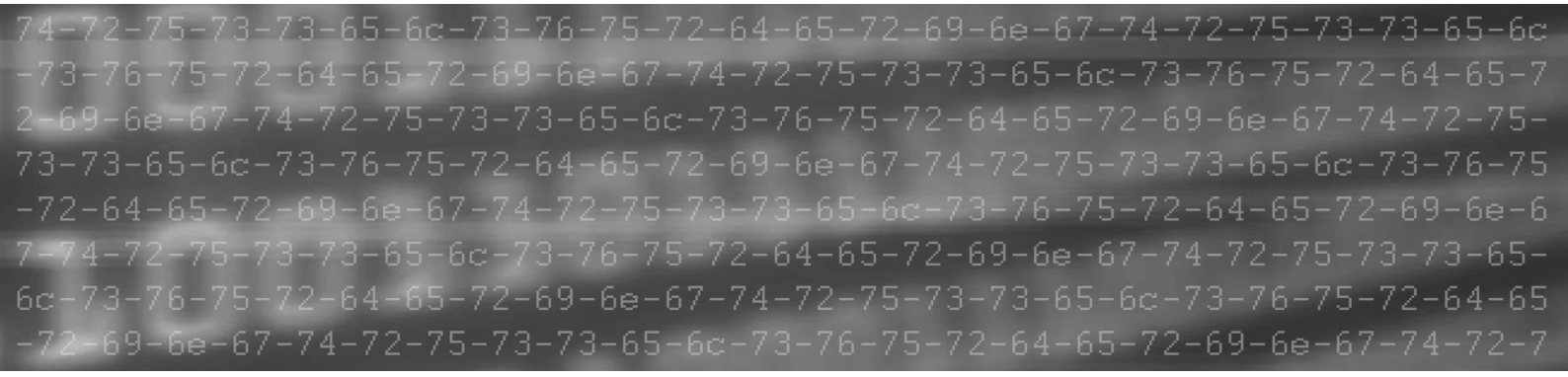
CENTER FOR
CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod telesektoren i Danmark



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Februar 2017

CENTER FOR CYBERSIKKERHED

Februar 2017

Trusselsvurdering: Cybertruslen mod telesektoren i Danmark

Denne trusselsvurdering redegør for de cybertrusler, som er rettet imod telesektoren i Danmark. Telesektoren i Danmark er af kritisk betydning for samfundets funktion, stabilitet og sikkerhed.

Hovedvurdering

- Overbelastningsangreb, som kan benyttes af alle typer cyberaktører, udgør den alvorligste trussel mod tilgængeligheden af teletjenesterne, og er samtidigt en trussel mod teleudbydernes forretning. CFCS vurderer, at truslen er **MEGET HØJ**.
- Telesektoren er, ligesom andre danske virksomheder og myndigheder, udsat for en omfattende trussel fra cyberkriminelle, og CFCS vurderer, at truslen fra cyberkriminalitet mod teleudbydernes forretning er **MEGET HØJ**.
- Cyberspionage mod telesektoren har til formål at opnå adgang til følsom information i telesektoren og dennes kunder samt at afdække sårbar infrastruktur. CFCS vurderer, at truslen fra cyberspionage mod telesektoren er **HØJ**.
- Der er ikke konstateret mange eksempler på cyberaktivisme i Danmark, og CFCS vurderer, at truslen mod telesektoren er **MIDDEL**. Hvis enkeltsager påkalder sig aktivisternes opmærksomhed, kan trusselsniveauet dog stige uden varsel.
- Selvom cyberkriminalitet udgør en alvorlig trussel mod teleudbydernes forretning, så vurderer CFCS, at truslen mod teletjenesterne fra cyberkriminalitet er **LAV**.
- CFCS vurderer, at truslen fra destruktive cyberangreb fra fremmede stater, herunder mod telesektoren, på nuværende tidspunkt er **LAV**. Truslen vil dog kunne stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.
- CFCS vurderer, at ingen terrorgrupper på nuværende tidspunkt har kapacitet til at udføre decideredе terrorhandlinger gennem internettet mod telesektoren, og at truslen fra cyberterror derfor er **LAV**.

Indledning

Denne trusselsvurdering beskriver cybertruslerne mod telesektoren i Danmark. Vurderingen er udarbejdet af Trusselsvurderingsenheden ved Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS). Trusselsvurderingen behandler cybertrusler mod teletjenesterne og teleudbydernes forretning. Formålet med trusselsvurderingen er at informere virksomheder i telesektoren om cybertruslen, således at sektoren bliver bedre i stand til at imødegå denne.

Vurderingen behandler først cybertrusler, der kan påvirke tilgængeligheden, fortroligheden og integriteten af teletjenesterne. Disse trusler er de alvorligste set fra et samfundsperspektiv, da der er tale om trusler mod samfundsvigtig infrastruktur. Heri indgår såkaldte DDoS-angreb og cyberspionage som de alvorligste trusler mod teletjenesterne.

Derefter behandler vurderingen cybertrusler, der hovedsageligt er rettet mod teleudbydernes forretning. Heri indgår cyberkriminalitet og cyberspionage som de alvorligste trusler mod forretningen.

Telesektoren i Danmark defineres som de erhvervsmæssige teleudbydere, der offentligt udbyder de tjenester og den teleinfrastruktur, som gør det muligt for myndigheder, virksomheder og borgere at kommunikere elektronisk. De typiske virksomheder er udbydere af fastnet, mobiltelefoni og satellittelefoni samt Internet service Providers (ISP), som udbyder internetforbindelser, og selskaber som udbyder erhvervsmæssige netværksløsninger.

Før digitaliseringen af teleinfrastrukturen i Danmark, som begyndte i 80'erne, blev telenettet primært brugt til taletrafik. Selvom denne funktion var vigtig for samfundet, så ville langt de fleste myndigheder og virksomheder dengang kunne fungere nogenlunde normalt, selvom telenettet blev afbrudt kortvarigt. Sådan er det ikke i dag. Den Nationale strategi for cyber- og informationssikkerhed, som blev publiceret i 2014, sætter fokus på blandt andet øget cybersikkerhed i telesektoren, og slår fast, at telesektoren er af væsentlig betydning for samfundets funktion, stabilitet og sikkerhed. Telesektoren har udviklet sig fra en leverandør af taletjenester, til en leverandør af den digitale platform som andre samfundsvigtige sektorers tjenester er afhængige af.

Når man skal identificere cybertruslerne mod teletjenesterne i Danmark, er det vigtigt at være bekendt med disse tjenester samt de kerneområder, som understøtter teletjenesterne:

- **Teletjeneste**
  En teletjeneste er en elektronisk kommunikationstjeneste, som overfører lyd, billede, tekst eller kombinationer heraf, mellem såkaldte nettermineringspunkter. Et nettermineringspunkt kan være en router, tv-modtagerboks, computer, mobiltelefon eller lignende. Eksempler på teletjenester er mobiltelefoni, fastnettelefoni, internetadgang, kystradio samt broadcasting og anden transmission af radio og tv udsendelser.

- **Teleinfrastrukturen**
  Teleinfrastrukturen udgøres af det udstyr og de transmissionsforbindelser, som danner grundlag for de teletjenester, som udbyderen tilbyder. En segmenteret teleinfrastruktur med flere netværk gør infrastrukturen mere robust overfor cyberangreb. En medvirkende faktor til denne

segmentering er eksistensen af flere teleudbydere med egen teleinfrastruktur.

- **Teleudbyderne**
  Teleudbydere ejer og driver teleinfrastrukturen. I praksis betyder det, at tilgængeligheden af teletjenesterne er afhængig af, at disse privatejede selskaber eksisterer, og har de nødvendige ressourcer til at etablere og drive teleinfrastrukturen. Teleudbyderne er i stor udstrækning afhængige af de systemer, værktøjer og data, som ligger på deres administrative netværk. Da dette netværk, modsat mange af kontrolsystemerne i selve teleinfrastrukturen, ofte er direkte forbundet til internettet, er det samtidig et mål for cyberangreb.

- **Underleverandørerne**
  Udbyderne i telesektoren er ofte afhængige af underleverandører for at kunne drive deres forretning og opretholde teletjenesterne. Opgaverne strækker sig fra etablering og drift af teleinfrastrukturen eller administrative netværk, til serviceopgaver som rengøring og vedligehold af bygninger og installationer. Underleverandører kan have adgang til følsom information hos teleudbyderen, enten via dataforbindelser mellem teleudbyderen og underleverandøren eller ved fysisk adgang til udbyderens dokumentation, administrative netværk eller teleinfrastruktur. Derfor kan cyberangreb mod en teleudbyder også ske via udbyderens underleverandører.

- **Driftscentre og field service**
  For at modvirke almindelige driftsforstyrrelser og tekniske nedbrud, overvåger, justerer og fejlretter driftscentre teleinfrastrukturen døgnet rundt, og såkaldte field service teknikere udfører dagligt kontrol og reparationer på infrastrukturen. Driftscentrenes kompetence og rutine i dagligt at opdage og rette fejl medvirker til at afbøde effekten af et destruktivt eller forstyrrende cyberangreb.

- **Elforsyningen**
  Trusler mod energisektoren behandles ikke i denne vurdering, men det skal nævnes, at uden en stabil elforsyning, vil teleinfrastrukturen ikke kunne fungere. Netværkskomponenter og driftssystemer vil slukke, eller manglende køling vil få udstyr til at brænde sammen. Der er ofte etableret nødstrøm eller batteribackup på særligt sårbare dele af infrastrukturen, men især batteribackup vil kun kunne afbøde virkningen af kortvarige strømafbrydelser.

Cybertrusler som kan påvirke teletjenesterne

Generelt er teleudbyderne og den samfundsvigtige teleinfrastruktur forholdsvis robust overfor cyberangreb. De afbrydelser af teletjenesterne som forekommer skyldes oftest fejl på udstyr i teleinfrastrukturen, overgravede kabler eller andre hændelser, der ikke skyldes cybertruslen.

Telesektoren er imidlertid udsat for en række alvorlige cybertrusler, som truer teleinfrastrukturen, teleudbyderne og deres kunder. Kommer cybertruslerne mod teletjenesterne til udtryk, kan det påvirke tilgængeligheden, fortroligheden og integriteten af teletjenesterne. Truslerne mod tilgængeligheden er den mest alvorlige og synlige, mens trusler mod fortroligheden eller integriteten kan betyde, at en teletjeneste ikke kan eller bør anvendes i tilfælde, hvor fortrolighed og integritet er vigtig for brugeren.

Truslen fra DDoS-angreb

Den alvorligste cybertrussel mod tilgængeligheden af teletjenesterne er i dag de såkaldte DDoS-angreb, også kaldet overbelastningsangreb. Disse angreb forekommer hyppigt og kan ramme alle myndigheder, virksomheder og borgere. DDoS-angreb udføres via internettet, samt i mindre grad via mobilnettene, imod teleudbyderne, deres kunder og imod teleinfrastrukturen.

Telesektoren er ganske robust overfor DDoS-angreb, og det er især telesektorens kunder, som påvirkes af angrebene. Hyppigheden af angrebene kombineret med det forhold, at DDoS-angreb udføres via teleinfrastrukturen og derfor kan påvirke tilgængeligheden af teletjenesterne gør imidlertid, at CFCS vurderer, at truslen fra DDoS-angreb udgør den alvorligste trussel mod tilgængeligheden af teletjenesterne, og at denne trussel er **MEGET HØJ.**

DDoS
Distributed Denial of Service (DDoS), betegner cyberangreb, hvor angriberen udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, således at hjemmesiden eller netværket ikke er tilgængeligt, mens angrebet står på.

DDoS-angreb benyttes af alle typer trusselsaktører, lige fra brugere af online spil, som ønsker at genere sine modspillere, over cyberkriminelle, som afprøver en virksomheds sikkerhedsniveau, kræver penge for at stoppe et angreb, eller som benytter DDoS-angreb til at sløre et mere alvorligt cyberangreb. Kontrollerede DDoS-angreb anvendes også legitimt af f.eks. sikkerhedsfirmaer til at teste en virksomheds modstandsdygtighed overfor overbelastningsangreb.

Kriminelle aktører brugte sandsynligvis et DDoS-angreb til at aflede opmærksomheden, da hackere i 2015 stjal følsomme kundedata og kreditkortoplysninger fra den engelske teleudbyder TalkTalk.

Statslige modstandere kan også benytte DDoS-angreb mod telesektoren og dennes kunder, i et forsøg på at påvirke tilgængeligheden af teletjenesterne. CFCS har ikke kendskab til DDoS-angreb mod telesektoren i Danmark, som kan tilskrives fremmede stater.

En årsag til den høje forekomst af DDoS-angreb er, at de er relativt lette at udføre. Hackerforums tilbyder værktøjer, råd og vejledning til DDoS-angreb, ligesom der findes gratis programmer til computere, smartphones og tablets, som kan generere mindre DDoS-angreb. Det er også muligt på internettet, gratis eller mod betaling, at bestille mindre DDoS-angreb. Disse mindre DDoS-angreb kan være generende for offeret, men udgør kun en minimal udfordring for teleinfrastrukturen.

En mere alvorlig trussel hidrører de ressourcestærke cyberaktører, som råder over botnet, der kan generere meget kraftige eller avancerede DDoS-angreb mod teleinfrastrukturen, teleudbyderne eller deres kunder. Disse angreb kan udgøre en alvorlig trussel mod teleinfrastrukturen.

Der har både i Danmark og i udlandet været DDoS-angreb rettet imod teleinfrastrukturen, som har haft alvorlige konsekvenser for tilgængeligheden af udbyderens teletjenester.

Selvom cybertruslen fra DDoS-angreb er meget høj, så påvirker størstedelen af DDoS-angrebene ikke teletjenesterne mærkbart. Det skyldes, at teleinfrastrukturen har stor kapacitet, som gør den i stand til at håndtere datamængden i de fleste DDoS-angreb uden at blive overbelastet. Selv kraftigere angreb vil ofte kun påvirke kunderne på en begrænset del af infrastrukturen. Det skyldes, at de store internetudbyderes såkaldte backbone netværk er segmenterede, så et effektivt DDoS-angreb ofte kun påvirker en afgrænset del af teleinfrastrukturen. Desuden har flere udbydere systemer og procedurer til at inddæmme og håndtere kraftige DDoS-angreb mod dem selv eller deres kunder, uden at dette får mærkbare konsekvenser for øvrige kunder. Der går dog typisk noget tid, inden et DDoS-angreb bliver opdaget af udbyderen, og inden eventuelle modforholdsregler bliver aktiveret. I den periode kan konsekvenserne af et kraftigt DDoS-angreb være alvorlige for teletjenesterne.

Data fra sikkerhedsfirmaer, som leverer beskyttelse mod DDoS-angreb, viser at størrelsen (båndbredden) på de kraftigste angreb stiger. En medvirkende årsag er, at flere og flere dagligdags produkter forbindes til internettet, en udvikling som kaldes Internet of Things (IoT). Når mange enheder forbindes til internettet, vil der uværligt være nogle af disse enheder, som indeholder sårbarheder, der kan udnyttes i DDoS-angreb. Risikoen er særlig stor, hvis enheden er fremstillet af et firma, som ikke prioriterer at tænke cybersikkerhed ind i internetforbundne enheder.

DDoS-angreb mod virksomheder som benyttede TDC's DDoS beskyttelse i 2015

- 80% var på 100 Mbit/s eller mere
- 57% var på 1 Gbit/s eller mere
- Kraftigste angreb var 39 Gbit/s

Kilde: TDC DDoS trusselsrapport for 2015

Små og mellemstore virksomheder har ofte internetforbindelser med en båndbredde under 50 Mbit/s, og større virksomheder ofte under 1 Gbit/s.

Målrettede DDoS-angreb kan være effektive, selvom angrebet ikke overstiger båndbredden på virksomhedens internetforbindelse.

Nylige eksempler fra udlandet på meget kraftige DDoS-angreb, som oversteg 600 Gbit/s, var angrebene mod nyhedsmediet KrebsOnSecurity i september og mod DNS-udbyderen Dyn i oktober. Det sidstnævnte angreb betød, at flere europæiske og amerikanske internetsites blev utilgængelige. Begge angreb udnyttede angiveligt usikre IoT enheder, som anvendte kendte standard passwords.

Det er i dag muligt at udføre DDoS-angreb fra smartphones, tablets og computere forbundet til mobilnettet. Mobilnettene har i dag så meget båndbredde, og mobile enheder så meget computerkraft, at de kan indgå i botnet og udnyttes til at udføre DDoS-angreb.

Teleudbyderne er også udsat for DDoS-angreb. Disse DDoS-angreb går efter teleudbydernes administrative netværk, og herunder deres webservere. Sådanne DDoS-angreb truer ikke umiddelbart teletjenesterne, med mindre der er tale om et meget kraftigt angreb som beskrevet ovenfor. Et DDoS-angreb kan dog betyde, at en udbyders hjemmeside ikke er tilgængelig, hvilket kan skade

forretningsdelen, når f.eks. salgs-, support- eller selvbetjeningsløsninger ikke er tilgængelige for kunderne.

I det tilfælde, at en teleudbyder flytter kritiske dele af forretningen ud til en underleverandør, f.eks. en leverandør af cloud computing, så vil teleudbyderen kunne påvirkes af DDoS-angreb mod denne underleverandør.

Truslen mod teletjenesterne fra cyberspionage

Cyberspionage mod offentlige myndigheder og private virksomheder udgør den alvorligste cybertrussel mod Danmark. Danske myndigheder og virksomheder er løbende udsat for forsøg på cyberspionage, der primært udføres af statslige aktører.

Cyberspionage udgør også en trussel mod teleudbyderne samt mod fortroligheden af teletjenesterne og truer potentielt også tilgængeligheden af teletjenesterne. Cyberspionage mod teleudbydere kan anvendes til at kortlægge udbyderens teleinfrastruktur, eller opnå adgang til oplysninger om udbyderens kunder, med det formål at spionere mod myndigheder, andre virksomheder og mod øvrige kunder hos udbyderen.

Cyberspionage mod teleinfrastrukturen kan også ske ved, at aktøren udnytter svagheder i leverandørkæden til at implementere eller opnå kendskab til sårbarheder i udstyr, som indgår i teleinfrastrukturen. Dette forhold betegnes ofte som Supply Chain Threats.

CFCS vurderer, at det er meget sandsynligt, at statslige aktører i udlandet har hensigt og kapacitet til at udføre cyberspionage mod telesektoren. CFCS ser dog ikke samme høje aktivitetsniveau af cyberspionage fra statslige aktører mod telesektoren i Danmark som mod andre sektorer i Danmark.

Mens truslen fra cyberspionage mod danske myndigheder og virksomheder generelt er **MEGET HØJ**, vurderer CFCS, at truslen fra cyberspionage mod telesektoren er **HØJ.**

Cyberspionage mod telesektoren kan også anvendes til at afdække sårbarheder i teleinfrastrukturen, som kan udnyttes til eventuelt fremtidige cyberangreb. Her kunne der f.eks. være tale om:

- Kortlægning af kritiske netværkskomponenter og support- og driftssystemer i udbyderens teleinfrastruktur, med det formål at forberede et eventuelt fremtidigt destruktivt cyberangreb.
- Adgang til teknisk driftsdokumentation for udbyderens netværkskomponenter, som også kan bruges til forberedelse af destruktive cyberangreb eller kompromittering af fortroligheden i teletjenesterne.
- Adgang til kritiske konfigurationsdata og kodeord til centrale servere og kontrolsystemer, som kan gøre det muligt at udføre yderligere cyberangreb mod udbyderens teleinfrastruktur.
- Identifikation af udbyderens nøglemedarbejdere, med adgang til følsomme data eller kritiske systemer. Denne viden kan bruges til at udføre målrettede cyberangreb mod medarbejderen for at få adgang til disse systemer og data.
- Kortlægning af systemer, som kan kompromitteres og misbruges som infrastruktur til yderligere cyberangreb mod mål i Danmark og udlandet.

Udover brugen af cyberspionage mod de enkelte virksomheder i telesektoren er det også muligt at udføre cyberspionage via det såkaldte SS7-netværk, som forbinder alle mobilnet. Svagheder i SS7-designet kan især udnyttes af statslige aktører til at følge eller aflytte personer, også selvom disse personer befinder sig i andre lande. Det er ligeledes potentielt muligt at forhindre opkald til eller fra bestemte personer, eller helt at afbryde visse mobiltjenester.

Udnyttelse af svaghederne i SS7-netværket kræver, at aktøren har adgang til nettet. Denne adgang udbydes af private virksomheder på kommercielle vilkår, eller kan opnås via samarbejde med en eksisterende udbyder. CFCS vurderer, at der er fremmede stater, som har denne adgang, og som søger at udnytte SS7-netværket til at udføre spionage.

Det er muligt for den enkelte teleudbyder at modvirke nogle af svaghederne i SS7-designet, for derved at gøre det sværere at spionere mod deres kunder eller påvirke teletjenesterne via SS7-netværket. CFCS udgav i december 2015, i samarbejde med de øvrige nordiske telemyndigheder, vejledningen "*Common Nordic Recommendations on SS7 Security Issues*". Dokumentet indeholder en række anbefalinger til imødegåelse af svaghederne i SS7-designet. Vejledningen er alene tilgængelig for teleudbyderne i de nordiske lande.

Truslen mod teletjenesterne fra cyberkriminalitet

Cyberkriminalitet dækker i denne vurdering handlinger, hvor gerningsmanden bruger it til at begå kriminalitet, som er motiveret af ønsket om økonomisk vinding. Som udgangspunkt udgør cyberkriminalitet en begrænset trussel mod tilgængeligheden af teletjenesterne.

CFCS vurderer, at truslen mod teletjenesterne fra cyberkriminalitet er **LAV**.

Den lave trussel skyldes blandt andet, at cyberkriminaliteten typisk er rettet mod virksomhedens forretning og ikke teleinfrastrukturen, samt at et målrettet cyberangreb mod centrale systemer i teleinfrastrukturen kræver særlig teknisk viden og kapacitet, som CFCS vurderer, at kun få cyberkriminelle besidder. En yderligere årsag er, at kontrolsystemerne i teleinfrastrukturen ofte er logisk adskilt fra teleudbyderens administrative netværk, der typisk er mål for de cyberkriminelle.

Teleudbyderens tekniske personale og underleverandører har dog ofte fjernadgang til teleinfrastrukturen via det administrative netværk. Hvis denne adgang ikke er ordentligt beskyttet, er der en mulighed for, at cyberkriminelle opnår adgang til teleinfrastrukturen, hvilket i sidste ende kan true teletjenesterne.

Cyberkriminelles brug af DDoS-angreb samt forsøg på kompromittering af kundeudstyr som kabelmodems og DSL-routere kan betyde, at kunder kompromitteres eller mister adgangen til internet, TV eller telefoni.

Meget arbejde med planlægning, udbygning og drift af teleinfrastrukturen foregår i it-systemer som ligger på teleudbydernes administrative netværk. Et cyberangreb, der anvender f.eks. ransomware mod en udbyders administrative netværk, kan derfor betyde, at der er driftsopgaver, som udbyderen midlertidigt ikke vil være i stand til at udføre. Disse it-systemer er dog typisk min-

dre kritiske for tilgængeligheden af teletjenesterne og benyttes eksempelvis til planlægning og test af ændringer i teleinfrastrukturen, trafikanalyse, frekvens- og ip-planlægning eller fakturering. CFCS vurderer derfor, at selvom angrebet kan forsinke projekter og skade udbyderens omdømme og økonomi, så vil et sådan angreb kun udgøre en begrænset trussel mod teletjenesterne.

Nogle cyberkriminelle aktører udnytter, at afsenderidentiteten ved opkald via internettet (VoIP) og SMS'er kan forfalskes og misbruges i spear-phishing angreb og forsøg på bedrageri. Dette misbrug udgør en trussel mod integriteten men ikke tilgængeligheden af disse teletjenester.

Truslen fra destruktive cyberangreb

En række lande opbygger cyberkapaciteter, der kan bruges mod samfundsvigtig infrastruktur såsom teleinfrastrukturen. Kapaciteterne vil kunne anvendes i forbindelse med militære operationer, men giver også staterne mulighed for destruktive angreb uden brug af traditionelle våben.

CFCS vurderer, at truslen fra destruktive cyberangreb fra fremmede stater, herunder mod telesektoren, på nuværende tidspunkt er **LAV**. Truslen vil dog kunne stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.

Et destruktivt cyberangreb kan blandt andet involvere sletning eller ændring af data, konfiguration eller software på kritiske systemer og netværkskomponenter. CFCS vurderer, at et enkeltstående destruktivt cyberangreb mod teleinfrastrukturen i de fleste tilfælde kun vil have kortvarig effekt, da konsekvenserne af angrebet hurtigt vil blive opdaget af udbyderens driftscenter, som ofte vil være i stand til at begrænse skaderne og genetablere teletjenesterne indenfor nogle timer. Gentagne angreb kan dog give alvorlige forstyrrelser over længere tid.

Destruktive cyberangreb mod teleinfrastrukturen kræver, at angriberen har skaffet sig adgang til eller kompromitteret teleinfrastrukturen. Metoderne til denne kompromittering kan være de samme som dem, der benyttes ved cyberspionage. Det betyder, at en angriber, som har kompromitteret et system med det formål at udføre cyberspionage, ofte vil være i stand til at udnytte den samme adgang til at udføre et destruktivt angreb.

Afbrydelsen af tv-signalet til YouSee's kunder nytårsaften 2016 er muligvis et eksempel på et destruktivt cyberangreb. Sagen er ved udgivelse af denne vurdering stadig genstand for politimæssig efterforskning, hvorfor det ikke er endeligt afklaret, om der reelt er tale om et destruktivt cyberangreb, og hvem, der i så fald udførte angrebet.

En fremmed stat vil sandsynligvis vægte udbyttet af et destruktivt cyberangreb mod teleinfrastrukturen op mod muligheden for at udføre aflytning af tale- og datatrafikken via samme teleinfrastruktur. Afbrydelse af dele af teleinfrastrukturen kan dog tænkes brugt til at tvinge kommunikation over på alternative kommunikationssystemer, som kan aflyttes af angriberen. For eksempel vil afbrydelse af mobilnettets 3G-signaler i mange tilfælde tvinge kommunikationen over på det svagere krypterede 2G-signal.

Truslen fra cyberterror

CFCS vurderer, at ingen terrorgrupper på nuværende tidspunkt har kapacitet til at udføre deciderede terrorhandlinger gennem internettet. Cyberterror er ideologisk motiveret, og formålet

er, som for øvrige terrorhandlinger, at skabe opmærksomhed på terrorgruppens sag gennem voldsomme handlinger, som ofte medfører fysisk destruktion eller drab, der fremkalder frygt i befolkningen.

CFCS vurderer, at truslen for cyberterror mod telesektoren er **LAV**.

Truslen vil dog stige, hvis det lykkes terrorgrupper at tiltrække medlemmer med tilstrækkelige tekniske færdigheder, eller hvis etablerede cyberaktivistiske grupper eller medarbejdere med adgang til kritiske systemer gennemgår en radikalisering.

CFCS vurderer, at teleinfrastrukturen har en robusthed som betyder, at et cyberterrorangreb sandsynligvis kun vil have begrænset effekt på teletjenesterne og derfor ikke direkte vil opfylde terroristernes ønske om at skræmme befolkningen. Et fysisk terrorangreb kombineret med et cyberangreb mod tilgængeligheden af teletjenesterne vil dog kunne forstærke frygten i befolkningen og dermed forøge virkningen af det fysiske angreb.

Cybertrusler mod teleudbydernes forretning

Virksomhederne i telesektoren er udsat for de samme cybertrusler som virksomheder i andre sektorer. I modsætning til de cybertrusler, som er rettet mod teletjenesterne, så vil cybertrusler rettet mod en teleudbyders forretningsdel sjældent, eller kun indirekte, påvirke tilgængeligheden af teletjenesterne.

Truslen fra cyberkriminalitet mod teleudbydernes forretning

Cyberkriminelle skelner som udgangspunkt ikke mellem de forskellige typer virksomheder, og virksomheder i telesektoren er derfor udsat for den samme trussel fra cyberkriminelle, som andre danske virksomheder og myndigheder.

CFCS vurderer, at truslen fra cyberkriminalitet mod teleudbydernes forretning er **MEGET HØJ**.

Cyberkriminalitet er en stigende udfordring for hele det danske samfund. Især brugen af såkaldt ransomware er i de seneste år vokset i omfang og kompleksitet. Formålet med ransomware er at afkræve løsepenge, efter angriberen har gjort ofrets data utilgængelige ved at kryptere dem. Andre metoder går ud på at stjæle virksomheders intellektuelle ejendom og data, som indeholder personfølsomme oplysninger eller oplysninger om betalings- eller kreditkort. Teleudbydere ligger typisk inde med sådanne data om deres kunder.

Et nyligt eksempel fra Danmark drejer sig om teleudbyderen 3, som i februar 2017 blev udsat for afpresning fra kriminelle, som var kommet i besiddelse af kundeoplysninger fra 3's kundedatabase. Sagen er ved udgivelse af denne vurdering stadig genstand for politimæssig efterforskning.

En anden teleudbyder, som har mærket effekterne af cyberkriminalitet, er den engelske teleudbyder TalkTalk, hvorfra cyberkriminelle i 2015 stjal ubeskyttede kundedata. Ifølge selskabet kostede hændelsen virksomheden mere end 400 millioner kroner og et tab af cirka 100.000 kunder.

Truslen fra cyberspionage mod teleudbydernes forretning

Cyberspionage mod teleudbyderne fokuserer på at opnå adgang til fortrolig information om teknologier, processer, strategier eller kommercielle oplysninger med det formål at fremme en

bestemt virksomhed eller et lands industri og økonomi generelt. Cyberspionage mod virksomhederne i telesektoren truer primært virksomhedernes økonomi og forretning.

CFCS har kendskab til statslige aktører, som aktivt udfører cyberspionage mod virksomheder i Danmark.

CFCS vurderer, at truslen fra cyberspionage mod virksomheder i telesektoren i Danmark er **HØJ**. Nedenstående er eksempler på information, som kan være attraktivt at opnå adgang til via cyberspionage:

- Fortroligt materiale fra telesektorens højteknologiske leverandører, såsom design- og driftsdokumentation og software, som kan være af stor interesse for uvedkommende, som ønsker adgang til teknologien.
- En teleudbyders egenudviklede it-værktøjer og systemer, som ofte ikke er beskyttet af patenter eller lignende.
- Sensitiv information om en teleudbyders interne forhold, arbejdsmetoder og tekniske løsninger. Forretningsstrategier, interne mødereferater, prisaftaler med kunder og underleverandører, konkurrenters tilbudsmateriale og lignende af konkurrencemæssig betydning.

Truslen fra cyberaktivisme

Cyberaktivisme har til formål at formidle et holdningsmæssigt eller politisk budskab gennem cyberangreb. Cyberaktivisme er typisk fokuseret på enkeltsager og personer, organisationer eller virksomheder, som aktivisterne opfatter som modstandere af deres sag.

CFCS vurderer, at truslen fra cyberaktivisme mod teletjenesterne samt virksomhederne i telesektoren er **MIDDEL**.

Cyberaktivisternes typiske metoder er såkaldt defacement, hvor indholdet på en hjemmeside ændres, så den understøtter deres budskab, læk af følsomme kundedata eller interne dokumenter samt DDoS-angreb mod en myndigheds eller virksomheds hjemmeside. Med mindre der er tale om et usædvanligt kraftigt DDoS-angreb, så truer cyberaktivisternes metoder ikke umiddelbart teletjenesterne.

Der er ikke konstateret mange eksempler på cyberaktivisme i Danmark, men enkeltsager kan pludseligt påkalde sig cyberaktivisters opmærksomhed, hvorved truslen kan stige med ingen eller kort varsel. Nogle cyberaktivister er motiverede af en ideologi om et frit og åbent internet. Eksempler på emner med en relation til telesektoren, der lige nu optræder i den offentlige debat, og som kan påkalde sig cyberaktivisters interesse, er netneutralitet, sessionslogning samt registreringen af mobilkundernes færden.

Tendenser i telesektoren med betydning for udviklingen af cybertruslen

Teknologien som understøtter telesektoren er i en fortsat udvikling. Nye tjenester og teknologier kan mindske driftsomkostninger eller øge indtjening eller markedsandele, og der kan være en forretningsmæssig fordel ved at være først på markedet med ny teknologi eller nye tjenester.

Det er en vigtig opgave for leverandører og teleudbydere at implementere og drive disse nye tjenester og teknologier på en måde, som tager højde for de nye trusler og sårbarheder, som følger med ny teknologi.

Eksempler på nye teknologier og tjenester, som kan påvirke truslens karakter:

- Network Function Virtualization (NFV), er software emulering af udstyr, som traditionelt er realiseret i hardware. NFV kan gøre det hurtigere at implementere nye teletjenester og mere effektivt at drive teleinfrastrukturen. I modsætning til den specialiserede hardware og software, som er udbredt i teleinfrastrukturen i dag, vil NFV være baseret på standardservere og software fra globale leverandører. Et cyberangreb mod disse servere vil kræve mindre specialviden end et cyberangreb mod de nuværende specialiserede netværkskomponenter.
- Software Defined Networks (SDN) vil kunne effektivisere driften af store netværk som teleinfrastrukturen. Netværksændringer vil kunne foretages hurtigere end i dag. For eksempel kan ende-punkter forbindes ved peg og klik, da den centrale software vil sørge for, at nødvendige ændringer på de mellemliggende netværkskomponenter foretages automatisk. Overgangen fra decentral til central styring af netværket gør imidlertid nettet ekstra sårbart ved en uautoriseret adgang til den centrale styring. Endvidere kan eventuelle sårbarheder i standardinterfacet mellem den centrale styring og de enkelte netværkskomponenter betyde, at alle SDN-enheder, uanset fabrikat, kan kompromitteres ved brug af samme metode.
- Cloud Computing gør det muligt at flytte data, teleinfrastruktur eller teletjenester ud i centrale datacentre, ved en dansk eller udenlandsk underleverandør. Hvis en teleudbyder gør brug af denne mulighed, kan det være en udfordring for udbyderen at opretholde kontrollen med de dele af udbyderens forretning, som flyttes ud i "skyen". Udflytningen kan også betyde, at data og infrastruktur som tidligere lå beskyttet på udbyderens interne netværk, fremover bliver eksponeret for de samme cybertrusler og sårbarheder, som leverandøren af cloud-servicen er udsat for.
- Narrowband IoT (NB-IoT), SIGFOX og 5G er eksempler på netværksteknologier, som er specialiserede til at understøtte trådløs kommunikation mellem fysiske enheder. NB-IoT er baseret på de eksisterende LTE-mobilnet, mens SIGFOX kræver opbygningen af et nyt landsdækkende accessnetværk. Det forventes, at både SIGFOX og NB-IoT vil blive udbudt kommercielt i Danmark i begyndelsen af 2017. 5G mobilteknologien er ved at blive udviklet og forventes at blive kommercielt tilgængelig omkring 2020. De nye teknologier vil medvirke til at accelerere udbredelsen af IoT enheder, herunder realiseringen af Smart Cities, men risikerer samtidig at åbne for nye sårbarheder, som cyberaktører vil forsøge at udnytte.
- Mobilteknologier og tjenester som Voice over LTE, Wi-Fi calling og internetforbundne Small Cells, anvendes og udbydes allerede af teleudbydere i Danmark. Teknologien kan øge mobildækningen i bygninger og muliggør talekald over LTE-mobilnettet, men tjenesterne åbner også for nye sårbarheder og cybertrusler, når Wi-Fi teknologi og internettet indgår som en del af infrastrukturen i mobilnettet.

På det forretningsmæssige område har samarbejde mellem udbyderne og sammenlægning af teleinfrastruktur været en måde at nedbringe udbydernes omkostninger og forbedre servicen til deres kunder. Nationale roamingaftaler og sammenlægning af mobilnetværk kan forbedre mobildækningen for brugerne samtidig med, at udbyderne mindsker behovet for at udbygge deres mobil-

net. Den øgede centralisering af teleinfrastrukturen, og deraf følgende lavere grad af redundans, kan imidlertid gøre teleinfrastrukturen mindre robust overfor cyberangreb.

Outsourcing af teleinfrastruktur eller driftsopgaver benyttes allerede af telesektoren i Danmark. Outsourcing stiller store krav til teleudbyderen i forhold til at sikre udbyderens opretholdelse af fuld kontrol med teleinfrastrukturen. Hvis en dansk udbyder outsourcer væsentlige dele af sin forretning til lande, som afviger meget fra danske forhold på områder som f.eks. lovgivning, sikkerhedskultur, national stabilitet, korruption eller kriminalitet, kan det medføre en ændring af cybertruslen mod teletjenesterne i Danmark. Hvis væsentlige dele af driften eller teleinfrastrukturen er outsourcet til udlandet, kan en eventuel hjemtagelse, eller overdragelse til anden leverandør, være udfordrende.

Anbefalinger

CFCS anbefaler, at topledelsen hos udbyderne i telesektoren, med udgangspunkt i denne trusselsvurdering, erkender og handler på baggrund af det beskrevne trusselsbillede. Forankringen i topledelsen skal sikre, at de rette tekniske kompetencer er til stede i et nødvendigt omfang i det videre arbejde. CFCS anbefaler endvidere, at der anvendes en risikobaseret tilgang i organisationens arbejde med cyberforsvar. Der bør foretages en risikovurdering med udgangspunkt i det aktuelle trusselsbillede, der inddrager forhold omkring organisationens erkendte sårbarheder. Forudsætningen for at kunne erkende disse sårbarheder er, at organisationen har et godt overblik over egen it-infrastruktur, it-processer, mv. Udarbejdelsen af en risikobaseret informationssikkerhedspolitik kan med fordel tage udgangspunkt i ISO/IEC-27001 standarden.

CFCS har udarbejdet et antal vejledninger, som kan inddrages i udbydernes generelle vidensindsamling på området. Som minimum bør alle mindre og lokale udbydere implementere top 4 sikringstiltag fra vejledningen ”Cyberforsvar der virker”, mens øvrige udbydere bør implementere alle 7 trin.

Øvrige relevante vejledninger:

- Spear-phishing – et voksende problem
- Reducér risikoen for ransomware
- Sådan kan du imødegå DDoS-angreb
- Logning – en del af et godt cyberforsvar
- Passwordvejledning

Endelig er det et helt grundlæggende princip, at kritiske netværkskomponenter samt drifts- og kontrolsystemer i teleinfrastrukturen bør adskilles logisk eller fysisk fra teleudbyderens administrative netværk samt sikres mod uautoriseret adgang via internettet. Dette er især væsentligt, hvis udbyderen har etableret mulighed for fjernadgang til teleinfrastrukturen via internettet. En sådan adgang bør beskyttes med en 2-faktor-autentifikation.

CFCS anbefaler alle teleudbydere at arbejde tæt sammen med deres leverandører for at sikre, at udstyr og teleinfrastruktur installeres, konfigureres og vedligeholdes i henhold til best practice.

Baseret på erfaringer skal CFCS understrege betydningen af, at teleudbyderne har god logning og god krisestyring samt opdateret viden om egen infrastrukturs design og opbygning.

Definition af trusselsniveauerne

Nedenstående oversigt beskriver kort de trusselsniveauer, som FE benytter sig af.

Trusselsniveau	Beskrivelse
Ingen	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
Lav	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
Middel	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
Høj	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
Meget høj	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynlighed i analyser: