Styrelsen for
Samfundssikkerhed

TRUSSELSVURDERING

Cybertruslen mod telesektoren

Marts • 2025

Indhold

Styrelsen for
Samfundssikkerhed

Datavej 20
3460 Birkerød
Telefon: + 45 4516 1666
E-mail: cfcs@cfcs.dk

Marts 2025

Cybertruslen mod telesektoren

Trusselsvurderingen beskriver cybertruslen mod telesektoren i Danmark. Formålet er at orientere risikoejere om trusselsbilledet samt stille viden til rådighed, der kan indgå i telesektorens arbejde med risikovurderinger. Trusselsvurderingen baserer sig på Styrelsen for Samfundssikkerhed (SAMSIK) seneste viden om cybertruslen og erstatter den tidligere udgave af "Cybertruslen mod telesektoren" fra juni 2022.

Hovedvurderinger

- Truslen fra cyberkriminalitet mod den danske telesektor er **MEGET HØJ**. Truslen kommer løbende til udtryk i form af kriminelle cyberangreb mod organisationer på tværs af sektorer, og dermed også telesektoren. Særligt ransomware og andre afpresningsangreb kan få alvorlige konsekvenser.

- Truslen fra cyberspionage mod den danske telesektor er **HØJ**. SAMSIK hæver dermed niveauet fra **MIDDEL** til **HØJ**. Baggrunden er, at der de seneste par år har været flere forsøg på cyberspionage mod den europæiske telesektor. SAMSIK vurderer, at aktiviteten er udtryk for en øget interesse for telesektoren i Europa fra statslige hackere, hvilket øger truslen mod den danske telesektor.

- Truslen fra cyberaktivisme mod den danske telesektor er **HØJ**. Truslen kommer især fra pro-russiske cyberaktivister, der løbende udfører DDoS-angreb mod hjemmesider i europæiske NATO-lande, herunder i telesektoren.

- Truslen fra destruktive cyberangreb mod den danske telesektor er **MIDDEL**. Det skyldes, at Rusland har både kapacitet til og intention om at bruge hybride virkemidler med destruktive effekter mod europæiske NATO-lande. Det er dog mindre sandsynligt, at Rusland vil udføre destruktive cyberangreb, der skal skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.

- Truslen fra cyberterror mod den danske telesektor er **INGEN**. Militante ekstremister har aktuelt ikke den tekniske kapacitet, der kræves for at udføre cyberterror. Samtidig er intentionen om at udføre den slags angreb yderst begrænset.

Indledning

Danmark er et af de mest digitaliserede lande i verden og dybt afhængig af en velfungerende digital infrastruktur. Konsekvenserne kan derfor være store for både samfundets funktion og sikkerhed, hvis telesektorens kommunikationsnet og -tjenester forstyrres af et cyberangreb. Det er derfor vigtigt, at telesektorens infrastruktur er tilstrækkeligt beskyttet mod cyberangreb, og i den sammenhæng er viden om cybertruslen en central forudsætning.

Siden den seneste vurdering af cybertruslen mod telesektoren er trusselsbilledet for telesektoren blevet mere alvorligt. For eksempel hæver SAMSIK i denne trusselsvurdering trussels-niveauet for cyberspionage mod telesektoren til **HØJ.** Det sker på baggrund af en øget aktivitet fra statslige hackergrupper mod den europæiske telesektor. Tele- og internetudbydere i Danmark skal derfor også være opmærksomme på forsøg på cyberangreb fra fremmede stater.

Derudover blev truslen hævet for destruktive cyberangreb mod Danmark til **MIDDEL** i juni 2024 samt for cyberaktivisme til **HØJ** i januar 2023. Begge trusselsniveauer gælder også for telesektoren. Endelig er truslen fra cyberkriminalitet mod telesektoren fortsat **MEGET HØJ**, herunder fra ransomware-angreb, der kan have meget alvorlige konsekvenser for det enkelte offer og for samfundet.

Samlet set tegner sig altså et komplekst og alvorligt trusselsbillede, hvor både statslige og ikke-statslige hackere udgør en trussel. Trusselsbilledet mod telesektoren kan opsummeres således:

Cybertruslen mod telesektoren

Truslen fra cyberkriminalitet er **MEGET HØJ**

Truslen fra cyberspionage er **HØJ**

Truslen fra cyberaktivisme er **HØJ**

Truslen fra destruktive cyberangreb er **MIDDEL**

Truslen fra cyberterror er **INGEN**

Trusselsvurderingen beskriver cybertruslerne mod den danske telesektor som helhed. Det omfatter de organisationer, der leverer elektroniske kommunikationsnet og -tjenester til myndigheder, virksomheder og private borgere i Danmark, herunder f.eks. teleudbydere, der leverer tele- og internettjenester via fast- og mobilnet, samt udbydere af internet.

Tidshorisonten for trusselsvurderingen er som udgangspunkt to år. Styrelsen for Samfundssikkerhed anvender i sine trusselsvurderinger Forsvarets Efterretningstjenestes (FE) trussels- og sandsynlighedsniveauer. En nærmere beskrivelse fremgår sidst i vurderingen, hvor også en oversigt over de mest gængse angrebsmetoder kan læses.

Systemfejl i telesektoren forhindrede opkald i store dele af landet

TDC NET's mobilnet var den 28. november 2024 ramt af tekniske fejl, der betød, at mobilkunder, der benyttede TDC NET's mobilnetværk, i nogle timer ikke kunne foretage opkald. Selvom nedbruddet ikke skyldtes et cyberangreb, understreger hændelsen de alvorlige konsekvenser, det kan have for samfundet, når telesektorens tjenester ikke er tilgængelige. For eksempel oplevede nogle mobilkunder problemer med at foretage nødopkald til alarmcentralen.

Cyberkriminalitet

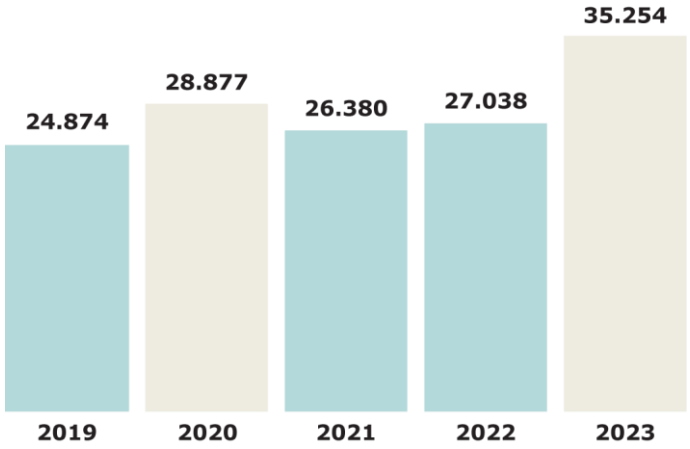
Truslen fra cyberkriminalitet mod den danske telesektor er **MEGET HØJ**.

Det skyldes, at telesektoren ligesom resten af samfundet er udsat for en vedvarende trussel fra opportunistiske cyberkriminelle. Truslen kommer løbende til udtryk i form af cyberangreb fra kriminelle hackere mod danske mål, og det er meget sandsynligt, at kriminelle hackere også vil rette cyberangreb mod den danske telesektor.

Hvad er cyberkriminalitet?

SAMSIK bruger cyberkriminalitet som en fællesbetegnelse for økonomisk motiveret it-kriminalitet begået ved hjælp af cyberangreb.

Ifølge Rigspolitiets Nationalt Center for IT-kriminalitet var anmeldelserne om økonomisk it-kriminalitet rekordhøjt i 2023 med en stigning på ca. 30 pct. fra 2022 til 2023. Økonomisk it-kriminalitet omfatter både cyberkriminalitet og it-kriminalitet uden brug af cyberangreb.



Kilde:
Nationalt Center for IT-kriminalitet

Kriminelle afpresningsangreb kan få alvorlige konsekvenser
Afpresningsangreb er en meget udbredt form for cyberkriminalitet, som kan få alvorlige konsekvenser for både det enkelte offer og for samfundet. Ved den slags angreb forsøger kriminelle hackere gennem forskellige teknikker at presse ofre til at betale en løsesum, typisk i form af kryptovaluta.

Selvom telesektoren sandsynligvis ikke er blandt de sektorer, som oftest rammes af afpresningsangreb, kan der i sektoren alligevel være attraktive mål. For eksempel har organisationer i telesektoren ofte høje omsætninger, store mængder følsomme data samt høje krav fra omverdenen omkring oppetid på deres samfundskritiske it-systemer og teletjenester. Kriminelle hackere kan derfor vurdere, at selskaber i telesektoren vil være tilbøjelige til at betale høje løsesummer.

En af de typer afpresningsangreb, som cyberkriminelle udfører, er ransomware-angreb. Her gør hackerne offerets data og systemer utilgængelige via kryptering, hvorefter de kræver en løsesum for at give offeret adgang til sine data og systemer. Såfremt telesektoren rammes af et ransomware-angreb, kan det få meget alvorlige konsekvenser for samfundet, hvis angrebet påvirker tilgængeligheden af samfundskritiske teletjenester. Samtidig kan det også få omfattende konsekvenser for det enkelte offer i form af bl.a. udgifter til genopretning eller tab af tillid hos kunder og investorer.

Tele- og internetudbydere verden over rammes løbende af ransomware-angreb fra kriminelle hackere. For eksempel var den britiske teleudbyder BT Group offer for et ransomware-angreb i december 2024. Tidligere har danske TT-Netværket, der driver Telias og Telenors mobilnet, og GlobalConnect også været udsat for ransomware-angreb i henholdsvis 2021 og 2020. Hændelserne i Danmark påvirkede dog ikke udbydernes teletjenester.

Ransomware rammer oftest teleudbyderes kontornetværk

Ransomware-angreb mod tele- og internetudbydere er oftest rettet mod kontornetværk frem for teleinfrastrukturen. Det skyldes, at dele af kontornetværket typisk er forbundet direkte med internettet og dermed mere sårbart, mens teleinfrastrukturen oftest skal tilgås fra kontornettet via lokale fjernadgange. Det er dog ikke ensbetydende med, at teleinfrastrukturen ikke kan blive ramt. Nogle cyberkriminelle har f.eks. også udviklet ransomware til Linux-software og cloud-infrastruktur, som anvendes i moderne teleinfrastruktur. Desuden kan teleinfrastruktur blive indirekte påvirket af et ransomware-angreb, hvis eksempelvis driftssystemer ikke kan tilgås eller må lukkes ned som følge af et ransomware-angreb mod kontornetværket.

Cyberkriminelle anvender også andre typer afpresningsangreb end ransomware-angreb i jagten på økonomisk berigelse. For eksempel har nogle kriminelle hackere specialiseret sig i at stjæle data og dernæst true med at lække eller sælge det, hvis ikke en løsesum betales. Selvom data og systemer i dette tilfælde ikke krypteres, kan et angreb fortsat få store konsekvenser, hvis f.eks. forretningshemmeligheder eller persondata sælges eller lækkes af hackerne.

Nogle cyberkriminelle udfører også Distributed Denial of Service-angreb (DDoS-angreb), som er en form for overbelastningsangreb, når de i forbindelse med deres afpresningsangreb kombinerer forskellige afpresningsteknikker. For eksempel bliver der ved nogle afpresningsangreb både stjålet data, anvendt kryptering samt udført DDoS-angreb mod offerets kundevendte services, der derfor ikke kan tilgås. Formålet med at kombinere afpresningsteknikkerne er at øge presset på offeret og dermed sandsynligheden for, at offeret betaler løsesummen.

DDoS-angreb har tidligere også været brugt som selvstændig afpresningsmetode blandt cyberkriminelle. SAMSIK vurderer dog, at det er mindre anvendt i dag.

Telesektorens systemer og data er eftertragtede
Nogle cyberkriminelle har specialiseret sig i at bryde ind i organisationers netværk for at sælge adgange og eventuelle data videre på digitale undergrundsmarkeder. Denne slags hackere forsøger bl.a. også at kompromittere organisationer i telesektoren verden over.

Hvis hackerne får adgang til en teleudbyders netværk, kan de f.eks. sælge adgangen videre til en ransomware-gruppe, som kan bruge dem i et ransomware-angreb. De kan også sælge adgangen videre til kriminelle, der ønsker at udføre SIM Swapping. Her udnytter cyberkriminelle adgangen til en teleudbyders netværk til at få kontrol over telefonnumre. Derefter kan numrene bl.a. bruges til at afsende phishing eller til at omgå flerfaktorautentifikation.

Kriminelle hackere kan også forsøge at sælge adgange og data videre til statslige hackergrupper, som f.eks. kan bruge dem til cyberspionage.

Dansk teleudbyder udsat for datakompromittering via leverandør

En dansk teleudbyder meddelte i juni 2023, at en af deres leverandører havde været udsat for et cyberangreb. Ifølge udbyderen betød angrebet, at hackerne fik adgang til leverandørens kopi af udvalgt kundedata, herunder navn, adresse, telefonnummer, ip-adresse og cpr-nummer fra i alt 6.625 kundenumre.

Kriminelle hackere forsøger at svindle organisationer via mail
En anden form for cyberkriminalitet, som tidligere har ramt telesektoren i Danmark, er Business E-mail Compromise (BEC-svindel). Ved denne type svindel forsøger kriminelle at franarre organisationer penge via falske anmodninger om pengeoverførsler.

BEC-svindel er ofte effektivt og leder løbende til store økonomiske tab verden over. Det skyldes, at de kriminelle bagmænd målretter deres anmodninger og får anmodningerne til at fremstå mere troværdige på baggrund af grundig research. Bagmændene kan bl.a. øge anmodningernes troværdighed ved at inkludere organisationsspecifikke oplysninger, som de har fundet på internettet, eller ved at kompromittere en mailkonto og dernæst fremsende anmodningerne i eksisterende mailtråde.

Cyberspionage

Truslen fra cyberspionage mod den danske telesektor er **HØJ**.

SAMSIK hæver dermed trusselsniveauet fra **MIDDEL** til **HØJ**, og det er nu sandsynligt, at den danske telesektor vil blive udsat for forsøg på cyberspionage.

Trusselsniveauet hæves, fordi der de seneste par år har været flere forsøg på cyberspionage mod den europæiske telesektor. SAMSIK vurderer, at aktiviteten er udtryk for en øget interesse for telesektoren i Europa fra statslige hackere, hvilket øger truslen mod den danske telesektor.

Fremmede stater anvender løbende deres cyberkapaciteter til at udføre cyberspionage mod telesektoren verden over og har gjort det i en årrække. Det gælder især Kina, men også stater som Rusland og Iran. Tidligere har cyberspionagen især været rettet mod teleudbydere i Asien og Mellemøsten, men nu rettes den altså i højere grad også mod teleudbydere i Europa.

Formålet med fremmede staters cyberspionage mod telesektoren er typisk at få adgang til udbydernes kundedata. Formålet kan dog f.eks. også være at forberede destruktive cyberangreb.

Hvad er cyberspionage?

Cyberspionage er en spionageform, hvor modstanderen via cyberangreb stjæler informationer fra IT-systemer, elektroniske enheder, software eller internettjenester såsom mail eller sociale medier.

Telesektorens kundedata er et attraktivt spionagemål for fremmede stater
Det er meget sandsynligt, at fremmede stater generelt anser telesektoren for at være et attraktivt cyberspionagemål. Det skyldes især, at de via cyberspionage mod tele- og internetudbydere kan få adgang til store mængder data om kunders brug af udbyderens infrastruktur, herunder opkaldsdata, internettrafik, kundedata og lokationsdata. SAMSIK vurderer, at det vil være det primære formål med eventuel cyberspionage mod danske udbydere.

Stater er bl.a. interesserede i den type data, fordi den kan bruges til at overvåge enkeltpersoners eller befolkningsgruppers kommunikations- og rejseaktivitet. Eksempelvis forsøger Kina løbende at overvåge den kinesiske diaspora generelt og især dissidenter, herunder fra mindretal som uighurer og tibetanere. En af måderne, Kina gør det på, går gennem brugen af cyberspionage mod telesektoren.

Derudover kan stater bruge stjålne kundedata fra telesektoren til at iværksætte yderligere spionage mod de kunder, de finder interessante. Det kunne f.eks. være teknisk aflytning af telefonnumre tilhørende politikere eller systemkritikere i udlandet, som staten måtte have en interessere i at følge og spionere imod.

Endelig er nogle tele- og internetudbydere – udover at være leverandører af tele- og internettjenester – også leverandører af datacentre og cloud-løsninger. Disse tele- og internetudbydere kan også blive interessante spionagemål for statslige hackere, hvis hackerne f.eks. vurderer, at udbyderne potentielt opbevarer information, som fremmede stater har interesse i at få adgang til.

Såfremt hackere får adgang til kundedata, kan det få alvorlige konsekvenser for de kompromitterede tele- og internetudbydere. Dels direkte i form af bøder, men også indirekte, såfremt cyberangrebet f.eks. svækker kunders og investorers tillid til udbyderen og derved medfører økonomiske tab.

Kinesiske hackere fik adgang til sensitive data via teleudbydere

Amerikanske cybersikkerhedsmyndigheder og medier har siden oktober 2024 beskrevet, hvordan kinesiske hackere har kompromitteret flere amerikanske teleselskaber. Formålet har ifølge amerikanske myndigheder været at muliggøre yderligere spionage mod teleudbydernes kunder. Blandt andet er det lykkedes hackerne at stjæle opkaldsdata samt at få adgang til privat kommunikation tilhørende udvalgte kunder. Desuden fik de i nogle tilfælde også adgang til data, der var indsamlet som følge af en retskendelse. Ifølge New York Times var den amerikanske præsident og vicepræsident, Donald Trump og J.D. Vance, blandt de kunder hos teleselskaberne, som var berørt af hændelsen. Det samme var dele af tidligere vicepræsident og præsidentkandidat Kamala Harris' stab.

Repræsentanter fra USA's sikkerhedstjeneste, National Security Agency, oplyste på et pressemøde i december 2024, at de kinesiske hackere, som står bag kompromitteringer af teleudbydere i USA, også har kompromitteret teleudbydere i bl.a. Europa og Sydøstasien.

Cyberspionage kan muliggøre destruktive angreb

Udover at få adgang til tele- og internetudbyderes kundedata kan fremmede stater også bruge cyberspionage mod telesektoren til at forberede destruktive cyberangreb eller fysisk sabotage. For eksempel vurderer SAMSIK, at en del af cyberspionagen fra russiske statslige hackere mod kritisk infrastruktur i Danmark har til formål at forberede destruktive cyberangreb.

Forberedelsen af destruktive angreb kan bl.a. bestå i kortlægning og indsamling af teknisk viden om udbyderes infrastruktur samt etablering af bagdøre i it-systemer. Derved får de statslige hackere bedre mulighed for at udføre destruktive cyberangreb mod deres mål med kort eller uden varsel, såfremt en stat skulle få intention herom.

Selvom cyberspionage således kan understøtte destruktive cyberangreb eller fysisk sabotage, er det dog ikke en forudsætning for alle destruktive cyberangreb. Hackere kan i nogle tilfælde udføre simple, destruktive cyberangreb mod systemer med dårlig beskyttelse med begrænset forberedelse.

Kinesisk cyberspionage skulle forberede destruktive cyberangreb

Cybersikkerhedsmyndigheder fra USA, Storbritannien, Canada, Australien og New Zealand advarede i februar 2024 om, at kinesiske hackere havde forsøgt at kompromittere organisationer i kritiske sektorer i USA. Blandt målene var organisationer i telesektoren. Ifølge myndighederne var det primære formål med angrebet at muliggøre destruktive cyberangreb i tilfælde af en større krise eller konflikt med USA. Hackerne forsøgte bl.a. at få adgang til IT-netværk, hvorfra det var muligt at sprede sig til organisationernes OT-netværk. Dermed ville hackerne kunne iværksætte destruktive angreb mod kritiske systemer, såfremt Kina skulle få intentioner herom.

Fremmede stater er interesserede i teknologier og intellektuel ejendom
Organisationer i den danske telesektor kan også blive attraktive spionagemål for stater, hvis de udvikler eller anvender moderne teknologi, eller hvis de har viden og intellektuel ejendom, som kan bruges til at fremme staters økonomiske interesser eller teknologiske udviklingsmål.

Særligt Kina anvender cyberspionage til at stjæle sensitive teknologiske hemmeligheder fra andre stater, herunder bl.a. viden om informations- og kommunikationsteknologi. I januar 2024 tiltalte amerikanske myndigheder eksempelvis syv kinesiske statsborgere for bl.a. at have udført økonomisk motiveret cyberspionage mod amerikanske mål på vegne af den kinesiske efterretningstjeneste, Ministeriet for Statssikkerhed. Ifølge anklagen var spionagen bl.a. rettet mod mål i telesektoren, heriblandt en førende leverandør af 5G-netværksudstyr.

Derudover er der også eksempler på, at stater har udført cyberspionage i forbindelse med indgåelsen af internationale økonomiske aftaler og investeringer.

Netværksudstyr angribes løbende af hackere
Routere og andet netværksudstyr er løbende udsat for forsøg på kompromittering fra både statslige og ikke-statslige hackere. Det gælder især routere, som udleveres af tele- og internetudbydere til kunder. Det skyldes blandt andet, at hackerne kan udnytte enhederne til flere forskellige formål, herunder som en del af botnet eller som en indledende angrebsvektor i cyberangreb mod både kunders og udbyderens netværk. Derudover er enhederne ofte mere sårbare og dermed nemmere at kompromittere end almindelige computere.

Selvom netværksudstyret er placeret ved teleudbydernes kunder, spiller teleudbydere oftest den afgørende rolle i beskyttelsen af enhederne. Det skyldes, at det typisk er udbyderne, der administrerer enhederne og bl.a. foretager sikkerhedsopdateringer.

Hackere anvender mange forskellige metoder til at kompromittere routere og andet netværksudstyr, herunder via brute force-angreb samt udnyttelsen af både kendte og ukendte sårbarheder. Hvilken metode, der anvendes, afhænger af det enkelte produkt, herunder dets design og opsætning.

Kinesiske hackere brugte routere i Frankrig til at skjule aktiviteter

Den franske cybersikkerhedsmyndighed ANSSI offentliggjorde i 2021, at hackergruppen APT31 havde kompromitteret et meget stort antal routere i Frankrig. Routerne var af en type, der hovedsageligt blev anvendt i hjemmet eller på mindre kontorer. Ifølge rapporten om hændelsen var et af hovedformålene med kompromitteringen at samle de kompromitterede routere i et botnet, som kunne bruges til at udføre cyberaktiviteter i det skjulte. EU har tidligere attribueret spionageaktiviteter fra APT31 til Kinas territorium.

Leverandører i udlandet kan udgøre en sikkerhedsrisiko

SAMSIK vurderer, at brugen af tele- og netværksudstyr samt driftsydelser fra lande, som Danmark ikke har et sikkerhedsmæssigt samarbejde med, kan udgøre en større sikkerhedsrisiko end brugen af udstyr fra lande, som Danmark samarbejder med. Det skyldes blandt andet, at nogle stater har mulighed for at pålægge virksomheder at bistå landets efterretningstjenester.

For eksempel gør Kinas efterretningslov fra 2017 det muligt for Kinas efterretningstjenester at kræve, at kinesiske virksomheder samarbejder med dem. Efterretningstjenesterne kan dermed pålægge kinesiske virksomheder at overdrage eventuelle systemadgange, data eller viden om de systemer, de måtte have legitim adgang til som leverandører. Disse adgange og oplysninger vil potentielt kunne udnyttes som led i bl.a. cyberspionage eller destruktive cyberangreb.

Selvom brugen af udstyr fra lande, som Danmark ikke har et sikkerhedsmæssigt samarbejde med, kan udgøre en større sikkerhedsrisiko, er det ikke ensbetydende med, at de ikke kan anvendes. Der kan nemlig være situationer, hvor risiciene ved brug af udstyret er acceptable. Blandt andet derfor skal brugen af udstyr, i henhold til lovgivningen på teleområdet, altid bero på en risikovurdering.

Cyberaktivisme

Truslen fra cyberaktivisme mod den danske telesektor er **HØJ**.

Det er meget sandsynligt, at den danske telesektor vil blive ramt af cyberaktivistiske angreb. Truslen kommer især fra pro-russiske cyberaktivister, der løbende udfører DDoS-angreb mod Danmark og andre europæiske NATO-lande. Angrebene rammer hjemmesider på tværs af kritiske sektorer, herunder telesektoren, og udføres i et sådant omfang, at de er blevet en del af normalbilledet.

Hvad er cyberaktivisme?

Cyberaktivisme er cyberangreb begået af grupper eller individer med det formål at skabe opmærksomhed omkring en dagsorden eller et budskab. Aktivisterne er typisk drevet af ideologiske eller politiske motiver og kan både fokusere på enkeltsager, personer eller organisationer, de anser som modstandere af deres sag.

DDoS-angreb skal signalere støtte til Ruslands krig mod Ukraine
Pro-russiske cyberaktivister retter løbende angreb mod mål i Danmark og andre europæiske NATO-lande i kontekst af spændingerne mellem Rusland og Vesten. Formålet er at straffe lande, der leverer støtte til Ukraine, for derved at skabe opmærksomhed om deres sag samt signalere opbakning til Ruslands krig mod Ukraine. I den sammenhæng udgør danske organisationer et mål bl.a. på grund af den fremtrædende rolle, Danmark spiller i forhold til støtten til Ukraine.

De fleste angreb fra de pro-russiske cyberaktivister er DDoS-angreb rettet mod hjemmesider og tilhørende services. Denne form for overbelastningsangreb er relativt simple at udføre og har typisk kun en forstyrrende effekt, såfremt systemer overbelastes og gøres midlertidigt utilgængelige. Angrebene er dog effektive i forhold til aktivisternes hensigt med angrebene, da forstyrrelserne skaber opmærksomhed.

Cyberaktivisterne forsøger løbende at øge chancerne for, at deres DDoS-angreb lykkes. Det gør de bl.a. ved at variere i måden, de udfører angrebene, eller ved at kombinere forskellige former for DDoS-angreb. SAMSIK har f.eks. set cyberaktivistiske grupper forsøge at overbelaste både netværkslaget og webapplikationen på samme tid.

Telesektoren er udsat for en direkte og indirekte DDoS-trussel
Selvom telesektoren nogle gange er mål for DDOS-angreb fra pro-russiske cyberaktivister, er det ikke telesektorens hjemmesider, der oftest bliver ramt. Det gør særligt hjemmesider i finans- og transportsektoren.

En af årsagerne er sandsynligvis, at finanssektoren og transportsektoren har mange brugervendte hjemmesider med et stort antal brugere. Cyberaktivisterne vurderer derfor sandsynligvis, at disse hjemmesider er mere oplagte mål at gøre utilgængelige i forhold til at skabe den opmærksomhed, de ønsker.

Danske teleudbydere kan imidlertid også blive påvirket indirekte af DDoS-angreb mod mål i andre sektorer, såfremt disse er kunder hos udbyderen, og udbyderens infrastruktur overbelastes af angrebet. Telesektoren udgør således både et direkte og indirekte mål for pro-russiske aktivisters DDoS-angreb.

Cyberaktivisme kan være andet end DDoS
Selvom det primært er DDoS-angreb, der fylder i trusselsbilledet, udfører nogle cyberaktivister også andre former for cyberangreb.

For eksempel har enkelte pro-russiske cyberaktivister også udført simple og opportunistiske destruktive cyberangreb mod mål i vestlige lande. Omfanget af disse angreb er dog begrænset sammenlignet med de mange DDoS-angreb, som rammer mål i Danmark og Vesten, og angrebene har primært også været rettet mod mål med lav beskyttelse. Blandt andet derfor vurderer SAMSIK, at truslen fra destruktive, cyberaktivistiske angreb er mindre relevant for telesektoren.

Cyberaktivister overdriver for at skabe opmærksomhed

Aktivistiske hackeres kommunikation omkring deres angreb er ofte misvisende og overdreven. Dette betyder, at der i mange tilfælde er usikkerhed om, hvorvidt cyberaktivistiske angreb har fundet sted, samt hvilken effekt angrebene har haft. SAMSIK vurderer, at aktivisters kommunikation om både falske og reelle angreb har til hensigt at skabe offentlig opmærksomhed omkring deres dagsorden. De cyberaktivistiske grupper søger således omtale i vestlige medier og deler vestlige, herunder danske, mediers artikler om gruppernes angreb.

Selvom SAMSIK er bekendt med gruppernes navne, bliver de derfor ikke nævnt i publikationer, medmindre det er afgørende for at give et retvisende trusselsbillede.

Udover at udføre destruktive cyberangreb er der også nogle cyberaktivister, som udfører defacement-angreb og hack og læk-angreb. Ved defacement-angreb ændrer hackerne en hjemmesides visuelle udtryk eller indhold og forsøger derved at sende et specifikt budskab. Ved hack og læk-angreb forsøger hackerne at stjæle data fra en person eller organisation og derefter lække det med henblik på at sende et bestemt budskab eller skade offerets omdømme. Hackerne kan f.eks. lække sensitive oplysninger såsom interne dokumenter, forretningshemmeligheder eller personfølsomme oplysninger.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod den danske telesektor er **MIDDEL**.

Truslen kommer især fra Rusland og retter sigt bredt mod organisationer i samfundsvigtige sektorer i Danmark. Truslen er således også rettet mod telesektoren.

Truslen gælder primært mindre omfattende destruktive cyberangreb, idet det fortsat er mindre sandsynligt, at Rusland i den nuværende sikkerhedspolitiske situation vil gennemføre destruktive cyberangreb, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.

Selv mindre omfattende angreb kan dog få betydelige konsekvenser for både samfundet og det enkelte offer. Det skyldes, at store dele af samfundet er afhængige af de tjenester, som telesektoren leverer. Destruktive cyberangreb med mindre omfattende konsekvenser kunne f.eks. være, hvis kunders adgang til tele- og internettjenester påvirkes i begrænset omfang, eller hvis angrebet medfører økonomiske omkostninger eller skaber generel utryghed uden at påvirke samfundsvigtige funktioner.

Hvad er destruktive cyberangreb?

Destruktive cyberangreb er cyberangreb, hvor formålet er at forandre informationer, data eller software, så de ikke kan genskabes, eller så det medfører skade på fysiske objekter og mennesker. Destruktive cyberangreb kan f.eks. bruges til påvirke kritisk it-infrastruktur, der understøtter samfundsvigtige funktioner

Ruslands risikovillighed er øget

Rusland har længe haft kapacitet til at udføre destruktive cyberangreb mod Danmark. Siden starten af 2024 har Rusland dog udvist større risikovillighed i forhold til at bruge hybride virkemidler med destruktive effekter mod europæiske NATO-lande. SAMSIK vurderer, at den øgede risikovillighed også omfatter brugen af destruktive cyberangreb.

Skulle organisationer i Danmark blive ramt af et destruktivt cyberangreb fra Rusland, vil formålet sandsynligvis være at påvirke befolkningen eller beslutningstagere, herunder at svække danskernes opbakning til Ukraine. Formålet vil således primært være at skabe opmærksomhed, mens den konkrete effekt vil være mindre vigtig.

Denne opmærksomhed kan Rusland opnå ved at udføre destruktive cyberangreb mod mange forskellige organisationer. Truslen er derfor ikke kun rettet mod Ukraine-relaterede mål, men bredt rettet mod organisationer i Danmarks samfundsvigtige sektorer inkl. telesektoren. Telesektoren har f.eks. en stor synlighed i Danmark, idet sektoren spiller en afgørende rolle i forhold til at levere sikker og effektiv kommunikation i et yderst digitaliseret samfund.

Hvorvidt organisationer udvælges som mål for et eventuelt destruktivt cyberangreb, vil også afhænge af andre forhold. Eksempelvis vil det sandsynligvis også afhænge af, om hackerne allerede har adgang til udbydernes netværk, eller hvor de nemt kan få det.

Ruslands hybride virkemidler

Destruktive cyberangreb er et af flere hybride virkemidler, som Rusland har til rådighed. Virkemidlerne dækker over metoder og kapaciteter af politisk, informationsmæssig, militær og økonomisk karakter og omfatter udover cyberangreb bl.a. også evnen til at jamme radiosignaler samt til at udføre sabotage mod kritisk infrastruktur. Såfremt Rusland gør brug af denne type angreb, vil det – i lighed med destruktive cyberangreb – kunne få konsekvenser for teleudbyderes tjenester.

Rusland anvender generelt hybride virkemidler mere systematisk, omfattende og aggresivt end noget andet land i verden. Formålet er at udnytte virkemidler, der ligger under tærsklen for væbnet konflikt, til at svække Vestens modstandskraft samt evne til at træffe effektive beslutninger. På den måde kan Rusland drage strategiske fordele uden at udløse en militær konflikt med NATO.

I Europa har der i 2024 været flere eksempler på angreb med hybride virkemidler mod civile mål, herunder offensive efteretningsoperationer, brandstiftelse, hærværk og desinformation. Desuden har flere lande officielt meldt ud, at Rusland står bag en række cyberangreb mod landene.

Omfattende DDoS-angreb kan påvirke samfundet

Ruslands øgede risikovillighed kan udover mindre omfattende destruktive cyberangreb også komme til udtryk i form af omfattende DDoS-angreb. Disse angreb kunne f.eks. blive rettet mod systemer i telesektoren eller hos telesektorens kunder.

DDoS-angreb er, som tidligere nævnt, ikke destruktive i sig selv, men kan alligevel afbryde eller forstyrre samfundsvigtige funktioner, hvis angrebene er tilstrækkeligt omfattende, eller forsvaret imod dem er utilstrækkeligt. Angrebene vil således også kunne påvirke befolkningen og beslutningstagere i lighed med destruktive cyberangreb.

Truslen fra alvorlige og omfattende angreb kan stige

Selvom det aktuelt er mindre sandsynligt, at Rusland vil udføre alvorlige og omfattende destruktive cyberangreb mod Danmark, vurderer SAMSIK, at statslige russiske hackergrupper udfører cyberspionage mod kritisk infrastruktur i Danmark for at forberede denne type angreb.

Truslen fra destruktive cyberangreb, hvor hensigten er at skabe alvorlige og omfattende konsekvenser, kan derfor stige med kort eller uden varsel, hvis Ruslands risikovillighed øges yderligere. Det kunne f.eks. ske, hvis den sikkerhedspolitiske situation eskalerer i retning af en militær konflikt mellem Rusland og NATO.

I forbindelse med Ruslands krig mod Ukraine er tele- og internetudbydere i både Rusland og Ukraine blevet ramt af destruktive cyberangreb. Angrebene viser dels, hvordan destruktive cyberangreb kan bruges til at destabilisere modstanderens samfund og øge

krigsomkostningerne. Men også hvordan angrebene kan understøtte kampen på slagmarken. Sidstnævnte var f.eks. tilfældet ved Ruslands destruktive cyberangreb mod satellit-udbyderen Viasat på dagen for den russiske invasion. Angrebet skulle bl.a. forstyrre Ukraines militærs evne til at kommunikere.

Krigen mellem Rusland og Ukraine har også understreget, at det især er wiper-angreb, som anvendes i forbindelse med destruktive cyberoperationer. Angrebene sletter, overskriver eller krypterer data, så systemer ikke virker og er svære at genskabe.

Destruktivt cyberangreb mod Ukraines største teleudbyder

Ukraines største teleudbyder, Kyivstar, blev den 12. december 2023 ramt af et destruktivt cyberangreb. Angrebet efterlod en stor del af selskabets 24 millioner kunder uden adgang til mobilnet i flere dage og påvirkede bl.a. varslingssystemer for missiler og hæveautomater. Ukraines sikkerheds- og efterretningstjeneste har meldt ud, at Ruslands mililtære efterretningstjeneste stod bag angrebet, nærmere bestemt hackergruppen Sandworm.

Andre aktører udgør også en potentiel trussel

Selvom truslen fra destruktive cyberangreb især kommer fra Rusland, er der også en potentiel trussel fra andre stater. For eksempel er det sandsynligt, at hackergrupper fra Iran har udført destruktive cyberangreb mod vestlige mål.

Derudover kan der også være en trussel fra ikke-statslige hackere. Det skyldes blandt andet, at stater kan forsøge at sløre deres involvering i et destruktivt cyberangreb ved at få kriminelle eller aktivistiske hackere til at udføre angrebene for dem.

Samtidig vurderer SAMSIK som beskrevet, at visse cyberaktivistiske grupper har intentioner om at udføre cyberangreb med destruktiv effekt. For eksempel blev et mindre dansk vandværk i slutningen af 2024 ramt af et destruktivt cyberangreb fra prorussiske cyberaktivister. Ved angrebet blev vandværkets operationelle systemer manipuleret, hvilket bl.a. medførte, at flere husstande var uden vand i en kortere periode.

Det er dog kun i få tilfælde, at en reel effekt fra et cyberaktivistisk destruktivt angreb er blevet bekræftet, og SAMSIK vurderer generelt, at aktivisternes evne til at udføre den type angreb er begrænset sammenlignet med fremmede staters. De udgør derfor primært en trussel mod organisationer med svage sikkerhedsforanstaltninger.

Cyberterror

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

Det er usandsynligt, at den danske telesektor vil blive udsat for forsøg på cyberterror på kort sigt.

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

Denne slags cyberangreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Samtidig er ekstremisternes hensigt om at udføre denne form for angreb mod Danmark yderst begrænset.

Hackernes angrebsmetoder

I dette afsnit beskrives nogle af de angrebsmetoder, som hackere anvender til at kompromittere deres ofre. Listen er ikke udtømmende, men indbefatter bl.a. de mest gængse angrebsvektorer samt de angrebstyper, SAMSIK vurderer, er særligt relevante for telesektoren. Flere af metoderne bruges både af cyberkriminelle og statslige aktører og har i nogle tilfælde været anvendt mod telesektoren i udlandet og i Danmark.

Phishing

SAMSIK vurderer, at phishing fortsat er en foretrukken angrebsmetode blandt hackere. Det illustreres bl.a. ved, at danske organisationer, herunder i telesektoren, løbende modtager phishing-mails og -beskeder.

Phishing er bl.a. attraktivt for hackerne, fordi det er billigt og skalerbart, men fortsat effektivt. Det skyldes, at phishing udnytter menneskelige svagheder til at få personer til at klikke på ondartede links eller filer for derved at installere malware eller franarre modtageren sine logininoplysninger. Denne type angreb kan derfor også være svære for organisationer at beskytte sig fuldstændigt imod.

Udbredelsen af generativ AI kan tilmed gøre phishing endnu sværere for medarbejdere at gennemskue, idet hackere kan misbruge teknologien til at lave mere detaljerede, fejlfrie mails – også på sprog, hackerne ikke selv behersker.

Angreb via leverandører

Leverandører, herunder især softwareleverandører og cloududbydere, er attraktive mål for både statslige og kriminelle hackere. Det skyldes, at leverandører ofte har særlige adgange til kunders systemer eller data, som hackerne kan misbruge.

Hackere har tidligere forsøgt at kompromittere leverandører for få adgang specifikke kunder, der var velbeskyttede og svære at kompromittere ad andre veje.

I takt med at teleinfrastruktur stigende grad rykkes i clouden, vil leverandørtruslen mod telesektoren sandsynligvis også stige.

Udnyttelse af sårbarheder

En anden form for angreb, som ofte benyttes af hackere, er udnyttelsen af sårbarheder i systemer, software og hardware.

Særligt sårbarheder, der f.eks. bliver offentliggjort i forbindelse med sikkerhedsopdateringer, er hackere hurtige til at udnytte. I nogle tilfælde er der f.eks. blot tale om minutter fra, at en sårbarhed offentliggøres, til at konkrete angrebsforsøg registreres.

Nogle hackere har også kapacitet til at identificere eller købe sig til såkaldte zero day sårbarheder. Disse sårbarheder er endnu ikke er kendte af leverandøren og kan derfor heller ikke mitigeres via en sikkerhedsopdatering. Angreb via zero day sårbarheder kan derfor være særligt svære at opdage og imødegå.

Flere stater har i mange år haft ressourcer til at identificere og købe sig til viden om zero day sårbarheder. Samtidig vurderer SAMSIK også, at flere kriminelle hackere investerer tid og ressourcer i at opdage eller købe sig til zero days. For eksempel udnyttede den cyberkriminelle hackergruppe, Cl0p, i maj 2023 en zero day i en filoverførsels-applikation til at angribe og afpresse et højt antal organisationer verden over. Blandt ofrene var bl.a. organisationer i telesektoren i udlandet.

Udnyttelse af svage eller kendte passwords

Simple angrebsmetoder som brute force-angreb er fortsat populære og effektive blandt hackere. Ved brute force-angreb forsøger hackere på forskellig vis at gætte brugernavne og passwords. Det kunne f.eks. være ved systematisk at gætte på forskellige kombinationer af tilfældige tegn på tværs af brugerkonti, men også ved at afprøve passwords fra datalæk eller standardpasswords.

Brute force-angreb kan udføres mod mange forskellige former for systemer og konti, herunder alt fra mailkonti til organisationers Virtual Private Network (VPN) løsninger samt fjernadgange via Secure Shell (SSH) og Remote Desktop Protocol (RDP).

Malvertising og vandhulsangreb

Ved malvertising bruger hackere online reklamer til at sprede malware. Ofte indsættes de malwareinficerede reklamer på ellers legitime hjemmesider. En typisk måde at udføre malvertising er f.eks. i tilbud om downloads af applikationer, herunder antivirusprogrammer.

En anden angrebsteknik, der udnytter hjemmesider, er vandhulsangreb. Her kompromitterer hackere legitime hjemmesider med malware. Brugere, der benytter hjemmesiden, risikerer således at blive inficeret. Ved et vandhulsangreb er hjemmesiden typisk udvalgt med henblik på at ramme specifikke eller mange besøgende. Hackere kan dog også overtage tilfældige hjemmesider, hvis de er nemme at kompromittere.

Insider-angreb

Medarbejdere med adgang til it-systemer, kundedata eller viden kan udgøre en potentiel insider-trussel, hvis de ubevidst eller bevidst udfører eller faciliterer cyberangreb eller svindel.

Der er f.eks. løbende eksempler på, at cyberkriminelle har forsøgt at snyde medarbejdere til at hjælpe dem i forbindelse med cyberangreb og svindel. Desuden forsøger kriminelle hackere også løbende at rekruttere virksomheders ansatte på digitale undergrundsmarkeder.

Brug af teleinfrastruktur

Nogle hackere har ved cyberangreb mod telesektoren i udlandet udvist omfattende teknisk forståelse for telesektorens infrastruktur og protokoller.

Cybersikkerhedsvirksomheden Crowdstrike har for eksempel beskrevet, hvordan statslige hackere har kompromitteret teleudbydere og anvendt telesektorspecifikke malware og protokoller som GTP til at kontrollere og kommunikere med de kompromitterede systemer. Brugen af Windows-systemer blev derved holdt på et minimum.

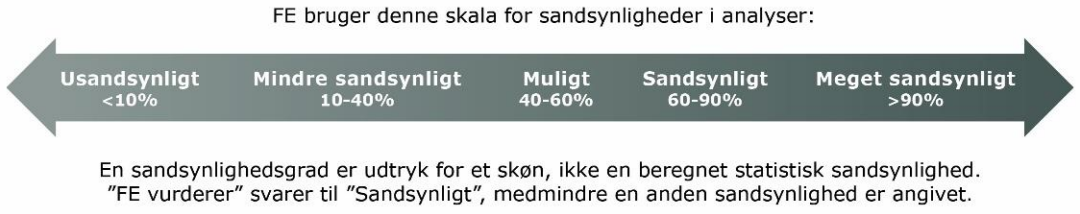
Eksemplerne understreger, at nogle cyberaktører råder over avancerede tekniske kapaciteter, som de kan tage i brug, hvis de vurderer det fordelagtigt i situationen.

Trusselsniveauer

Styrelsen for Samfundssikkerhed anvender i sine trusselsvurderinger Forsvarets Efterretningstjenestes (FE) trussels- og sandsynlighedsniveauer.
Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer:

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, eller en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for FE's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.



Andre relevante publikationer

Nedenfor fremgår en række af de publikationer, som kan være relevante for organisationer i den danske telesektor. Publikationerne kan tilgås på WWW.CFCS.DK.

Cybertruslen mod Danmark 2024
I denne årlige trusselsvurdering beskrives den generelle cybertrussel for hhv. cyberkriminalitet, cyberspionage, cyberaktivisme, destruktive cyberangreb og cyberterror mod Danmark.

Cybertruslen mod IoT-enheder
Trusselsvurderingen beskriver cybertruslen mod IoT-enheder, inkl. netværksudstyr, der ligesom almindelige it-systemer rammes af cyberangreb.

Anatomien af et målrettede ransomware-angreb
Denne rapport kortlægger, hvordan særligt målrettede ransomware-angreb typisk forløber, og giver konkrete anbefalinger til, hvordan myndigheder og virksomheder kan beskytte sig endnu bedre.

Et wiper-angrebs anatomi
Rapporten belyser, hvordan den klart mest udbredte type destruktive cyberangreb, wiper-angreb, fungerer, og hvordan du forsvarer dig imod dem.

Logning – en del af et godt cyberforsvar
Vejledningen giver gode råd til, hvor i netværket man skal logge og hvad man bør logge. Den bygger på erfaringer fra bl.a. it-sikkerhedsfirmaer i forbindelse med bistand ved hændelseshåndtering.

Vejledning om cybersikkerhed i leverandørforhold
Vejledningen "Cybersikkerhed i leverandørforhold" giver gode råd til, hvordan man kan oprette og bibeholde et godt samarbejde mellem kunden og leverandøren af it-driften, gennem hele samarbejdsperioden. Fra valg af leverandør til ophør af samarbejdet.

Vejledning om password-sikkerhed
Vejledningen beskriver nogle af de angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Vejledningen indeholder desuden en række konkrete anbefalinger til, hvordan man – på forskellige niveauer i en organisation – bør arbejde med password-sikkerhed.

Vejledning om at imødegå ransomware-angreb
Vejledningen "Reducér risikoen for ransomware" giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket.

Vejledning om at imødegå phishing-angreb
Vejledningen ”Beskyt din organisation mod phishing-angreb” hjælper organisationer med at imødegå truslen fra phishing-mails.

Vejledning om beskyttelse mod DDoS-angreb
Vejledningen ”Beskyt mod DDoS-angreb” kommer med en række forholdsregler, som en organisation kan tage for at beskytte sig mod DDoS-angreb.