektoren er det væsentligt, at kinesiske Huawei er nævnt på listen. Hvis forbuddet effektueres, kan det betyde, at Huawei på kort sigt ikke vil være i stand til at levere nye produkter og sikkerhedsopdateringer, som indeholder hardware eller software fra amerikanske selskaber.

Ikke alt cyberspionage er avanceret
Selvom flere stater har kapacitet til at udføre avanceret cyberspionage, sker det ofte ved brug af mindre avancerede metoder og kendte sårbarheder, som også anvendes af cyberkriminelle. Derfor er en kompromittering, uanset hvor ubetydelig den synes, et tegn på, at der er en sårbarhed, som potentielt kan udnyttes mere effektivt af en avanceret modstander.

Vandhulsangreb
I et vandhulsangreb kompromitteres og misbruges en legitim hjemmeside som platform til at kompromittere et eller flere mål, der forventes at besøge siden.

De simple metoder anvendes, fordi de ofte er tilstrækkelige samt slører, at der er tale om cyberspionage og mindsker eksponeringen af avancerede hackerværktøjer og hidtil ukendte sårbarheder. Som eksempel er phishing, social engineering og vandhulsangreb almindeligt anvendte metoder ved både cyberspionage og cyberkriminalitet.

Teknisk personale i it- og sikkerhedsafdelinger er attraktive mål for social engineering, fordi disse personer ofte har administrative rettigheder til netværket samt adgang til netværksværktøjer, som angriberen kan misbruge i et cyberangreb mod organisationen.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod telesektoren i Danmark er **LAV**.

Det betyder, at det er mindre sandsynligt, at telesektoren vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Truslen kan dog stige i forbindelse med en skærpet politisk eller militær konflikt med lande, der besidder denne kapacitet.

En række lande opbygger cyberkapaciteter, som kan bruges i destruktive cyberangreb mod samfundsvigtig infrastruktur som for eksempel teleinfrastruktur.

Det er muligt, at danske teleudbydere kan blive ramt af følgevirkningerne af et destruktivt cyberangreb mod mål udenfor Danmark. Det gælder især, hvis teleudbyderen er til stede i lande såsom Saudi-Arabien og Ukraine, hvor fremmede stater sandsynligvis har stået bag destruktive cyberangreb.

Et målrettet destruktivt cyberangreb mod en teleudbyder vil kræve, at angriberen har detaljeret viden om udbyderens it- og teleinfrastruktur. Denne viden kan opnås ved hjælp af cyberspionage, som derfor kan være et tegn på forberedelse af et eventuelt fremtidigt destruktivt cyberangreb.

Telesektoren understøtter et stigende antal digitale løsninger, som kobler den digitale og fysiske verden sammen. Den kommende 5G mobilteknologi forventes at medvirke til at øge denne sammenkobling yderligere. Udviklingen kan på mellemlang sigt medføre en stigende risiko for, at et alvorligt cyberangreb mod telesektoren kan føre til ødelæggelser i den fysiske verden.

Cyberaktivisme

Truslen fra cyberaktivisme mod telesektoren i Danmark er **LAV**.

Det betyder, at det er mindre sandsynligt, at telesektoren vil blive udsat for forsøg på cyberaktivisme inden for de næste to år.

På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år. Cyberaktivister retter sjældent deres fokus mod danske myndigheder og virksomheder.

Der er eksempler på cyberaktivisme mod telesektoren i udlandet, men CFCS vurderer, at cyberaktivister generelt ikke har fokus på telesektoren i Danmark. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige evner og ressourcer til at udføre cyberangreb. Truslen kan derfor pludseligt stige, hvis virksomheder i telesektoren kommer i cyberaktivisters søgelys.

Formålet med cyberaktivisme er at skabe størst mulig opmærksomhed om en given sag, og formidle et budskab. Aktiviteterne spænder fra opportunistiske angreb til mere organiserede kampagner, hvor der på sociale medier varsles eller opfordres til angreb. Der er også en tendens til, at fysisk aktivisme ledsages af cyberaktivisme.

Cyberaktivisme mod CAT Telecom
I 2015 stod den cyberaktivistiske gruppe Anonymous bag et læk af data samt en række DDoS-angreb mod det thailandske teleselskab CAT Telecom. Angrebene var angiveligt en reaktion på Thailands påståede planer om at overvåge internettrafikken i landet.

DDoS-angreb mod udbydere i Sudan
Teleudbydere og myndigheder i Sudan var i slutningen af 2018 mål for flere DDoS-angreb, som Anonymous påstod at stå bag. Angrebene var bl.a. motiveret af, at Sudans regering har pålagt telesektoren at begrænse borgernes adgang til internettet.

Cyberaktivister har generelt evnen til at ramme hjemmesider med DDoS-angreb eller såkaldte defacements, hvor budskaber indsættes på hackede hjemmesider. En anden metode er at hacke og lække eksempelvis e-mails, der kan stille ofret i et dårligt lys.

Den cyberaktivisme, der er set mod telesektoren i udlandet, har ofte været motiveret af krav om et frit og åbent internet. Cyberaktivismen har primært været rettet imod myndigheder, som har indført overvågning eller begrænsninger i borgernes adgang til internettet, men har også ramt de teleudbydere, som har været forpligtet til at implementere myndighedernes beslutninger.

Ønsket om et frit og åbent internet optræder også i den offentlige debat i Danmark. Det gælder for eksempel når emner som netneutralitet, lovgivning om logning af teletrafik samt indgreb mod brugen af ulovlige streamingtjenester debatteres. Lignende emner har tidligere ført til cyberaktivisme mod politiske mål i Danmark, men har ikke ramt telesektoren. I øjeblikket har den kommende 5G teknologi givet anledning til en debat om, hvorvidt teknologien kan skade miljøet.

Cyberterror
Truslen fra cyberterror mod telesektoren i Danmark er **INGEN**.

Det betyder, at det er usandsynligt, at telesektoren i Danmark, vil blive udsat for forsøg på cyberterror inden for de næste to år.

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

Denne type alvorlige cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

DDoS-angreb

Telesektoren er særlig udsat for truslen fra DDoS-angreb, også kaldet overbelastningsangreb, som derfor uddybes i dette afsnit.

DDoS-angreb er udbredt, fordi de er lette at udføre og anvendes af mange aktører, hvor formålet kan være spænding, afpresning, chikane mod konkurrent eller modstander, sløring af et andet cyberangreb eller afbrydelse af tjenester og services på internettet.

Telesektoren er særlig udsat for DDoS-angreb, fordi alle DDoS-angreb sker via teleinfrastruktur, som derved kan blive overbelastet og medføre forringede eller afbrudte teletjenester. Eksempler på udsatte netværkskomponenter er routere, firewalls og udstyr til Carrier Grade Network Address Translation (CGNAT). Sidstnævnte gør det muligt for udbyderen at dele samme offentlige IP-adresse mellem flere kunder, og kan medføre, at et DDoS-angreb mod en specifik IP-adresse rammer flere kunder.

Konkurrent køber DDoS-angreb mod teleudbyder i Liberia

I januar 2019 blev en britisk statsborger dømt for i 2016 at have udført et kraftigt 500 Gbit/s DDoS-angreb mod Liberias største teleselskab Lonestar MTN. Angrebet var bestilt og betalt af en konkurrerende teleudbyder.

Samme person blev i 2017 dømt i Tyskland for at have skabt det botnet, som blev anvendt i dette og andre angreb. Botnettet bestod af enheder inficeret med Mirai malware. Et forsøg på at indlemme hjemmeroutere i botnettet, afbrød i 2016 internetforbindelsen for 900.000 kun-der hos Deutsche Telecom.

Meget kraftige DDoS-angreb kan påvirke centrale funktioner i udbyderens netværk og medføre, at mange kunder bliver berørt af angrebet. I 2017 og 2018 oplevede kunder hos Ålcom, der er teleudbyder i det finske selvstyre Åland, således afbrudte eller forringede teletjenester, som skyldtes en række DDoS-angreb mod andre af selskabets kunder.

Ligesom andre hjemmesider kan også teleudbydernes hjemmeside blive udsat for DDoS-angreb. Udover at spærre for adgangen til hjemmesiden kan angrebet afbryde eventuelle tjenester, som leveres via

hjemmesiden eller det netværk, som den angrebne web-server befinder sig i.

Modsat hovedparten af teleinfrastrukturen har udbydernes kundevendte DNS-servere offentlige IP-adresser og kan derfor blive mål for DDoS-angreb. Et succesfuldt angreb kan betyde, at udbyderens kunder oplever problemer med at tilgå hjemmesider eller tjenester via internettet.

Antal og størrelse af registrerede DDoS-angreb varierer over tid, men ligger generelt på et højt niveau. It-sikkerhedsfirmaer registrerer hvert år flere millioner angreb verden over.

Aktørerne udvikler hele tiden nye angrebsmetoder. I februar 2018 blev der registreret et rekordstort DDoS-angreb på 1.7 Tbit/s mod et unavngivet amerikansk firma. Dette og andre angreb blev som noget nyt forstærket ved hjælp af åbne Memcached servere, der typisk anvendes til at forbedre ydelsen for dynamiske hjemmesider. It-sikkerhedsfirmaer har også observeret, at CoAP-protokollen, som er specielt udviklet til kommunikation mellem internetforbundne fysiske enheder (IoT), nu bliver udnyttet til at forstærke DDoS-angreb.

Sårbarheder i det stigende antal IoT-enheder udnyttes også af cyberaktører til at skabe store botnet, som kan generere kraftige DDoS-angreb.

Åbne servere
Er enheder på internettet, som accepterer og besvarer enhver forespørgsel fra internettet. En angriber kan forstærke et DDoS-angreb ved at dirigere svar fra åbne servere til den IP-adresse, som DDoS-angrebet er rettet imod.

Botnet
Betegner et netværk af internetfor-bundne enheder, som er inficeret med malware, der gør det muligt at fjernstyre enhederne fra en såkaldt kommando og kontrolserver (C2). Et botnet kan f.eks. indgå i et koordi-neret DDoS-angreb.

Mirai-botnettet er et eksempel på et botnet, som i 2016 blev berygtet for en række meget kraftige DDoS-angreb. Siden er der opstået varianter af dette botnet, som stadig er aktive.

Ved at registrere IP-adresser, som kommunikerer med kendte C2-servere, og scanne internettet for åbne servere, kan sikkerhedsfirmaer vise, at der i de danske teleudbyderes kundenetværk er hundredevis af enheder, som indgår i botnet, og endnu flere åbne servere, som kan udnyttes til at generere kraftige DDoS-angreb.

Trusselsniveauerne

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 sandsynligheder i analyser