CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod telesektoren

1. udgave juni 2022

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave juni 2022

CENTER FOR CYBERSIKKERHED

Center for cybersikkerhed hæver trusselsniveauet for cyberaktivisme til HØJ for telesektoren

Dato: 8. februar 2023

Truslen fra cyberaktivisme mod telesektoren hæves fra **MIDDEL** til **HØJ**. Det betyder, at det er sandsynligt, at virksomheder og myndigheder i sektoren vil blive ramt af cyberaktivistiske angreb inden for de næste to år.

CFCS hævede den 31. januar 2023 truslen fra cyberaktivisme mod Danmark. CFCS vurderer, at den øgede trussel fra cyberaktivisme også gælder for telesektoren.

CFCS hævede niveauet på baggrund af pro-russiske cyberaktivisters høje aktivitetsniveau mod NATO-lande, herunder Danmark, samt deres mere formaliserede angrebsmodus og øgede kapacitet.

Teksten i trusselsvurderingen er ikke opdateret, og kapitlet om cyberaktivisme afspejler ikke det gældende trusselsniveau.

For yderligere information om, hvorfor niveauet for cyberaktivisme er hævet, og hvordan truslen kommer til udtryk, henvises til CFCS' trusselsvurdering "CFCS hæver trusselsniveauet for cyberaktivisme mod Danmark fra **MIDDEL** til **HØJ**" udgivet d. 31. januar 2023.

Trusselsvurderingen kan findes på www.cfcs.dk.

Cybertruslen mod telesektoren

Denne trusselsvurdering har til formål at give beslutningstagere inden for telesektoren en opdateret indsigt i cybertrusler rettet mod sektoren. I vurderingen sænker CFCS truslen fra cyberspionage mod sektoren fra HØJ til MIDDEL og hæver truslen fra cyberaktivisme fra **LAV** til **MIDDEL**. Vurderingen afløser den hidtidige trusselvurdering for telesektoren fra 2019.

Hovedvurdering

- Der er en **MEGET HØJ** trussel fra cyberkriminalitet. Den generelle trussel fra kriminelle hackere mod virksomheder i Danmark gælder også for telesektoren. Nogle typer virksomheder, også i telesektoren, kan være særligt udsatte for cyberkriminalitet. Truslen fra cyberkriminalitet er så alvorlig, at teleselskaber dagligt udsættes for hackeres rekognoscering eller forsøg på kompromittering.
- Der er en **MIDDEL** trussel fra cyberspionage mod den danske telesektor. Trusselsniveauet er sænket fra **HØJ** til **MIDDEL**, da det vurderes, at sektoren på nuværende tidspunkt ikke er et højt prioriteret angrebsmål. Fremmede stater har dog fortsat kapacitet til at spionere mod telesektoren og kompromittere teleinfrastruktur, og det er muligt, at telesektoren i Danmark vil blive udsat for forsøg på cyberspionage.
- Truslen fra cyberaktivisme hæves fra **LAV** til **MIDDEL**. CFCS hæver trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod vesteuropæiske NATO-lande i forbindelse med situationen i Ukraine. Det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark, herunder telesektoren.
- Der er en **LAV** trussel fra destruktive cyberangreb. Det er mindre sandsynligt, at fremmede stater vil udføre destruktive cyberangreb mod Danmark. Virksomheder og myndigheder, som har aktiviteter eller leverandører i konfliktområder, er mere udsatte for truslen.
- Der er **INGEN** trussel fra cyberterror. Alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som ved konventionel terror, forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten blandt disse grupper er samtidigt begrænset.

Indledning

Danmark er et at de mest digitaliserede samfund i verden. En forudsætning for det digitale samfund er, at mennesker og maskiner kan kommunikere digitalt på en effektiv og sikker måde. Derfor er tilgængelighed, fortrolighed og integritet af teletjenesterne af kritisk betydning for samfundets funktion og sikkerhed.

Trusselsvurderingen beskriver cybertruslerne mod teleudbydere i Danmark, som leverer elektroniske kommunikationsnet og -tjenester til myndigheder, virksomheder og private borgere. Eksempler på teletjenester er adgang til taleopkald og internetforbindelse via fast- eller mobilnet samt tjenester dedikeret til kommunikation mellem maskiner, også kaldet IoT eller "tingenes internet".

Cyberangreb mod telesektoren har forskellige formål. Nogle angreb er primært en trussel mod selskaberne og deres økonomi, mens andre angreb også kan have konsekvenser for selskabernes kunder. Cyberangreb, der truer teletjenesterne er særligt alvorlige. Hvis teletjenesterne ikke er tilgængelige, kan det, udover at være generende for private brugere, påvirke produktionen i virksomheder og forhindre, at andre kritiske sektorer i Danmark fungerer optimalt. Det kan eksempelvis dreje sig om beredskab, energiforsyning og sundhedssektoren.

Trusselsvurderingen er opdelt i trusler fra cyberangreb, der understøtter kriminalitet, spionage, destruktive cyberangreb, aktivisme og terrorisme, og beskriver det aktuelle trusselsbillede med en varslingshorisont på to år. Sidst i vurderingen beskrives 5G's betydning for cybertruslen mod telesektoren.

Væsentlige ændringer i forhold til den tidligere trusselsvurdering er, at niveauet for truslen fra cyberspionage er sænket fra **HØJ** til **MIDDEL** og truslen fra cyberaktivisme er hævet fra **LAV** til **MIDDEL**.

Efter Ruslands invasion af Ukraine den 24. februar 2022 står Danmark overfor et forandret sikkerhedspolitisk landskab, hvor fremtiden på flere områder tegner mere usikker end før. Denne usikkerhed har også spredt sig til cyberområdet, hvor trusselsbilledet hurtigt kan ændre sig, hvis eksempelvis forholdet mellem NATO-landene og Rusland bliver væsentligt forværret.

CFCS følger løbende trusselsbilledet, herunder også tendenser i udlandet, der kan have betydning for cybertruslen mod telesektoren i Danmark, og vil opdatere trusselsvurderingen, hvis der sker væsentlige ændringer.

Cyberkriminalitet

Der er en **MEGET HØJ** trussel fra cyberkriminalitet mod telesektoren. Det betyder, at det er meget sandsynligt, at teleudbydere i Danmark vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

CFCS bruger begrebet cyberkriminalitet som en fællesbetegnelse for handlinger, hvor hackere anvender cyberangreb til at begå kriminalitet, der er motiveret af økonomisk berigelse.

CFCS vurderer, at den generelle trussel fra cyberkriminalitet også gælder for telesektoren. Det er dermed meget sandsynligt, at telesektoren dagligt udsættes for kriminelle hackeres forsøg på kompromittering eller rekognoscering efter sårbarheder.

Kriminelle hackere går som udgangspunkt ikke efter bestemte sektorer men angriber bredt myndigheder og virksomheder, der er til stede på internettet. Nogle virksomheder i telesektoren kan dog være attraktive mål for bl.a. afpresningsangreb. Det skyldes, at sektoren er samfundsvigtig, håndterer følsomme data og er afhængig af en høj oppetid på it-systemer og teletjenester. Hackere kan derfor vurdere, at selskaber i telesektoren vil være villige til at betale en løsesum for hurtigere at kunne reetablere normal drift efter et afpresningsangreb.

Afpresningsangreb med ransomware kan få konsekvenser for teletjenesterne
Ransomware-angreb er et af de typer afpresningsangreb, som udgør en trussel mod den danske telesektor. Ved denne type angreb krypterer kriminelle centrale it-systemer hos myndigheder og virksomheder for derefter at afpresse ofrene en løsesum mod at udlevere den digitale nøgle, der kan låse systemerne op igen. Udover at kryptere data hos deres ofre afpresser de kriminelle også deres ofre for løsesummer ved at true med offentliggørelse af data, der er stjålet i forbindelse med angrebet.

Omfanget af afpresning gennem ransomware-angreb er nu så stort, at det er meget sandsynligt, at danske teleudbydere på kort sigt vil opleve forsøg på kompromittering med ransomware.

Danske teleudbydere har været ramt af ransomware
TT-Netværket, som driver Telias og Telenors fælles mobilradionet, blev i december 2021 ramt af ransomware. Ved angrebet blev der stjålet data, som hackerne truede med at lække. Mobilnetværket blev ikke påvirket af hændelsen.

GlobalConnect i Danmark som bl.a. leverer kommunikationsnet, internetforbindelser, telefoni og it-services til erhverv, blev i november 2019 ramt af ransomware i deres kontornet. Angrebet ramte dele af selskabets danske og tyske forretning, men påvirkede ikke kunderne.

I maj 2020 blev GlobalConnect igen mål for et ransomware-angreb. Denne gang ramte angrebet selskabets it-services og lammede flere kunders it-systemer. Ifølge selskabet påvirkede angrebet ikke kundernes teletjenester.

Ransomware-angreb rammer sædvanligvis kontornettet. Det skyldes primært, at kontornettet, modsat teleinfrastrukturen, næsten altid er forbundet til internettet, og at medarbejdernes mailklienter befinder sig i kontornettet. Malware, der bl.a. kommer ind via mails eller fjernadgange, som f.eks. anvendes til at arbejde hjemmefra, lander derfor først i kontornettet.

Hvis ransomware i kontornettet forhindrer driftspersonalets adgang til teleinfrastrukturen fra kontornettet, kan det vanskeliggøre driften af teleinfrastrukturen og derved påvirke teletjenesterne. Det samme er tilfældet, hvis data eller it-værktøjer i kontornettet, som er kritiske for opretholdelsen af teletjenesterne, er blevet utilgængelige på grund af ransomware. Ransomware i kontornettet kan desuden afskære kunder fra eventuelle selvbetjeningstjenester og teletjenester, der leveres via selskabets hjemmeside.

Særligt alvorligt er det, hvis ransomware rammer teleinfrastrukturen. At teleinfrastruktur kan rammes af ransomware understreges af, at ransomware også bliver udviklet til at kunne ramme Linux software og cloud infrastruktur, der ofte anvendes i moderne teleinfrastruktur.

Selvom flere teleudbydere i Danmark og resten af verden har været ramt af ransomware, er der endnu kun få eksempler på, at det har påvirket teletjenester. Det skyldes blandt andet, at teleinfrastrukturen traditionelt ikke er forbundet direkte til internettet. Udvalgte medarbejdere har dog typisk mulighed for at tilgå systemer i teleinfrastrukturen via en portal i kontornettet. Det samme kan gælde for leverandører i forbindelse med drift- eller supportopgaver.

Alle steder hvor medarbejdere eller leverandører kan tilgå teleinfrastrukturen, er der en risiko for, at hackere også får adgang. Hvis hackere opnår adgang til kontornettet, er der således en risiko for, at malware, herunder ransomware, kan sprede sig til teleinfrastrukturen.

Målrettede ransomware-angreb er udført af professionelle kriminelle aktører med det formål at tjene penge. Der er dog også andre typer af afpresningsangreb, der ligeledes udgør en trussel mod telesektoren, men hvor både aktører og formål i højere grad kan variere. Det gælder eksempelvis for DDoS-angreb.

DDoS-angreb udgør også en trussel mod telesektoren

Telesektoren er udsat for en vedvarende trussel fra DDoS-angreb. DDoS står for Distributed Denial of Service og er et overbelastningsangreb, hvor hackere genererer usædvanligt store mængder datatrafik mod en hjemmeside eller et netværk, så disse bliver utilgængelige for legitim trafik, mens angrebet står på.

DDoS-angreb mod Norlys påvirkede teletjenester

I maj 2021 blev Norlys ramt af et DDoS-angreb rettet mod selskabets DNS-servere. Angrebet berørte en stor del af selskabets kunder, som bl.a. oplevede forstyrrelser eller nedbrud på Webmail, TV- og internetløsninger.

DDoS-angreb kan overbelaste kritisk teleinfrastruktur og derved påvirke kunders internetforbindelse, uanset om angrebet er rettet mod teleudbyderen eller en af udbyderens kunder. Det er blandt andet set i forbindelse med DDoS-afpresning. Teleselskabernes hjemmesider kan også blive ramt, hvilket kan påvirke bl.a. streaming- og mailtjenester, der leveres via hjemmesiden.

DDoS-afpresning er et gammelt fænomen, som i 2020 blussede op igen verden over. Særligt i maj og juni 2021 blev flere danske virksomheder, herunder teleudbydere, ramt. Angrebene viste, hvordan kraftige DDoS-angreb målrettet kritisk teleinfrastruktur kan påvirke teletjenester.

Dansk teleudbyder ramt af DDoS-afpresning
I maj 2021 blev Gigabit, nu Wizer, ramt af DDoS-afpresning. DDoS-angrebet ramte selskabets DNS-servere og hjemmeside. Angrebet påvirkede bl.a. kunders internetforbindelse og gjorde det vanskeligt at kontakte selskabet via telefon.

Selskabet genetablerede sin telefonforbindelse og kundernes internetforbindelser uden at betale den krævede løsesum.

Iværksættelsen af DDoS-angreb kræver ikke avancerede hackerkompetencer. Derfor kan metoden anvendes af flere typer aktører med forskellige motiver. Det kan være kriminelle, der vil afpresse et offer eller genere en konkurrent, men det kan potentielt set også være en stat, der vil forstyrre samfundsvigtig infrastruktur. Der er også flere eksempler på, at gamere laver DDoS-angreb mod andre spillere eller spiludbydere.

Andre typer cyberkriminalitet rammer også telesektoren
Udover at afpresse teleudbydere gennem DDoS- og ransomware-angreb for at omsætte eventuelle adgange eller data til kontanter er der også kriminelle, som via social engineering forsøger at narre eksempelvis teleudbydere til at overføre penge til de kriminelles konti.

Den type svindel kaldes bl.a. Business Email Compromise eller direktørsvindel. Angrebene varierer meget i kompleksitet fra simple phishingmails til organiserede kriminelle, der sender troværdige phishingmails fra en kompromitteret leverandør eller samarbejdspartner.

Hackerne udnytter de oplysninger en teleudbyder eksponerer på internettet via sin egen eller andre hjemmesider, til at øge deres troværdighed overfor ofret. Det kan f.eks. være oplysninger om ansatte, organisation, mailadresser, kunder eller leverandører.

Telesektorens kundekonti og selvbetjeningsløsninger er et andet attraktivt mål for hackere. Adgangsoplysningerne til en selvbetjeningsportal kan sælges til andre hackere og adgangen til en kundes webmail kan bruges til yderligere kriminalitet. Eksempelvis kan mailkontoen udnyttes til at udsende spam- eller phishing-mails og adgangen til en streamingtjeneste kan videresælges.

Hackere kan også udnytte en kompromitteret selvbetjeningsløsning til at bestille et nyt simkort i kundens sted og derved overtage kundens mobilnummer for at misbruge det til yderligere kriminalitet.

Cyberkriminelle hackere udnytter alle veje ind
Leverandører bliver brugt som angrebsvinkel i de såkaldte supply-chain-angreb. De leverandører, der har en legitim og privilegeret adgang til deres kunders it-systemer, er særligt attraktive for hackere.

Ved at udnytte en leverandør som springbræt ind i en teleudbyders netværk kan hackere sætte en teleudbyders perimeterforsvar skakmat. På samme måde kan en kompromittering af en softwareleverandør føre til, at en teleudbyder uden at vide det installerer software eller en softwareopdatering, indeholdende malware i it- eller teleinfrastrukturen.

Kaseya udnyttet i ransomware-angreb
VSA (Virtual System Administrator) er et softwareprodukt til fjernovervågning og drift af it-netværk fra det amerikanske selskab Kaseya. Ved at udnytte en sårbarhed i produktet uploadede hackere i juni 2021 ransomware på Kaseyas kunders VSA-servere. Ransomwaren blev derved spredt til de computere, som var forbundet til serverne.

Ifølge Kaseya blev omkring 50 kunder, herunder Managed Service Providers (MSP), ramt af hændelsen. Det førte til, at yderligere 800 til 1500 virksomhedskunder hos MSP'erne blev ramt af ransomwaren.

CFCS har ikke kendskab til, at danske teleudbydere blev ramt af hændelsen.

Cyberspionage

Der er en **MIDDEL** trussel fra cyberspionage. Det betyder, at det er muligt, at telesektoren vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Trusselsniveauet er sænket fra **HØJ** til **MIDDEL** i forhold til den tidligere trusselvurdering fra 2019. Ændringen er sket på baggrund af en fornyet analyse, der viser, at selvom det er muligt, at fremmede stater planlægger cyberspionage mod telesektoren i Danmark, så er den danske telesektor sandsynligvis ikke et højt prioriteret angrebsmål på nuværende tidspunkt.

Cyberspionage mod telesektoren retter sig især mod sektorens kunder
Spionage har primært til formål at indhente information, der kan give en stat sikkerhedspolitisk viden eller fremme et lands industri og økonomi. Telesektoren i Danmark er ikke i sig selv en traditionel kilde til information af sikkerhedspolitisk karakter, og udvikler ikke ny teknologi, der umiddelbart kan understøtte fremmede staters økonomi. Derfor er det sandsynligt, at cyberspionage mod telesektoren i

mindre grad er rettet mod selve teleudbyderne, og i større grad mod den information teleudbyderne besidder om deres kunder og disses brug af teletjenester.

Formålet med cyberspionage mod telesektoren i udlandet har ofte været at lokalisere eller følge enkeltpersoner eller stjæle opkaldsdata og sms-beskeder, der kan afsløre en kundes kontakter og kommunikation. Der har dog også været eksempler på generel indhentning af store mængder opkaldsdata.

Cyberspionage mod telesektoren kan også have til formål at aflytte kunders datakommunikation, hvilket potentielt kan ske ved at hacke en teleudbyder. Ofte vil andre metoder dog være mere effektive for en angriber.

Der er kapacitet til og mulig hensigt om at spionere mod telesektoren
Hændelser i udlandet viser, at fremmede stater har både kapacitet og vilje til at udføre avancerede cyberangreb mod teleselskaber og teleinfrastruktur. Kapaciteten omfatter spionage via kompromittering af teleudbydernes kontornetværk eller selve teleinfrastrukturen.

Det kræver særlige adgange, evner og viden at kompromittere teleinfrastruktur. Det skyldes, at infrastrukturen normalt ikke er direkte forbundet til internettet og ofte anvender hardware, software og protokoller, som er forskellige fra de it-systemer, der indgår i et almindeligt kontornetværk.

Statslige hackere har stjålet opkaldsdata fra teleudbydere
Et amerikansk it-sikkerhedsfirma har i august 2021 afsløret, hvordan hackere, der ifølge sikkerhedsfirmaet var støttet af Kina, i årevis har stjålet opkaldsdata fra teleudbydere i Sydøstasien.

Hackerne har blandt andet udnyttet sårbarheder i Microsoft Exchange servere, som blev kendt af offentligheden i marts 2021.

Den cyberspionage der er set mod telesektoren i udlandet knytter sig ofte til sikkerhedspolitiske interesser. Det kan eksempelvis dreje sig om konflikter mellem stater eller mellem stater og bestemte personer eller befolkningsgrupper. Der er tegn på, at særligt teleselskaber i Asien og Mellemøsten er udsat for den type cyberspionage, mens omfanget generelt er mindre i Europa.

CFCS vurderer, at det er muligt, at danske teleudbydere vil blive mål for den type cyberspionage. Det gælder særligt, hvis der i Danmark bor eller opholder sig personer, en fremmed stat opfatter som spionagemål. Det kan være, fordi personen vurderes at udgøre en sikkerhedsrisiko eller har kontakter eller adgang til informationer, som er eftertragtede af en fremmed stat.

Stater spionerer via usikre protokoller i teleinfrastrukturen
Fremmede stater udnytter den såkaldte SS7-protokol til at forsøge at lokalisere mobiltelefoner og derved deres brugere. Protokollen kan også udnyttes til at opsnappe en persons opkald og sms-beskeder. SS7-protokollen anvendes i det netværk, der forbinder verdens mobilnet. Protokollen benyttes i 2G og 3G mobilnet til bl.a. til at lokalisere i hvilket land og ved hvilken mobilmast, en mobiltelefon befinder sig.

Metoden er enkel at bruge, og fremmede stater kan have gode muligheder for at få adgang til SS7-netværket i deres hjemland. Det er derfor muligt, at fremmede stater vil forsøge at anvende metoden til at spionere mod målpersoner, der er kunder hos danske teleudbydere.

I 4G mobilnet og de 5G mobilnet som anvender 4G kernenettet, er SS7-protokollen erstattet af Diameter-protokollen. Diameter har arvet flere svagheder fra SS7-protokollen. Det er derfor muligt, at stater fremadrettet vil forsøge at udnytte svaghederne i Diameter-protokollen til at spionere.

Telesektoren er truet af cyberspionage via forsyningskæden
Fremmede stater kan ligesom cyberkriminelle udnytte telesektorens leverandører som angrebsvektor, når de udfører cyberspionage. Truslen omfatter både den direkte leverandør og en leverandørs egne underleverandører.

En leverandør, der leverer it-drift eller -support, kan give direkte adgang til et spionagemål via leverandørens fjernadgang. Alternativt kan malware smugles ind i en organisation ved at tilføje den skadelige kode til en leverandørs legitime softwareprodukt eller softwareopdatering. Metoden er effektiv, fordi teleselskaber, ligesom andre selskaber, er nødt til at stole på deres leverandører.

Solarwinds udnyttet til cyberspionage via forsyningskæden
I december 2020 opdagede sikkerhedsfirmaet FireEye et af de mest omfattende offentligt kendte cyberspionageangreb nogensinde. Organisationer verden over, herunder i Danmark, var blevet kompromitterede via softwaren Orion fra den amerikanske virksomhed SolarWinds. Offentligt kendte ofre er bl.a. Microsoft og Deloitte.

CFCS vurderer, at kompromitteringen via SolarWinds' software var en meget alvorlig trussel. Det er sandsynligt, at formålet med kompromitteringen var spionage.

Angrebet blev ifølge åbne kilder udført ved, at hackere kompromitterede virksomheden SolarWinds, som leverer software til organisationer verden over. Hackerne tilføjede i marts 2020 ondsindet kode i legitime opdateringer til SolarWinds' software Orion. Ifølge SolarWinds downloadede op imod 18.000 kunder verden over de kompromitterede opdateringer. Den ondsindede kode gav hackerne en indledende adgang til ofrenes systemer, som de kunne udnytte yderligere. CFCS vurderer, at aktøren kun udnyttede adgangene mod de mest interessante ofre.

Den kompromitterede software blev blandt andet downloadet af danske teleselskaber. CFCS har dog ikke kendskab til, at aktøren efterfølgende udnyttede adgangen.

Cyberspionage mod telesektoren kan have et destruktivt formål
Cyberspionage kan anvendes som forberedelse af et destruktivt cyberangreb mod telesektoren. Forberedelsen kan bl.a. bestå i at indsamle teknisk viden om

telesektorens it- og teleinfrastruktur. Den viden kan udnyttes til at planlægge et eventuelt fremtidigt destruktivt cyberangreb eller til at installere bagdøre i infrastrukturen, som senere kan anvendes til destruktive formål.

Cyberaktivisme

Truslen fra cyberaktivisme mod telesektoren er **MIDDEL**. CFCS hæver dermed trusselsniveauet fra **LAV** til **MIDDEL** i forhold til den tidligere vurdering fra 2019.

Trusselsniveauet **MIDDEL** betyder, at der er en generel trussel mod telesektoren, samt at det er muligt, at danske teleudbydere vil blive ramt af aktivistiske cyberangreb på kort sigt.

CFCS hæver trusselsniveauet på baggrund af aktivistiske cyberangreb udført i forbindelse med Ruslands invasion af Ukraine og efterfølgende reaktioner på krigen. Cyberaktivistiske angreb ramte i krigens indledende fase hovedsageligt mål i Rusland, Ukraine og Belarus, men har efterfølgende bredt sig til mål i vesteuropæiske NATO-lande. CFCS vurderer, at det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark, herunder telesektoren.

Cyberaktivisme udføres af individer og hackergrupper, der udfører cyberangreb for at få mest mulig opmærksomhed på deres dagsorden eller for at straffe organisationer, som cyberaktivisterne ser som symbolske mål eller modstandere af deres sag. Cyberaktivisme er typisk drevet af forskellige ideologiske eller politiske motiver, der strækker sig fra dyrevelfærd over politiske enkeltsager til modstand mod magthavere.

Aktivistiske cyberangreb varierer meget i kompleksitet fra relativt simple overbelastningsangreb til mere ressourcekrævende hack og læk operationer.

Krigen i Ukraine har medført en stigning i cyberaktivistiske angreb rettet mod parterne i konflikten. Aktører på begge sider af konflikten udgør derfor en trussel for aktivistisk motiverede cyberangreb mod Danmark, herunder telesektoren.

Krigen i Ukraine har endnu ikke har medført en markant stigning i cyberaktivisme mod danske mål. Det kan imidlertid ske med kort eller ingen varsel, hvis cyberaktivistiske grupper sætter fokus på Danmark. Pro-russiske aktivister kan være interesserede i at straffe eller påvirke dansk støtte til Ukraine, herunder støtte fra telesektoren, mens pro-ukrainske aktivister kan være interesserede i enten at straffe organisationer med tilknytning til Rusland eller angribe mål i lande, som de mener ikke gør nok for at støtte Ukraine.

Truslen gælder dermed også for danske organisationer eller personer med relationer til Ukraine, der kan blive ramt af angreb rettet mod mål i Ukraine. Danske ofre kan f.eks. få lækket følsomme oplysninger i forbindelse med hack og læk-angreb rettet mod organisationer i Ukraine.

Destruktive cyberangreb

Der er en **LAV** trussel fra destruktive cyberangreb. Det betyder, at det er mindre sandsynligt, at telesektoren vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Flere fremmede stater, herunder Rusland, har kapacitet til at udføre cyberangreb, der kan bruges destruktivt mod samfundsvigtig infrastruktur såsom telesektoren. Destruktive cyberangreb er cyberangreb, hvor den forventede effekt er død eller personskade, betydelig skade på fysiske objekter og/eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

Aktuelt er det mindre sandsynligt, at fremmede stater har til hensigt at udføre destruktive cyberangreb mod telesektoren i Danmark. Truslen kan stige i forbindelse med en skærpet konflikt eller geopolitiske spændinger mellem Danmark og stater, der har kapacitet til at udføre destruktive cyberangreb, hvis disse staters intention ændrer sig.

Aktiviteter eller leverandørforhold i konfliktområder kan hæve truslen
I konfliktområder uden for Danmarks grænser kan truslen for destruktive cyberangreb være højere. Det betyder, at et teleselskab med aktiviteter eller leverandørforhold i et konfliktområde kan blive ramt af et angreb, der ikke er rettet mod Danmark men generelt mod organisationer, som opererer i området.

Cyberterror

Der er **INGEN** trussel fra cyberterror. Det betyder, at det er usandsynligt, at virksomheder i 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.

Fraværet af cyberterror skyldes, at hensigten er begrænset, og at militante ekstremister ikke har den fornødne kapacitet til at udføre cyberangreb, der er så ødelæggende, at de kan sammenlignes med konventionel terror.

Militante ekstremister har i årevis udnyttet internettet til at understøtte deres organisationer og til at planlægge konventionel terror og udføre simple aktivistiske cyberangreb som DDoS-angreb og defacement. Alligevel har der endnu ikke været nogen eksempler på, at terrorister har været i stand til at udføre egentlig cyberterror.

5G har ikke øget cybertruslen mod telesektoren

Introduktionen af 5G mobilnet i Danmark har ikke ført til en øget cybertrussel mod telesektoren. 5G introducerer dog forhold, som på sigt kan øge risikoen ved og konsekvenserne af et cyberangreb, ligesom det forventede øgede antal forbundne enheder vil kunne udnyttes af hackere.

5G er mere kompleks end tidligere teknologier, og er fra grunden designet som en cloudløsning. Det betyder, at telesektoren skal forholde sig til nye angrebsflader- og vektorer. Samtidig kan det blive mere krævende at holde infrastrukturen opdateret og korrekt konfigureret til at kunne imødegå cybertruslen. Når teleudbyderne i Danmark inden for de kommende år har opgraderet kernenettet i mobilinfrastrukturen til 5G, medfører det samtidig et endegyldigt farvel til kernenettet som et velafgrænset fysisk netværk, der relativt let kan beskyttes mod hackere.

De første kommercielle 5G mobilnet i Danmark blev tændt i slutningen af 2020. Endnu anvendes 5G kun i radionettene, mens kernenetværket stadig er 4G. Det giver primært højere datahastighed. Først når teleudbyderne i de kommende år bygger 5G kernenetværk, vil de funktioner, som adskiller 5G fra tidligere mobilnetværk blive tilgængelige.

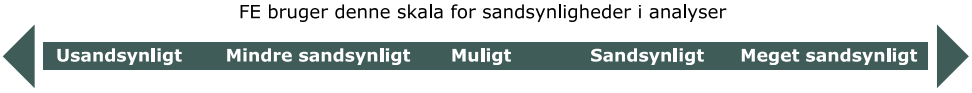
5G vil gøre det muligt at designe nye tjenester, som indebærer mere end blot telekommunikation. 5G forventes således at understøtte nye innovative løsninger i blandt andet byer, industrien, transportsektoren, underholdningsindustrien og sundhedssektoren. 5G kan eksempelvis gøre det muligt at sende live 3D-billeder fra et skadested eller en ambulance til en læge på et hospital, som derved mere effektivt kan assistere behandlerne i felten.

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



Andre relevante publikationer

Center for Cybersikkerhed (CFCS) udgiver løbende vejledninger og trusselsvurderinger. Nedenfor er fremhævet en række produkter af særlig relevans for telesektoren. Alle produkterne er tilgængelige på CFCS' hjemmeside.

Cyberforsvar der virker
Center for Cybersikkerheds grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb. Læs vejledningen her:
https://cfcs.dk/da/forebyggelse/vejledninger/cyberforsvar-der-virker/

Beskyt mod DDoS-angreb
Vejledningen giver en række anbefalinger til hvordan man forebygger, forsinker og håndterer DDoS-angreb. Læs vejledningen her:
https://cfcs.dk/da/forebyggelse/vejledninger/DDoS-angreb/

Reducer risikoen for ransomware
Vejledningen giver anbefalinger som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Læs vejledningen her:
https://cfcs.dk/da/forebyggelse/vejledninger/ransomware/

Informationssikkerhed i leverandørforhold
Vejledningen giver råd til styringsmekanismer og forventningsafstemning i forholdet mellem forretningen og leverandøren. Læs vejledningen her:
https://cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

Cybersikkerhed for bestyrelser
Vejledningen stiller skarpt på cyber- og informationssikkerhed i bestyrelseslokalet. Læs vejledningen her:
https://cfcs.dk/da/forebyggelse/vejledninger/cybersikkerhed-for-bestyrelser/

Digitale gidseltagere på storvildtjagt
Trusselsvurderingen beskriver truslen fra såkaldte målrettede ransomware-angreb, der kan have alvorlige konsekvenser for en organisation. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

Anatomien af målrettede ransomware-angreb
Undersøgelsesrapporten går i dybden med, hvordan sådanne angreb foregår. Rapporten indeholder konkrete råd til, hvordan angrebene kan imødegås. Læs rapporten her:
https://www.cfcs.dk/da/cybertruslen/rapporter/anatomien-i-ransomware-angreb/

Cybertruslen fra phishing-mails
Trusselsvurderingen går i dybden med, hvordan hackere benytter phishing- og spear-phishing-mails i deres forsøg på at kompromittere virksomheder eller franarre dem følsomme oplysninger. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/phishing/

Hackere scanner dit netværk for sårbarheder hver dag året rundt
Trusselsvurderingen beskriver hvordan hackere afsøger internettet for udstyr med sårbarheder, de kan udnytte til at kompromittere organisationer. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/hackere-scanner-dit-netvaerk/

Cybertruslen fra bevidste og ubevidste insidere
I trusselsvurderingen kan du læse mere om truslen fra insidere og anbefalinger til mitigerende tiltag. Læs vurderingen her:
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/insidertruslen/