CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod sundhedssektoren

1. udgave juli 2018
Seneste opdatering juni 2022

Indhold

CENTER FOR CYBERSIKKERHED

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

3. udgave juni 2022

CENTER FOR CYBERSIKKERHED

Center for cybersikkerhed hæver trusselsniveauet for cyberaktivisme til HØJ for sundhedssektoren

Dato: 8. februar 2023

Truslen fra cyberaktivisme mod sundhedssektoren 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 sundhedssektoren.

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 sundhedssektoren

Denne trusselsvurdering redegør for cybertrusler, der er rettet imod den danske sundhedssektor. Sundhedssektoren i Danmark er vigtig for samfundets funktion, stabilitet og velfærd. Hensigten er at orientere sundhedssektoren om truslerne, så den bedre kan beskytte sig. Trusselsvurderingen kan eksempelvis indgå i risikovurderingen for sektoren i forbindelse med den nationale strategi for cyber- og informationssikkerhed.

Trusselsvurderingen er første gang opdateret i juni 2020 med ændringer i kapitlet om cyberterror som følge af ændrede trusselsniveauer i den årlige nationale trusselsvurdering "Cybertruslen mod Danmark" udgivet i 2020, samt tilføjelsen af et trusselsniveau til vurderingen af destruktive cyberangreb. Den øvrige tekst er uændret.

Trusselsvurderingen er igen opdateret i juni 2022 med et tilpasset kapitel om truslen fra cyberaktivisme som følge af en ændring af trusselsniveauet beskrevet i CFCS' vurdering "CFCS hæver trusselsniveauet for cyberaktivisme mod Danmark fra **LAV** til **MIDDEL**" udgivet d. 18. maj 2022. Trusselsniveauet for cyberaktivisme er hævet fra **LAV** til **MIDDEL**. Den øvrige tekst er uændret.

Hovedvurdering

- Truslen fra cyberspionage mod den danske sundhedssektor er **MEGET HØJ**. Fremmede stater har blandt andet interesse i at stjæle forskningsdata og intellektuel ejendom fra sektoren.

- Truslen fra cyberkriminalitet er **MEGET HØJ**. Der er muligt, at cyberkriminelle angreb kan forstyrre patientbehandlingen.

- Truslen fra cyberaktivisme hæves fra **LAV** til **MIDDEL**. CFCS hæver trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine. Det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark, herunder sundhedssektoren.

- Truslen fra destruktive cyberangreb mod den danske sundhedssektor er **LAV**. Det er dog muligt, at den danske sundhedssektor kan blive påvirket af destruktive cyberangreb i udlandet.

- Truslen fra cyberterror er **INGEN**. Denne type angreb forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt yderst begrænset.

Indledning

Vurderingen beskriver den generelle cybertrussel, der er rettet imod den danske sundhedssektor.

Den tager primært udgangspunkt i nordiske og internationale eksempler på cyberangreb mod sundhedssektoren, som sammenholdes med danske forhold samt viden om trusselsaktørernes kapacitet og intention.

Sundhedssektoren har en samfundskritisk rolle i Danmark. Cyberangreb mod den danske sundhedssektor kan få betydning for samfundets funktion, stabilitet og velfærd. Cyberangreb kan i yderste tilfælde føre til dødsfald, personskade og tab af tillid til sundhedsvæsenet blandt befolkningen. Det er derfor vigtigt, at denne trussel håndteres, så organisationerne, infrastrukturen og ydelserne i videst muligt omfang og hele tiden er tilgængelige og stabile, og den daglige patientbehandling ikke forstyrres.

Sundhedssektoren består af mange forskellige delelementer med forskellige særpræg og sårbarheder. Denne trusselsvurdering analyserer cybertruslen mod sundhedssektoren som helhed. Sundhedssektoren inkluderer i denne vurdering derfor alt fra behandlingssteder, såsom hospitaler, lægepraksisser og tandlæger, til leverandører og producenter, der understøtter behandlingen. Sidstnævnte inkluderer eksempelvis medicinalindustrien, life science-industrien, medicoindustrien og udbydere af it-løsninger til behandlingssteder. Organisationer, der beskæftiger sig med sundhedsforskning, både privat og offentligt, samt myndigheder, der beskæftiger sig med sundhed, såsom Sundheds- og Ældreministeriet, indgår også som en del af sundhedssektoren.

Trusselsvurderingen giver et overblik over cybertruslerne mod sektoren som helhed, og der skelnes kun mellem enkeltdelene af sektoren i et begrænset omfang.

Hvad er cybertrusler

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) definerer cybertrusler som trusler fra cyberangreb, hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Anden brug af internettet, der kan have negative konsekvenser for samfundet, såsom salg af ulovlig medicin på internettet, indgår ikke i denne definition af cybertrusler.

Trusselsbilledet kan beskrives ud fra flere vinkler. I denne vurdering er der fokus på, hvilket formål anvendelsen af cyberangreb har for de aktører, der udfører dem. CFCS beskriver og vurderer her aktiviteter, der har til formål at udføre cyberspionage, cyberkriminalitet, cyberaktivisme eller cyberterror. Desuden vurderer CFCS den potentielle trussel fra destruktive cyberangreb.

Trusselsniveauerne er baseret på en analyse af aktørernes intention og cyberkapaciteter. CFCS vurderer en aktørs cyberkapacitet ud fra de menneskelige og materielle ressourcer, aktøren har til rådighed. Det kan være teknisk dygtige hackere og udviklere af malware eller viden om mål, der kan bruges til eksempelvis social engineering. Det

kan også være it-infrastruktur, tid, penge og adgang til information. Hvor stor en cyberkapacitet, en aktør har, vil derfor afhænge af flere forskellige forhold og aktørens evne til at udnytte dem.

Vurderingen tager udgangspunkt i det aktuelle trusselsbillede og har en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt, både generelt og for den enkelte myndighed eller virksomhed. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Cyberspionage

Danske myndigheder og virksomheder er løbende udsat for forsøg på cyberspionage, der primært udføres af statslige aktører. CFCS vurderer, at cyberspionage også udgør en **MEGET HØJ** trussel mod den danske sundhedssektor.

CFCS vurderer, at det er meget sandsynligt, at fremmede stater har hensigt og kapacitet til at udføre cyberspionage mod den danske sundhedssektor. Det er sandsynligt, at fremmede stater særligt har interesse i de dele af sundhedssektoren, der har adgang til forskningsdata eller intellektuel ejendom. Fremmede stater har sandsynligvis også interesse i de dele af sektoren, der har adgang til store mængder patientoplysninger.

Cyberspionage mod f.eks. intellektuel ejendom fra sundhedssektoren udgør en samfundsøkonomisk trussel mod Danmark og kan skade danske interesser. Tyveri af følsomme patientoplysninger kan skade danskernes tillid til, at sektoren kan håndtere deres data på en sikker og forsvarlig måde. Tab af tillid kan udfordre den fortsatte digitalisering af patientbehandlingen.

Forskningsdata eller intellektuel ejendom kan benyttes af fremmede stater til at styrke deres nationale sundhedsindustri eller -forskning, samt til at udbygge eller forbedre deres eget sundhedssystem. Statsstøttede hackergrupper er tidligere gået efter intellektuel ejendom fra sundhedssektoren i udlandet, herunder private virksomheder, der beskæftiger sig med biokemi, biotek og lægemidler.

Endvidere kan følsomme oplysninger fra sundhedssektoren være værdifulde for andre staters efterretningsarbejde. Cyberspionage kan f.eks. give en fremmed stat adgang til oplysninger, den kan bruge til at profilere og afpresse personer i nøglefunktioner.

Et eksempel på, at cyberspionage mod sundhedssektoren foregår, er en hændelse i Norge. I januar 2018 blev det offentligt kendt, at hackere var trængt ind i et it-system på et sygehus, hvorfra de kunne tilgå store mængder data. Hændelsen foregik i Helse Sør-Øst, hvilket svarer til en dansk region. Den administrerende direktør for Helse Sør-Øst har udtalt, at der var tale om et it-system, der blev driftet lokalt på det pågældende sygehus. Det er efterfølgende blevet besluttet, at sygehusene ikke længere selv skal drifte deres servere, og at Sykehuspartner HF, der er et datterselskab under Helse Sør-Øst, skal overtage driften. Den administrerende direktør har yderligere fortalt, at hackerne havde foretaget sårbarhedsscanninger forud for selve indtrængningen, og at hackerne havde forsøgt at holde et lavt aktivitetsniveau, da de først var inde i systemerne, for at gøre det sværere at opdage dem. Den norske efterretningstjeneste beskrev i deres årlige risikovurdering *Fokus 2018* cyberangrebet som efterretningsaktivitet. Den norske efterretningstjeneste brugte ydermere angrebet til at understrege, hvor sårbar samfundsvigtig infrastruktur er overfor angreb.

Truslen fra cyberspionage mod enkeltdelene af den danske sundhedssektor afhænger af, hvilken og hvor meget data myndigheden eller virksomheden har adgang til. Det danske sundhedsvæsen er dog meget digitaliseret og forbundet, så en aktør kan angribe en sårbar del af sektoren i forsøget på at få adgang til andre mål.

Cyberspionage mod sundhedssektoren kan også foregå ved, at hackere angriber en leverandør. Hackerne kan enten udnytte leverandøren til at opnå adgang til det egentlige mål, eller de kan stjæle data, leverandøren behandler for sin kunde. Ofte har leverandører eller producenter fjernadgang til deres produkter på eksempelvis danske sygehuse. Det kan muliggøre, at hackere kan få adgang til et system eller udstyr, hvorfra de kan sprede sig videre ud i f.eks. et sygehus' øvrige systemer.

Leverandøren eller producenten af f.eks. medicoudstyr kan også være det egentlige mål. Hackere kan i dette tilfælde forsøge at kompromittere behandlingssteder såsom hospitaler for gennem dem at få adgang til leverandører eller producenter.

Cyberspionage kan desuden understøtte andre typer cyberangreb og trusler. Det kan eksempelvis være, at en fremmed stat ønsker at afdække sårbarheder i sundhedssektoren i tilfælde af en fremtidig skærpet konflikt. Denne viden kan anvendes forud for destruktive cyberangreb, særligt hvis cyberspionagen giver adgang til kritiske systemer eller informationer af relevans for det destruktive angreb. Cyberspionage kan også give en modstander adgang til følsomme oplysninger, der senere kan lækkes til offentligheden med henblik på at påvirke meningsdannelsen. En allerede kompromitteret virksomhed eller myndighed er derfor mere sårbar over for destruktive cyberangreb eller hack og læk angreb.

Cyberkriminalitet

Cyberkriminelle angriber sundhedssektoren for at tjene penge på bl.a. afpresning og datatyveri. De dele af sektoren, der behandler patienter, er meget afhængige af deres systemer og data for at udføre deres typisk tidskritiske og ofte livreddende arbejde, hvilket gør dem sårbare overfor afpresning i form af eksempelvis ransomware. Endvidere har dele af sektoren været præget af mange ældre og sårbare systemer, og tidligere har der ikke været samme fokus på cybersikkerhed. Dette kan have ført til, at cyberkriminelle har rettet deres fokus mod disse systemer. Derudover bliver sektoren ramt af mere tilfældige angreb, som ikke er rettet mod bestemte sektorer.

Ransomware kan forstyrre patientbehandlingen

Sundhedssektoren har i både Danmark og i udlandet været ramt af ransomware. Årsagen kan være, at de kriminelle håber, at sektoren er mere tilbøjelig til at betale løsesummen, fordi især hospitalers arbejde ofte er tidskritisk.

Ransomwareangreb

Ransomware bliver, som andre typer malware, typisk spredt via phishing-mails eller via inficerede hjemmesider, som offeret besøger.

Ransomware gør offerets data eller systemer utilgængelige, og bagmændene kræver en løsesum for at gøre disse tilgængelige igen. Der findes mange varianter af ransomware. Mere målrettede ransomwareangreb forsøger at ramme eksempelvis administrative netværk i specifikke virksomheder og myndigheder.

Særligt sundhedssektoren har i udlandet været offer for disse mere målrettede ransomwareangreb, hvor løsesummen har været af ganske betragtelig størrelse.

WannaCry er et af de større eksempler på et ransomwareangreb, der også ramte sundhedssektoren i udlandet og i mindre grad i Danmark. Effekten af Wannacry var i udlandet særdeles omfattende og illustrerede, at ransomware kan forstyrre samfundsvigtig infrastruktur. Især det britiske sundhedsvæsen var berørt, hvor tusindvis af patientaftaler blev aflyst, herunder presserende aftaler med patienter, der potentielt havde kræft. WannaCry viste, hvordan cyberangreb kan få direkte konsekvenser for patientbehandlingen. Wannacry er endvidere et eksempel på cyberkriminalitet, der af flere lande er blevet tilskrevet en statslig aktør.

Det er dog ikke kun ransomwareangreb mod hospitaler eller lægepraksisser, der kan påvirke patientbehandlingen. Patientbehandlingen kan også blive påvirket af ransomwareangreb mod virksomheder, der forsyner hospitalerne eller lægepraksisser med f.eks. medicin.

Det såkaldte NotPetya-angreb, der var et destruktivt cyberangreb forklædt som ransomware, illustrerede dette, da den påvirkede medicinalkoncernen Merck & Co's medicinproduktion. Hospitalerne har nødlagre af medicin, men større angreb på medicinproducenterne kan stadig give udfordringer for deres forsyningskæde.

Cyberangreb mod medicinalproducenter, der forstyrrer produktionen eller medfører store økonomiske tab for producenten, kan også have negative konsekvenser for den

danske sundhedssektor ved, at prisen på et givent præparat stiger. Medicinalvirksomheder fastsætter selv priser på deres lægemiddelpakninger og kan hver 14. dag indberette prisændringer til lægemiddelstyrelsen.

En nyere udvikling er, at kriminelle enten stjæler eller forcerer en leverandørs adgangsoplysninger for at tilgå sundhedsorganisationens systemer via fjernadgang. Herefter lægger hackerne ransomware på systemer, de får adgang til. I januar 2018 blev det amerikanske hospital Hancock Health eksempelvis ramt af ransomware, hvor hackerne tilsyneladende havde fået adgang til systemerne gennem fjernadgang. Angiveligt havde hackerne også formået at ødelægge hospitalets backup af data gennem denne fjernadgang. Samme måned blev den amerikanske virksomhed Allscripts, der udbyder et system til at administrere elektroniske patientjournaler, også ramt af ransomware gennem en fjernadgang.

Cyberkriminelle er ude efter sundhedssektorens data
CFCS vurderer, at der er cyberkriminelle med både intentioner om og kapacitet til at udføre datatyveri mod den danske sundhedssektor. Sektoren rummer en stor mængde data, som kriminelle kan udnytte til afpresning eller sælge. Disse data er f.eks. patient- eller forskningsdata eller informationer om udstyr eller produkter anvendt i sektoren.

Nogle cyberkriminelle forsøger at afpresse organisationer ved at true med at frigive sundhedsdata, de har hacket sig til. Særligt en aktør, der ofte benævner sig som "The Dark Overlord" har udført denne type afpresning i udlandet. Det har primært været organisationer i USA og England, som aktøren har angrebet. Danskere har dog været berørt af et lignende angreb i udlandet. Danskerne havde været patienter ved en udenlandsk plastikkirurgisk klinik, hvor kriminelle hackede og lækkede billeder af patienterne. Det er muligt, at også danske klinikker eller behandlingssteder vil blive forsøgt hacket og afpresset af cyberkriminelle.

Forceringsangreb
Et angreb hvor angriberen systematisk, ofte vha. software, afprøver et stort antal adgangskoder sam-men med udvalgte brugernavne for at "gætte" den korrekte kode og dermed tiltvinge sig afgang til digi-tale tjenester eller systemer.

Endvidere er der en risiko for, at cyberkriminelle forsøger at udnytte den nye persondataforordning til at afpresse myndigheder og virksomheder. De kriminelle kan enten true med at hacke organisationen, medmindre den betaler, eller hvis de allerede har hacket virksomheden, kan de forlange betaling for ikke at lække eventuelle stjålne data og offentliggøre, at de har hacket virksomheden.

Den brugerbetalte del af sundhedssektoren har finansielle oplysninger, der kan misbruges. Personhenførbare data kan i visse tilfælde også misbruges til identitetstyveri eller forsikringssvindel. Forsikringssvindel er dog et mindre problem i Danmark end i eksempelvis USA, hvor patienterne er mere afhængige af sundhedsforsikringer, og der er et større marked at sælge sundhedsdataene på.

Cyberkriminelle kan også gå efter forskningsdata eller intellektuel ejendom fra sundhedssektoren for at videresælge disse. Det kan være alt fra informationer om produktion og udvikling af medicin til informationer om udstyr eller software anvendt i sundhedssektoren.

Eksempelvis stjal en hacker i 2016 kildekoden til software udviklet af PilotFish Technology, som bruges til at integrere forskelligt medicinsk udstyr. Hackeren forsøgte først at sælge koden og senere at afpresse PilotFish Technology ved at true med at frigive de stjålne informationer. Hackeren påstod også, at han havde adgang til virksomhedens klienters elektroniske patientjournaler, hvilket han havde fået ved at sende en bagdør ud i en opdatering til softwaren fra PilotFish Technology. Den danske sundhedssektor gør i høj grad brug af leverandører af bl.a. softwareløsninger, og en lignende situation kan derfor ske i Danmark. Dette illustrerer vigtigheden af, at cybersikkerhed tænkes ind i valg af og aftaler med leverandører.

Et andet eksempel på en hackergruppe, der muligvis har udført cyberangreb med henblik på industrispionage mod sundhedssektoren, er en gruppe, som bl.a. kaldes Orangeworm. Orangeworm er ifølge it-sikkerhedsselskaber gået målrettet efter sundhedssektoren og har haft held med at sprede malware til bl.a. røntgen- og MRI-maskiner. Gruppen er gået efter både hospitaler og deres leverandører.

Cyberkriminelle kan også udføre datatyveri i forbindelse med børsspekulationer. Grundet de store omkostninger forbundet med forskning og udvikling af nye produkter inden for medicinal- og biotekindustrien kan et enkelt vellykket eller fejlslagent produkt have stor betydning for prisen på virksomhedens aktie. Viden om, hvilke produkter virksomheden har under udvikling, og hvor godt de klarer sig i forsøgsstadiet, kan derfor potentielt benyttes til børsspekulation.

Malware, der udvinder kryptovaluta, stiger i omfang
Der er en stigende tendens til, at cyberkriminelle benytter malware, som misbruger ofrets processorkraft til at udvinde kryptovaluta, såsom Bitcoins. Tendensen gælder på tværs af sektorer, så der er risiko for, at sundhedssektoren også bliver ramt af angreb.

Malwaren kræver typisk en stor mængde af den inficerede computers processorkraft til at generere kryptovalutaen, hvilket kan medføre driftsforstyrrelser. Medicinsk udstyr og software kan være særligt følsom over for malware, der udvinder kryptovaluta, da medicinsk udstyr typisk er designet og testet til at fungere under nogle bestemte vilkår, hvilket øger risikoen for, at malwaren har utilsigtede konsekvenser.

Selv hvis det ikke medfører driftsforstyrrelser, er det problematisk, hvis systemerne i sundhedsorganisationer bliver inficeret med malware, der udvinder kryptovaluta. Malwaren kan eksempelvis have sideeffekter eller et ressourceforbrug, der gør, at it-afdelingen starter en større undersøgelse af, hvad der forårsager forbruget. Det kan også lægge beslag på it-afdelingens tid og ressourcer at fjerne malwaren, og systemerne kan være utilgængelige, mens arbejdet står på.

De cyberkriminelle kan senere også benytte malwaren og adgangen til systemet til andre formål eller forvolde utilsigtet skade. Eksempelvis oplevede et hospital i Tennessee i september 2017, at den server, der huser deres elektroniske patientjournalsystem, blev inficeret med malware, der udvinder kryptovaluta. Det medførte, at hospitalet

blev nødt til at informere mere end 20.000 patienter om, at deres patientdata måske var blevet kompromitteret.

Overbelastningsangreb er en mindre alvorlig trussel
Der er cyberkriminelle, der benytter Distributed Denial of Service (DDoS) angreb som et værktøj til afpresning. De truer med at overbelaste organisationens hjemmeside eller andre tilgængelige services, medmindre ofret betaler. I visse tilfælde er personerne bag ikke reelt i stand til at udføre DDoS-angreb, men håber, at truslen er nok til, at ofret betaler.

DDoS-angreb
Distributed Denial of Service (DDoS) betegner cyberangreb, hvor angriberen udnytter kompromitterede elektroniske enheder til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk. Hjemmesiden eller netværket er utilgængeligt, mens angrebet står på.

CFCS vurderer, at det er vanskeligt at forstyrre sektorens services i alvorlig grad med DDoS-angreb. De services, der er kritiske i forhold til patientbehandlingen, bliver som udgangspunkt holdt på behandlingsstedernes interne netværk. Det vil derfor være vanskeligt for cyberkriminelle at ramme disse med DDoS-angreb.

Det er dog muligt, at de kriminelle vil være i stand til at være til gene ved eksempelvis at gøre en hjemmeside til en lægepraksis utilgængelig. CFCS vurderer dog ikke, at cyberkriminelle vil være i stand til at udføre DDoS-angreb i et omfang, så det påvirker den samlede samfundsvigtige ydelse, sundhedssektoren udbyder.

Business Email Compromise (BEC) er fortsat en udfordring
Såkaldte BEC-scams har til formål at franarre virksomheder og myndigheder penge gennem falske anmodninger om pengeoverførelser. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også ofte for CEO-fraud eller direktørsvindel.

De bedrageriske e-mails sendes ofte fra fremmede mailkonti, men i nogle tilfælde kan bedrageriforsøget misbruge kompromitterede mailkonti, der tilhører ledende medarbejdere i virksomheden. Hvis en ondsindet aktør er lykkedes med at kompromittere medarbejderes konti, øger dette risikoen for et succesfuldt bedrageriforsøg. CFCS har kendskab til, at dele af sundhedssektoren ligesom resten af Danmark oplever mange forsøg på BEC-scams, og at en del af disse bliver mere og mere avancerede.

Cyberaktivisme

Truslen fra cyberaktivisme mod sundhedssektoren er **MIDDEL**. CFCS hævede d. 18. maj 2022 trusselsniveauet for den generelle cybertruslen mod Danmark fra **LAV** til **MIDDEL** på baggrund af cyberangreb mod mål i europæiske NATO-lande udført af pro-russiske cyberaktivister. CFCS vurderer, at den generelle vurdering af truslen fra cyberaktivisme mod det danske samfund også gælder for den danske sundhedssektor.

Trusselsniveauet **MIDDEL** betyder at der er en generel trussel mod sundhedssektoren, samt at det er muligt, at virksomheder og myndigheder i sektoren vil blive ramt af aktivistiske cyberangreb inden for de næste to år.

CFCS har hævet trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine. CFCS vurderer, at cyberaktivister ofte går efter symbolske mål. Der er ikke en særskilt trussel mod sundhedssektoren, men cyberaktivister har tidligere ramt mål i sundhedssektoren i andre lande.

Cyberaktivister har kapacitet til at ramme offentlige hjemmesider i sundhedssektoren med DDoS-angreb eller såkaldte defacement-angreb, hvor budskaber indsættes på hackede hjemmesider.

En anden af cyberaktivisternes typiske angrebsmetoder er at lave hack og læk-angreb, der stiller ofret i et dårligt lys. Sundhedsdata kan blive et mål for denne type angreb, da de er følsomme og derfor kan skabe opmærksomhed. En anden årsag til, at sundhedssektoren kan være et mål, er, at dataene kan være knyttet til den holdning eller det budskab, aktivisterne vil formidle. En person hackede eksempelvis et system, der bliver brugt til at booke aftaler i det britiske sundhedsvæsen, for at understrege sin kritik af dårlig it-sikkerhed i sundhedssektoren.

Da cyberaktivisterne bruger deres angreb til at formidle et budskab, er det vigtigt for dem, at den tilsigtede modtager opfanger, hvad deres budskab er. De angriber derfor ofte i forbindelse med en konkret enkeltsag, som er blevet omtalt i medierne.

Eksempelvis angreb aktivister investoren Martin Shkrelis hjemmeside og konti på sociale medier efter, at han var blevet beskyldt for at have manipuleret og mangedoblet priserne på livsvigtig medicin. Et andet eksempel, der illustrerer mediernes betydning i forhold til aktivisme, er en operation af aktivistgruppen Anonymous kaldet #OpJustina. Medlemmer fra Anonymous angreb i 2014 Bostons børnehospital på baggrund af medieomtale om den dengang 15-årige patient Justina Pelletier, som var blevet indlagt på hospitalet mod hendes forældres vilje. Da angrebene fandt sted, havde hun været indlagt i over et år.

Truslen fra cyberaktivisme mod den danske sundhedssektor påvirkes derfor af, dels hvilke holdninger eller budskaber aktivisterne ønsker at promovere, og dels hvilken mediebevågenhed de kan udnytte til at promovere deres sag.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod sundhedssektoren er **LAV**.

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

Truslen kan stige i forbindelse med en skærpet politisk eller militær konflikt, hvor Danmark deltager.

Destruktive cyberangreb
CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt af angrebet er død, personskade, betydelig skade på fysiske objekter eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

En række lande har cyberkapaciteter, der potentielt kan bruges destruktivt mod samfundsvigtig infrastruktur, såsom sundhedssektoren.

På nuværende tidspunkt er det dog muligt, at danske myndigheder og virksomheder kan blive ramt som følgevirkning af destruktive cyberangreb mod mål uden for Danmark. Det gælder især danske virksomheder fra bl.a. sundhedssektoren, der er til stede i konfliktområder, hvor fremmede stater eller organiserede hackergrupper med kapacitet til at udføre alvorlige cyberangreb har interesser, såsom Ukraine og Saudi Arabien.

Såfremt fremmede landes vilje til at anvende destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark ændrer sig, kan destruktive cyberangreb mod sundhedssektoren have meget skadelige effekter. Sundhedssektoren kan også blive påvirket af destruktive cyberangreb mod andre samfundsvigtige sektorer, såsom energisektoren.

Cyberspionage er som tidligere nævnt ofte en forudsætning for destruktive cyberangreb. Kompromitterede institutioner er derfor mere sårbare overfor den potentielle trussel fra destruktive cyberangreb.

Cyberterror

CFCS vurderer, at truslen for cyberterror mod sundhedssektoren er **INGEN**.

Det betyder, at 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 mere konventionel terror, f.eks. 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 samtidigt yderst begrænset.

Et velfungerende sundhedsvæsen er dog vigtigt for at kunne reagere på et terrorangreb. Terrorister kan derfor forsøge at øge effekten af et konventionelt terrorangreb ved at kombinere det med mere simple cyberangreb mod sundhedssektoren.

TDoS
Telephony Denial of Service (TDoS) betegner cyberangreb, hvor angriberen overbelaster ofrets telefonnetværk med en stor mængde opkald, så det ikke kan modtage legitime opkald. Angriberen kan eksempelvis inficere en lang række mobiltelefoner med malware, som gør, at telefonerne konstant ringer op til et bestemt telefonnummer.

Det er derfor vigtigt, at sikre centrale dele af Danmarks sundhedsberedskab mod cyberangreb, så disse er robuste. Hvis cybersikkerhed ikke prioriteres, kan simple cyberangreb have negative konsekvenser for sundhedsberedskabet. Dette skete eksempelvis i 2016 i USA, hvor en 18-årig mand kom til at udføre et TDoS-angreb mod flere alarmcentraler. Han havde lavet og delt et link, der fik iPhones til konstant at ringe 911. Linket endte med at blive delt og klikket på af langt flere, end han havde forudset. Det førte til, at flere alarmcentraler blev gjort utilgængelige. Den funktion, han udnyttede til at få en iPhone til at foretage opkaldene, er siden blevet fjernet.

Tendenser i sundhedssektoren med betydning for cybertruslen

Der er en række forhold i sundhedssektoren, som kan have betydning for cybertruslen. Blandt andet er sektoren sårbar overfor, at cyberangreb faciliteres af medarbejdere, der mere eller mindre bevidst nedprioriterer cybersikkerhed. Behandlingen i sundhedssektoren er også i stigende grad afhængig af teknisk medicinsk udstyr og it-systemer, og disse er i stadig udvikling. Endvidere åbner den teknologiske udvikling op for, at behandlingen kommer til at foregå på andre vilkår.

Patientfokus over it-sikkerhed

Mange cyberangreb lykkes, fordi medarbejdere i myndigheder eller virksomheder ofte ubevidst giver hackerne adgang. Det kan eksempelvis ske ved, at en medarbejder downloader en fil fra en phishingmail eller anvender et password, som er nemt at gætte eller forcere. Lægers, sygeplejerskers og andet sundhedspersonales arbejde er centreret omkring patienten, og det arbejde kan være tidskritisk. Dette kan føre til, at personalet omgår it-sikkerhedsforanstaltninger, hvis foranstaltningerne opfattes som hæmmende for patientbehandlingen, eller hvis personalet kan spare tid ved det. Cyberangreb kan dog i sidste ende få negative konsekvenser for patientbehandlingen, og det er derfor vigtigt også at have fokus på cybersikkerhed i alle dele af en organisation.

Behandlingen foregår hjemme hos patienten

Der bliver i stigende grad benyttet telemedicin, hvor eksempelvis en lægekonsultation foregår ved hjælp af digitale medier, såsom e-mail, video, billeder og lyd over internettet. Det har de fordele, at der spares unødvendige hospitalsbesøg, indlæggelser og transport, så lægerne kan se flere patienter med færre ressourcer. Det kan dog også få en effekt på de cybertrusler, behandlingsstederne står overfor. Dels kan det være med til at åbne op for nye adgange, hackere kan udnytte til at kompromittere behandlingsstedets netværk. Endvidere kan de telemedicinske løsninger være mere sårbare overfor overbelastningsangreb som DDoS eller TDoS. Desuden kan der være en risiko for, at patienternes udstyr bliver inficeret med malware, som også spreder sig til behandlingsstederne. Det kan eksempelvis ske, hvis en patient kommunikerer med sin læge via e-mail, og patienten bliver ramt af malware, der spreder sig til lægen og videre til dennes e-mailkontakter.

Internet of Things på hospitaler

Begrebet "Internet of Things" (IoT) beskriver en tendens, hvor flere og flere elektroniske apparater bliver koblet til internettet. Denne tendens gør sig også gældende for hospitaler, men her forbindes apparaterne dog normalt til hospitalernes interne net. Apparaterne er derudover ofte udstyret med sensorer, som automatisk indsamler data. IoT-apparaterne har mange fordele, da de eksempelvis kan give lægerne mere data om deres patienter, gøre det nemmere at udveksle dataene og endda medvirke til at holde apparater sterile, da de ikke skal håndteres manuelt.

Der er dog mange af disse IoT-apparater, hvor cybersikkerhed ikke er tænkt ind fra producentens side. Det kan f.eks. skyldes, at producenten har fokus på at mindske apparatets størrelse, øge dets batterilevetid eller på at gøre det nemmere for leverandøren at supportere. IoT-apparaternes dårlige sikkerhed kan i sig selv være en adgang for hackere, men den trådløse deling af data imellem apparaterne kan også gøre det nemmere for hackere at opsnappe data, hvis disse ikke er krypterede i forsendelsen. At medicinske apparater i højere grad er forbundne kan desuden potentielt få konsekvenser for patientsikkerheden.

Sikkerhedsforskere har i flere tilfælde illustreret, hvordan forskelligt medicinsk udstyr under visse omstændigheder kan hackes med alvorlige konsekvenser for patientsikkerheden. Forskere fandt eksempelvis i et tilfælde en medicinpumpe, hvor en angriber kunne få fjernadgang og styre medicindoseringen.

IoT-apparaternes indtog på hospitaler og andre behandlingssteder kan være vanskelig at administrere for it-afdelingen. Mange IoT-apparater er simple at aktivere, men kan kræve en del administration at holde på et fornuftigt sikkerhedsniveau. Der kan også være en risiko for, at ansatte på klinikker og hospitalsafdelinger selv medbringer eller indkøber IoT-apparater, som bliver sat op uden om it-afdelingen. Det er derfor vigtigt at være opmærksom på, at hackere ikke udnytter disse apparater som indgangsvinkel til sundhedssektoren.

Trusselsniveauer

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

Usandsynligt | **Mindre sandsynligt** | **Muligt** | **Sandsynligt** | **Meget sandsynligt**

"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.