CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod sundhedssektoren

Maj 2024

Indhold

CENTER FOR CYBERSIKKERHED

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

Maj 2024

Cybertruslen mod sundhedssektoren

Formålet med denne trusselsvurdering er at beskrive cybertruslen rettet mod den danske sundhedssektor. Vurderingen kan styrke risikoejeres forståelse af cybertruslen og bl.a. indgå som en del af grundlaget for risikovurderingsarbejdet i sektoren.

Vurderingen erstatter "Cybertruslen mod sundhedssektoren", der blev udgivet i 2018 og løbende er blevet opdateret.

Hovedvurdering

- Truslen fra cyberkriminalitet mod sundhedssektoren i Danmark er **MEGET HØJ**. Sundhedssektoren er et attraktivt mål for de cyberkriminelle, der for eksempel forsøger at afpresse deres ofre ved at kryptere data og systemer.

- Truslen fra cyberspionage mod sundhedssektoren i Danmark er **MEGET HØJ.** Det er meget sandsynligt, at fremmede stater har interesse i at stjæle data og oplysninger, der findes i sektoren.

- Truslen fra cyberaktivisme mod sundhedssektoren i Danmark er **HØJ**. Truslen kommer særligt fra pro-russiske aktivister, der fortsat udviser et højt aktivitetsniveau mod organisationer i NATO-lande.

- Truslen fra destruktive cyberangreb mod sundhedssektoren er **LAV**. Selvom fremmede stater har kapaciteten til at udføre destruktive cyberangreb, er det mindre sandsynligt, at de aktuelt har intention om at udføre angreb mod sundhedssektoren i Danmark.

- Truslen fra cyberterror mod sundhedssektoren i Danmark er **INGEN**.

Indledning

Sundhedssektoren i Danmark
Sundhedssektoren i Danmark består af mange forskellige typer af organisationer. I denne trusselsvurdering anses alle myndigheder og virksomheder, der direkte eller indirekte leverer sundhedsydelser, eller arbejder med regulering af området, som en del af sundhedssektoren. Det er for eksempel hospitaler, regioner, medicinalproducenter, praktiserende læger og tandlæger.

Der kan være myndigheder og virksomheder, som falder ind under denne definition af sundhedssektoren, men som primært er en del af en af de andre samfundskritiske sektorer. Det kan f.eks. være en transportvirksomhed, der primært leverer varer til sundhedssektoren. Her kan man med fordel også orientere sig i andre relevante trusselsvurderinger på cfcs.dk

Der er en alvorlig cybertrussel mod sundhedssektoren i Danmark. Det har der været siden Center for Cybersikkerhed (CFCS) udgav sin første trusselsvurdering for sektoren i 2018.

Det betyder ikke, at trusselsbilledet er uændret. Siden den første trusselsvurdering udkom, er trusselsbilledet kun blevet mere komplekst. Det skyldes blandt andet, at de ondsindede aktører hele tiden udvikler sig i forhold til både organisering og metoder. Selvom trusselsniveauerne i dette produkt er de samme som for Danmark generelt, er de specifikt baseret på en analyse af trusselsbilledet for sundhedssektoren.

Sundhedssektoren i Danmark udvikler sig også. Den bliver løbende mere digital og mere forbundet, både nationalt og internationalt. Forbundenhed og digitalisering skaber nye muligheder for sundhedssektoren. Det skaber dog også nye angrebsflader, som kan udnyttes i cyberangreb.

COVID-19-pandemien betød, at der var et stort fokus på cyberspionage og cyber-kriminalitet rettet mod sundhedssektoren. Mange stater havde for eksempel interesse i at følge med i vaccineudviklingen rundt omkring i verden. Blandt andet har USA, Canada og Storbritannien anklaget Kina og Rusland for at udføre cyberspionage mod COVID-19-forskning. Internationalt var sundhedssektorerne samtidig blandt de sektorer, der oftest blev ramt af angreb fra cyberkriminelle.

Der er dog ikke noget, der tyder på, at afslutningen på pandemien har betydet en ende på hackernes interesse for sundhedssektoren. Truslen fra cyberspionage og fra cyberkriminalitet er således stadig **MEGET HØJ**

CFCS vurderer, at truslen fra cyberaktivisme mod sundhedssektoren i Danmark er **HØJ.** Det er blevet en del af normalbilledet, at pro-russiske aktivister angriber myndigheder og virksomheder i NATO-lande, primært i kræft af overbelastnings-angreb.

Krigen i Ukraine har også medført et fornyet fokus på truslen fra destruktive cyberangreb. CFCS vurderer imidlertid, at truslen fra destruktive cyberangreb mod sundhedssektoren i Danmark er **LAV**.

Trusselsvurderingen bygger på CFCS' samlede vidensgrundlag fra ind- og udland, og har en varslingshorisont på to år. Vurderingen anvender de trusselniveauer og sand-synlighedsgrader, der er forklaret sidst i trusselsvurderingen.

Cyberkriminalitet

CFCS vurderer, at truslen fra cyberkriminalitet mod den danske sundhedssektor er **MEGET HØJ**. Det er meget sandsynligt, at myndigheder, virksomheder eller leverandører i sektoren vil blive udsat for forsøg på cyberkriminalitet inden for de næste to år.

Det er mange forskellige typer af cyberkriminalitet, som kan ramme sundhedssektoren i Danmark. For de cyberkriminelle handler det om at tjene penge, og ofte involverer det en eller anden form for afpresning. Der er også cyberkriminelle, der forsøger at sælge oplysninger, som de har fået uberettiget adgang til.

I sundhedssektoren er der store mængder af værdifulde data. Det kan være medvirkende til, at en organisation i sektoren kommer i de kriminelles søgelys. Det kan bl.a. være person- og sundhedsdata, forskningsresultater eller forretningshemmeligheder, som de kriminelle ønsker at få adgang til.

Nogle cyberkriminelle grupper har tilkendegivet, at de af etiske grunde ikke vil angribe mål i sundhedssektoren. Der er dog ikke noget, der tyder på, at de cyberkriminelle generelt afholder sig fra det. Uanset typen så er det meste cyberkriminalitet fortsat opportunistisk af natur. De cyberkriminelle angriber for økonomisk vindings skyld uden hensyn til hvem eller hvad, de rammer.

Tyske hospitaler angrebet af cyberkriminelle

Juleaftensdag 2023 blev Katholische Hospitalvereinigung Ostwestfalen (KHO), der administrerer en række hospitaler i Tyskland, ramt af et cyberangreb. Ifølge KHO var der tale om et ransomware-angreb, hvor data var blevet krypteret. Det betød, at tre hospitaler under KHO ikke kunne bruge flere af deres IT-systemer, og ikke kunne modtage akutpatienter, der måtte omdirigeres til andre hospitaler.

Afpresning og dobbelt afpresning

I forbindelse med ransomwareangreb er der mange eksempler på, at kriminelle bruger dobbeltafpresning for at få penge ud af offeret, når de har krypteret systemer eller data. Det betyder, at de kræver betaling for at udlevere dekrypteringsnøglen, og samtidig truer med at lække data, hvis de ikke bliver betalt. I sundhedssektoren kan det være meget følsomme patient- eller forskningsoplysninger, som de kriminelle truer med at offentliggøre, hvilket yderligere er med til at øge presset på den ramte organisation.

Hvad er et ransomware angreb?

I ransomware-angreb forsøger kriminelle at afpresse offeret ved at gøre deres data, systemer eller begge dele utilgængelige. Det gør de ofte ved at kryptere data eller systemer. De kriminelle kræver så en løsesum, typisk i form af kryptovaluta, for at gøre data eller systemer tilgængelige igen.

Der er også eksempler på, at cyberkriminelle afpresser organisationer uden at kryptere data eller systemer. Her truer de typisk med at videresælge eller offentliggøre den data, de har fået adgang til. Kriminelle kan også bruge oplysningerne til at afpresse enkeltpersoner direkte. Det kan være en ekstra indtjeningskilde og en måde at øge presset på den organisation, der er blevet ramt.

Vastaamo – flere variationer af afpresning

Flere medier har beskrevet, hvordan en hacker i 2020 fik adgang til en stor mængde patientjournaler fra den finske virksomhed Vastaamo. Der var bl.a. tale om journaler fra psykologsamtaler, hvor meget følsomme emner blev beskrevet. Ifølge medierne forsøgte hackeren først at afpresse virksomheden. Da det ikke lykkedes, lækkede hackeren patientjournalerne for at øge presset på virksomheden. Da det heller ikke virkede, begyndte hackeren at tage kontakt til de patienter, hvis journaler der var adgang til. Her blev patienterne truet med, at deres oplysninger om psykologiske problemer, familieforhold osv. ville blive offentliggjort, hvis ikke de betalte.

I 2023 afsluttede finsk politi efterforskningen af en 26-årig mands rolle i sagen. Sagen er videregivet til den finske anklagemyndighed.

Cyberkriminalitet og Internet of Things-enheder (IoT-enheder)
CFCS vurderer, at cybertruslen mod Internet of Things-enheder (IoT-enheder) er **MEGET HØJ.** Der er tale om en generel trussel, som ikke er rettet specifikt mod sundhedssektoren i Danmark.

Truslen er særligt aktuel for de organisationer i sundhedssektoren, som bruger IoT-enheder i forbindelse med f.eks. forskning eller behandling. Der har i Danmark været enkelte eksempler på, at medico-udstyr med internetforbindelse er blevet ramt af malware. CFCS vurderer dog, at det ikke har været målrettet udstyret.

Hvad er IoT-enheder?

IoT-enheder er en samlebetegnelse for alle enheder, der forbindes til internettet. Det kan f.eks. være enheder, der kobles til internettet for at sende eller modtage data mellem en patient og et behandlingstilbud. Begrebet dækker i denne trusselsvurdering ikke over almindelige computere, servere eller telefoner. Det dækker heller ikke operationelle teknologier som f.eks. industrielle kontrol-systemer.

Kriminelle hackere bruger bl.a. kompromitterede IoT-enheder til at tjene penge. De kan f.eks. bruge enhederne i såkaldte botnet til at generere kryptovaluta eller til at udføre DDoS-angreb mod betaling. De kan også bruge kompromitterede enheder som indledende adgang til f.eks. ransomware-angreb.

Mange IoT-enheder indeholder kendte sårbarheder, som ikke er blevet lukket via sikkerhedsopdateringer. Det udnytter de cyberkriminelle. Det betyder også, at truslen kan være forhøjet mod soft- eller hardware, der ikke længere opdateres af leverandøren eller udvikleren.

Truslen fra leverandørangreb
Cyberkriminelle angriber også gennem leverandører eller samarbejdspartnere. Denne type angreb kaldes supply chain-angreb. Det kan for eksempel ske ved, at der gemmes malware i en opdatering, som leverandøren utilsigtet distribuerer til sine kunder. Den specifikke type angreb kaldes også et software supply chain-angreb.

Mange organisationer i sundhedssektoren har et komplekst systemlandskab med mange forskellige leverandører. Det er også en sektor, hvor der er en høj grad af dataudveksling. Det kan være dataudveksling mellem en organisation i sundheds-sektoren og en leverandør, men også dataudveksling mellem to organisationer i sektoren i forbindelse med f.eks. patientbehandling. Det betyder, at der er mange led i kæden, som de kriminelle kan kompromittere.

Angreb fra cyberkriminelle kan påvirke organisationer, selvom de ikke bliver direkte kompromitteret. Hvis en leverandør eller samarbejdspartner er nødvendig for at tilgå data eller systemer, så kan angreb mod dem resultere i, at man som organisation ikke kan løse sine opgaver. For eksempel blev driften af et ikke-kritisk system i den danske sundhedssektor i 2023 påvirket af et ransomware-angreb mod en hostingleverandør.

Cyberspionage

CFCS vurderer, at truslen fra cyberspionage mod sundhedssektoren i Danmark er **MEGET HØJ**. Det er meget sandsynligt, at organisationer i sektoren vil blive udsat for forsøg på cyberspionage inden for de næste to år.

CFCS vurderer, at sundhedssektoren også på længere sigt vil være mål for spionage. Det skyldes blandt andet Danmarks position i forhold til udvikling og produktion af lægemidler samt de store mængder af personhenførbare oplysninger, der behandles i sektoren.

Hvad er cyberspionage?

Cyberspionage er en spionageform, hvor udefrakommende stjæler informationer fra it-systemer, elektroniske enheder, software eller internettjenester som for eksempel mail eller sociale medier. Cyberspionage udføres oftest af statslige eller statsstøttede aktører.

Cyberspionage er en delmængde af den samlede spionagetrussel mod Danmark. Den samlede spionagetrussel er beskrevet af Politiets Efterretningstjeneste i deres vurdering af spionagetruslen mod Danmark, Færøerne og Grønland.

Fremmede stater kan blandt andet bruge cyberspionage til at fremme egne økonomiske interesser og teknologiske udviklingsmål eller til at indsamle informationer om borgere og beslutningstagere. Cyberspionage kan også bruges som en trædesten for andre typer af cyberangreb eller andre typer spionage.

Truslen fra cyberspionage mod sundhedssektoren udspringer særligt fra Rusland og Kina. Det kan dog ændre sig, hvis andre stater får en konkret interesse i bestemte dele af den danske sundhedssektor.

CFCS vurderer, at den cyberspionage sundhedssektorer verden over udsættes for, ofte har til formål at styrke fremmede staters økonomiske og teknologiske interesser. Der er ofte tale om spionage rettet mod virksomheder og myndigheder, som er førende inden for deres felt. Der er blandt andet eksempler på, at ondsindede aktører har forsøgt at kompromittere medicinalvirksomheder og organisationer, der forsker i vacciner i Danmarks nærområde.

De store mængder af personoplysninger, der findes i nogle dele af sundhedssektoren, kan også være et attraktivt mål for cyberspionage. Oplysninger om enkeltpersoner kan bl.a. bruges til at finde og overvåge borgere, som fremmede stater har en særlig interesse i, til at rekruttere efterretningskilder, til målrettede påvirkningskampagner eller til andre former for spionage.

Det er meget sandsynligt, at statsstøttede hackere kompromitterer IoT-enheder i hele samfundet bl.a. med henblik på at bruge dem som indgangsvinkel for cyberspionage. For hackere, der ønsker at udføre cyberspionage, kan IoT-enheder være en relativt

nem vej ind i et netværk. Det skyldes de samme forhold, som gør IoT-enheder til et attraktivt mål for cyberkriminelle.

IoT-enheder kan også være et selvstændigt mål for cyberspionage fra fremmede stater. Netværksudstyr kan f.eks. være et interessant mål, fordi det kan give adgang til mails, filer og anden data, som sendes via enheden, hvis trafikken ikke er krypteret tilstrækkeligt. Overvågningskameraer kan også udgøre et mål for cyberspionage. Det gør sig f.eks. gældende, hvis kameraerne er opsat på en måde, så man via dem kan se informationer, som kan være af interesse for en fremmed stat.

En vedvarende kinesisk interesse

I løbet af de seneste år har der været adskillige eksempler på, at kinesiske hacker-grupper har udført cyberspionage mod sundhedssektorer flere steder i verden. Det er meget sandsynligt, at det både er grupper, der er direkte og indirekte tilknyttet staten, som udfører spionagen. Det er også sandsynligt, at spionagen mod sundhedssektorer i f.eks. Vesten blandt andet skyldes, at den kinesiske stat har et erklæret mål om at styrke og udvikle landets egen sundhedssektor.

Stjålet viden fra organisationer, der arbejder med bl.a. udvikling og forskning inden for sundhedsområdet, er med til at fremme den kinesiskes stats udviklingsmål og økonomiske interesser.

Det amerikanske justitsministerium har flere gange anklaget kinesiske hackere for på vegne af den kinesiske stat at stjæle forretningshemmeligheder fra virksomheder, herunder inden for sundhedsområdet, i hele verden.

USA anklager kinesiske hackere for at stjæle viden fra Vesten

I 2021 offentliggjorde det amerikanske justitsministerium en stævning mod fire kinesiske statsborgere. Ifølge stævningen har de mellem 2011 og 2018 forsøgt at hacke sig ind i IT-systemer ved universiteter, private virksomheder og statslige organisationer i USA og en lang række andre lande, herunder Tyskland, Østrig og Norge. Ifølge anklagerne har hackerne blandt andet forsøgt at få adgang til forskning i smitsomme sygdomme som f.eks. Ebola og MERS.

Cyberaktivisme

Truslen fra cyberaktivisme mod sundhedssektoren er **HØJ**, og det er sandsynligt, at virksomheder og myndigheder i sektoren vil blive udsat for cyberaktivistiske angreb inden for de næste to år.

DDoS-angreb mod Region Hovedstaden
I februar 2023 blev en række hospitalshjemmesider i Region Hovedstaden ramt af cyberaktivistiske overbelastnings-angreb. Det resulterede i, at en nødfunktion blev aktiveret, så hjemmesidebesøgende fik vist en fast startside med telefonnumre til alle regionens hospitaler.

Truslen fra cyberaktivisme har været **HØJ** siden januar 2023. Trusselsniveauet skyldes primært det høje aktivitetsniveau hos pro-russiske aktivistiske hackergrupper. Gruppernes aktivitet er hovedsageligt rettet mod NATO-lande, herunder Danmark, i forbindelse med krigen i Ukraine.

Cyberaktivisme er generelt drevet af forskellige ideologiske eller politiske motiver, der strækker sig fra politiske enkeltsager til modstand mod magthavere. Cyberaktivistiske angreb udføres derfor også som reaktion på enkelthændelser. Cyberaktivisme udføres af individer og grupperinger for at få mest mulig opmærksomhed til deres dagsorden eller for at straffe organisationer, som de anser som modstandere af deres sag.

Cyberaktivistiske hackere benytter sig oftest af DDoS-angreb mod hjemmesider. Det gør de sandsynligvis, fordi det er en type angreb, der ikke kræver avancerede tekniske færdigheder. Samtidig er det også en type cyberangreb, der tiltrækker opmærksomhed til aktivisternes dagsorden. Denne type angreb virker forstyrrende, men har ikke varige eller destruktive konsekvenser for ofrenes systemer.

Destruktive cyberangreb

CFCS vurderer, at truslen fra destruktive cyberangreb mod sundhedssektoren i Danmark er **LAV**, og at det er mindre sandsynligt, at sundhedssektoren vil blive udsat for forsøg på destruktive cyberangreb inden for de næste to år.

Det er dog sandsynligt, at statsstøttede hackergrupper forbereder sig på at kunne udføre destruktive cyberangreb rettet mod kritisk infrastruktur i Danmark. Netop fordi fremmede stater har kapaciteten til at udføre destruktive angreb, er det kun disse staters hensigt, der skal ændre sig, for at truslen ændrer karakter. Truslen fra destruktive cyberangreb kan derfor stige med kort eller ingen varsel. Det kan f.eks. ske, hvis den sikkerhedspolitiske situation eskalerer i retning af en militær konfrontation mellem Rusland og NATO.

Sundhedssektoren er en helt central del af det danske samfund. Derfor kan det få omfattende både direkte og afledte konsekvenser, hvis sektoren bliver ramt af destruktive cyberangreb. Det kan f.eks. ramme de patienter, der er i behandling på hospitalerne eller andre borgere, der er afhængige af kontakt til sundhedsvæsnet. Samtidig kan det også skabe frygt og usikkerhed i store dele af samfundet.

Truslen fra destruktive cyberangreb er rettet mod alle dele af Danmarks kritiske infrastruktur, herunder også sundhedssektoren. Der er altså ikke tale om en specifik trussel mod sektoren.

Cyberterror

Truslen fra cyberterror mod sundhedssektoren er **INGEN**. Det er usandsynligt, at sundhedssektoren 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 konventionel terror. Det kan f.eks. være cyberangreb, der forårsager fysisk skade på mennesker eller omfattende forstyrrelser af kritisk infrastruktur.

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

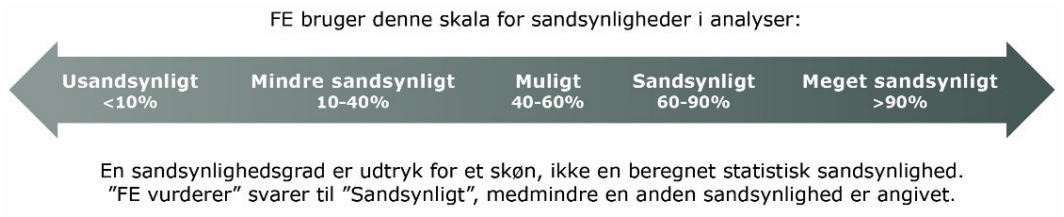
CFCS har fulgt truslen fra cyberterror siden 2016 med fokus på militante ekstremister. Center for Terroranalyse ved PET vurderer for nuværende, at truslen fra konventionel terror mod Danmark er alvorlig. Derfor følger CFCS udviklingen, uagtet at truslen fra cyberterror har været vurderet til **INGEN** i flere år.

Trusselsniveauer

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

Center for Cybersikkerhed udgiver løbende trusselsvurderinger og vejledninger på cyberområdet. Derudover udgiver Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste en række årlige publikationer, der beskriver truslerne mod Danmark. Nedenfor er fremhævet en række af de publikationer, som kan være relevante for myndigheder og virksomheder i sundhedssektoren i Danmark. Alle publikationer kan tilgås på myndighedernes hjemmesider.

Publikationer fra efterretningstjenesterne

UDSYN
Forsvarets Efterretningstjeneste beskriver i denne årlige efterretningsmæssige risikovurdering de ydre vilkår for Danmarks sikkerhed og danske interesser

Vurdering af spionagetruslen mod Danmark, Færøerne og Grønland
Denne trusselsvurdering udgives af Politiets Efterretningstjeneste og beskriver fremmede staters efterretningsvirksomhed mod Rigsfælleskabet, dvs. især spionage, påvirkning og forsøg på ulovligt at anskaffe teknologi og viden.

Vurdering af terrortruslen mod Danmark
I denne trusselsvurdering fastsætter Center for Terroranalyse (PET) det nationale terrortrusselsniveau og beskriver terrortruslen mod Danmark og danske interesser i udlandet.

Vejledninger fra Center for Cybersikkerhed

Vejledning om at imødegå ransomwareangreb
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 håndteres, når skaden er sket.

Vejledning om beskyttelse af IoT-enheder
Vejledningen "Beskyt IoT-enheder" kommer med en række konkrete anbefalinger til, hvordan organisationer kan beskytte IoT-enheder efter best practice.

Vejledning om leverandørstyring
Vejledningen "Informationssikkerhed i leverandørforhold" indeholder en række forslag til, hvordan styringen af forholdet mellem organisationer og leverandører kan varetages.

Vejledning om beskyttelses 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.