RAPPORT 2022

Sundhedssektorens trusselsbillede 2022

Udarbejdet af DCISsund

SUNDHEDSDATA-
STYRELSEN

Udgiver	Den decentrale cyber- og informationssikkerhedsenhed i sundheds-sektoren (DCISsund)
Ansvarlig institution	Sundhedsdatastyrelsen
Version	1.0
Versionsdato	24. maj 2022
Web-adresse	www.sundhedsdata.dk
Titel	Sundhedssektorens trusselsbillede 2022

Vælg (eller skriv) tekst vedr. reference

Indhold

Forord

Denne publikation er udarbejdet af den decentrale cyber- og informationssikkerhedsenhed (DCISsund) i sundhedssektoren, som er etableret på baggrund af den sektorspecifikke strategi for cyber- og informationssikkerhed 2019-2022.

Formålet med publikationen er at understøtte sundhedssektorens aktørers arbejde med cyber- og informationssikkerhed. Trusselsbilledet skal bidrage til sundhedssektorens evne til at forudse, forebygge, opdage og håndtere tværgående cyber- og informationssikkerhedshændelser.

Informationer om hændelser, trusler og mulige hændelser vil kunne indgå i de risikovurderinger, der løbende udarbejdes og vedligeholdes i sektoren. Publikationen har på den baggrund til formål at understøtte sektorens aktører i udarbejdelsen af lokale sårbarheds- og risikovurderinger. På sigt vil dette også være med til at styrke sundhedssektorens decentrale cyber- og informationssikkerhedsenheds i udarbejdelsen af samlede sårbarheds- og risikovurderinger for hele sektoren.

DCISsund ønsker at sige tak til de aktører, som har bidraget i arbejdsgrupper om operativ koordinering, malware, trusler, beredskab og hændelseshåndtering, samt de aktører, der har bidraget ved at indrapportere hændelser og delt informationer om trusler. Det har været et væsentlig bidrag, hvorigennem det har været muligt at få en kvalificeret forståelse af de eksisterende trusler.

Denne publikation er TLP:WHITE - Informationerne anses ikke som særligt følsomme og kan frit deles. TLP:WHITE vælges, når afsenderen har vurderet, at der er minimal eller slet ingen risiko ved at offentliggøre informationerne.

Ledelsesresume

2021 var et udfordrende år for cybersikkerheden med flere store hændelser, samt vækst i både antal og kompleksitet af angreb. Sundhedssektoren er som en af de kritiske sektorer afhængig af til stadighed at vedligeholde og udbygge et modstandsdygtigt cyberforsvar, der kan beskytte sektorens vitale interesser mod angreb.

Baseret på en trendanalyse af cyberkriminelles taktik, teknikker og procedurer (TTP'er) samt rapporter fra en række lukkede og åbne kilder giver den decentrale cyber- og informationssikkerhed for sundhedssektoren (DCISsund) i Trusselsbilledet 2022 sit bud på de væsentligste trusler for 2022 samt oplister generelle mitigeringer, der kan styrke sektorens robusthed mod disse trusler.

Rapporten går i dybden med de fem største cybertrusler mod sundhedssektoren i 2022; ransomware, phishing, insidere, Supply-chain angreb og legacy systemer. Dertil indeholder rapporten en oversigt over øvrige væsentlige cybertrusler, sundhedssektoren står over for.

Formålet med Trusselsbillede 2022 er at understøtte sundhedssektorens aktørers arbejde med cyber- og informationssikkerhed. Trusselsbilledet skal herigennem bidrage til sundhedssektorens evne til at forudse, forebygge, opdage og håndtere tværgående cyber- og informationssikkerhedshændelser.

Krigen i Ukraine

Trusselsbilledet for 2022 er udarbejdet på baggrund af hændelser, der har fundet sted i 2021. Men da særligt en storpolitisk begivenhed, krigen i Ukraine, har forrykket rammerne for hvilke lande og institutioner, der må anses som særligt sårbare, har DCISsund for hver enkelt af de fem store trusler indskrevet sine observationer i en epilog ift. krigens betydning for den pågældende trussel.

Top fem cybertrusler 2022

Ransomware

Sammenholdt med den MEGET HØJE hyppighed af angreb og den KATASTROFALE konsekvens vurderes det, at ransomware-angreb udgør en MEGET HØJ trussel mod sundhedssektoren.

Phishing

Sammenholdt med den MEGET HØJE hyppighed af angreb og de meget KATASTRO-FALE konsekvenser vurderes det, at phishing-angreb udgør en MEGET HØJ trussel mod sundhedssektoren.

Insidere

Grundet det MEGET HØJE antal forekomster af brud relateret til insidertruslen og de potentielt KATASTRO-FALE konsekvenser ved hændelser i denne kategori vurderes det, at insidertruslen udgør en MEGET HØJ trussel mod sundhedssektoren.

Supply-chain

Det vurderes, at der en MEGET HØJ hyppighed af Supply-chain angreb, og cyberkriminelle forventes også fremadrettet at forsøge at udnytte sektorens leverandører i angreb mod sektoren. Sundhedssektoren an-vender mange leverandører, der forsyner sektorens aktører med både it-systemer og infrastruktur, og den fortsatte drift af nationale og andre større net- og informationssystemer er direkte afhængig af disse leverandører. Et angreb mod forsyningskæden vurderes at kunne have ALVORLIGE konsekvenser, hvis it-understøttelsen af sundhedsydelserne kompromitteres. Supply-chain angreb vurderes at udgøre en MEGET HØJ trussel mod sundhedssektoren.

Legacysystemer

Det vurderes, at der en MEGET HØJ hyppighed af legacy-systemer, og cyberkriminelle forventes også fremadrettet at forsøge at udnytte sektorens sårbarhed i angreb mod sektoren. Et angreb mod et eller flere legacy vurderes at kunne have ALVORLIGE konsekvenser. Angreb mod legacy-systemer vurderes at udgøre en MEGET HØJ trussel mod sundhedssektoren.

Indledning og metode

Sundhedssektoren har til formål at sikre borgernes liv og helbred. En grundlæggende forudsætning er, at behandling og pleje finder sted i trygge og sikre rammer. Sikkerhed er således en integreret del af hverdagen i det danske sundhedsvæsen.

De trusler, sårbarheder og risici, der har betydning for cyber- og informationssikkerheden i sundhedssektoren, udgør sammen med den stadige teknologiske udvikling og opfindsomheden på modstandersiden en kompleks og dynamisk udfordring for sektoren.

Denne publikation indeholder et overblik over trusler og hændelsestyper, der skal understøtte aktørernes arbejde med cyber- og informationssikkerhed på det strategiske og taktiske niveau.

Informationer om trusler og mulige hændelser vil bl.a. kunne bruges i de risikovurderinger, der løbende udarbejdes og vedligeholdes i sektoren. I forlængelse heraf vil oplysningerne i Trusselsbillede 2022 kunne bruges til at vurdere hvilke tekniske og organisatoriske foranstaltninger, der er passende og tidsvarende.

Vurderingen af trusler og tilhørende risici i denne publikation afspejler en generel vurdering på tværs af sektoren. Risikoen for den enkelte aktør kan afvige alt efter eksponering og sårbarhed.

Målgruppe og kontekst

Trusselsbillede 2022 henvender sig til personer, der arbejder med cyber- og informationssikkerhed på det strategiske og taktiske niveau i bred forstand.

Dermed henvender publikationen sig både til informationssikkerhedsspecialisten og sikkerhedsarkitekten, mens teknikere, der overvåger eller vedligeholder net- og informationssystemer, vil have større værdi af de detaljerede trusselsbriefinger og varsler, der løbende sendes ud fra DCISsund.

På baggrund af erfaringerne fra 2021 har det været muligt at udarbejde et fast årshjul for sektorens arbejde med trussels-, sårbarheds- og risikovurderinger, der koordineres ift. initiativerne omkring hændelseshåndtering, beredskab og øvelser. Dette betyder, at planlægningen af beredskabsøvelser kan tage udgangspunkt i trusselsbilledet, mens opdateringen af beredskabsplaner sker i forlængelse af sektorens risikovurdering.

Centrale begreber

Trussel

En trussel forstås som ethvert fænomen, begivenhed eller omstændighed, der vurderes at kunne lede til en hændelse. Inden for cyber- og informationssikkerhed kan man opdele som trusler som følgende:

- En 'cyber-trussel' er et fænomen, en begivenhed eller en omstændighed, der medfører intentionelle angreb på net- og informationssystemer.
- En 'informationssikkerhedstrussel' er bredere og omfatter fænomener, begivenheder eller omstændigheder, der negativt kan påvirke mulighederne for at nå målsætninger med en aktivitet, der involverer net- og informationssystemer.

Trusselsvurderingen er i denne rapport et produkt af hyppighed og konsekvens.

Niveauerne kan aflæses i de kommende tabeller.

Tabel 1 Trusselsniveauer

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

Tabel 2 Hyppighedsniveauer

Trussel	Beskrivelse
Meget høj	Det ventes, at truslen leder til en eller flere hændelser.
Høj	Der er forekommet hændelser pba. denne trussel inden for de sidste 12 måneder
Middel	Truslen fører jævnligt til hændelser i andre offentlige og private virksomheder (omtales ofte i pressen)
Lav	Det er sandsynligt, at hændelsen vil forekomme.
Ingen	Man har erfaring med hændelser på baggrund af denne trussel, men ikke inden for de sidste 12 måneder

Tabel 3 Konsekvensniveauer

Trussel	Beskrivelse
Katastrofale	Alvorligt fald i serviceniveauet. Kan føre til, at det ikke er muligt at gennemføre vigtige aktiviteter.
Alvorlige	Borgere modtager ingen eller meget mangelfuld service. Eksempelvis hvis hele organisationen har ingen eller meget begrænset adgang til nødvendige systemer.
Moderate	Flere vigtige forpligtelser over for borgere kan ikke overholdes, og borgerne vil opleve en væsentlig forringelse af den forventede service.
Minimale	Kan være en påvirkning af flere vigtige aktiviteter i en afgrænset periode, fx hvis dele af organisationen ingen adgang har til vigtige systemer.
Ubetydelige	Vil medføre et markant fald i det generelle serviceniveau. Enkelte vigtige forpligtelser kan ikke overholdes.

Sårbarhed

En sårbarhed forstås som en svaghed, omstændighed eller egenskab ved en organisation, aktiv eller proces, der negativt påvirker evnen til at forudse, forebygge, opdage eller håndtere en hændelse.

Risiko

Risiko ses som et produkt af sandsynlighed og konsekvens, hvor sandsynligheden findes gennem trussels- og sårbarhedsanalyser, og konsekvensen findes ved at vurdere direkte eller indirekte negativ påvirkning af robusthed, tilgængelighed, autenticitet, integritet og fortrolighed. Jf. ISO/IEC 27001:2017 defineres risiko som "the effect of uncertainty on objective" eller effekten af usikkerheder ift. organisationens målsætninger. Jf. ISO 27001 omhandler risikostyring både mulige hændelser og muligheder, der kan have negative og positive konsekvenser.

Kritikalitet

Nedenstående tabel viser den skala, DCISsund benytter til at vise kritikalitet/risiko for en hændelse eller trussel. DCISsund benytter kritikalitetsskalaen til varsler, som sendes via varselssystemet.

Modellen tager afsæt i Center for Internet Security's (CIS) Alert Level Information, men den er tilpasset til at fungere for DCISsunds varsler til sundhedssektoren.

Tabel 4 Kritikalitetsniveauer

Trussel	Beskrivelse
Kritisk	En begivenhed udgør en overhængende og umiddelbart risiko for den fortsatte drift af væsentlige eller kritiske tjenester.
Høj	Det er sandsynligt, at en begivenhed leder til alvorlig indvirkning på folkesundheden eller borgernes grundlæggende rettigheder og frihedsrettigheder.
Middel	En begivenhed kan potentielt påvirke folkesundheden eller borgernes grundlæggende rettigheder og frihedsrettigheder. Eller hændelsen vurderes til på sigt at kunne lede til negativ påvirkning af folkesundhed og/eller folkesikkerhed og organisationens økonomisk sikkerhed.
Generel	Det er sandsynligt, at en begivenhed leder til betydelig indvirkning på folkesundheden eller borgernes grundlæggende rettigheder og frihedsrettigheder.
Lav	Begivenheder af almindelig drift eller rutinemæssige karakter. Fx datatab eller hændelser der kan løses med det samme. Hvor der er en risiko for, at hændelsen kan sprede sig.

Angrebsvektorer/TTP

TTP står for Taktikker, Teknikker og Procedurer (på engelsk: Tactics, Techniques and Procedures).

- 'Taktikker' er en overordnet redegørelse for en aktørs måde at arbejde eller virke på.
- 'Teknikker' er en mere detaljeret beskrivelse af adfærd i sammenhæng med taktikker.
- 'Procedurer' er en meget detaljeret beskrivelse i forbindelse med en teknik.
- Værktøjer er de redskaber, en trusselsaktør anvender som en del af aktørens TTPs.

I denne rapport er der vurderet på TTP i bred forstand, og disse er beskrevet i afsnittene 'Angrebsvektorer' under hvert trusselsafsnit.

Hændelse

En hændelse forstås overordnet som et afgrænset forløb eller begivenhed med negative konsekvenser. Fx en hændelse med uautoriseret adgang, utilgængelige services og/eller ødelæggelse, videregivelse eller ændring af data.

Mitigering

En mitigering er en handling, en aktør kan tage for at få nedsat risikoen for den givne trussel. Mitigeringerne, som er beskrevet i indeværende rapport, skal ses som bedste praksis og er på et generelt niveau.

The Dark Web

Internettet består af flere lag. Når man til daglig surfer på internettet, bevæger man sig på det område, der kaldes 'Surface web'. Under dette øverste lag findes dybere lag (bunden af isbjerget), som kaldes hhv. 'Deep Web' og 'Dark web'

Dark web er designet til at give anonymitet ved at holde kommunikationen privat gennem kryptering og routing af onlineindhold gennem flere lag af webservere. Det er her, den "mørke" del kommer ind; adgang til dark web kræver brug af specifik software, der holder brugeren anonym.

Dark web er ofte afbildet som et anarkistisk forum for kriminel aktivitet, men det er ikke nødvendigvis sandt. Dark web er et anonymt område på nettet, der kan bruges eller misbruges.

Surface web

Består af offentligt søgbare websteder såsom nyhedssider, web-handel, YouTube, blogs mv.

The deep web

Består af sider som krævet et login, som f.eks. e-mail, online bank, Facebook mv.

The dark web

Kræver et specielt værktøj for at kunne tilgås, som en Tor-browser (The onion router[1]).

[1] https://www.torproject.org/

Cyberhændelser i 2022

Begivenheder relevante for trusselsvurderingen

Solarwinds – Supply-chain angreb

I starten af 2021 lå efterdønningerne efter Solarwinds Orion Supply-chain-hændelsen. Der var stadig organisationer i Danmark, der arbejdede hårdt på at finde ud af om og hvor meget, hændelsen havde haft effekt på deres organisation.

Tidlinje for hændelsen:

- Marts 2019 - Cyberkriminelle får uautoriseret adgang til SolarWinds-netværket
- Oktober 2019 - Cyberkriminelle tester indledende kodeinjektion i Orion
- 20. februar 2020 - Ondsindet kode kendt som Sunburst injiceret i Orion
- 26. marts 2020 - SolarWinds begynder ubevidst at sende Orion-softwareopdateringer med hacket kode
- December 2020 - Offentligt opdaget og rapporteret efter mere end et år

Mere end 18.000 SolarWinds-kunder installerede de ondsindede opdateringer med malware, som spredte sig uopdaget. Gennem malwaren fik hackere adgang til SolarWinds kundeinformationssystemer, som de derefter kunne bruge til at installere endnu mere malware til at spionere på andre virksomheder og organisationer.

Efterforskningen[2] mener, at en russisk spionageoperation - sandsynligvis Ruslands udenlandske efterretningstjeneste (SVR) - står bag SolarWinds-angrebet. Den russiske regering har nægtet enhver involvering i angrebet og frigivet en erklæring[3], der sagde: ”Ondsindede aktiviteter i informationsrummet er i modstrid med principperne i den russiske udenrigspolitik, nationale interesser og forståelse af mellemstatslige forbindelser.” De tilføjede også, at ”Rusland ikke udfører offensive operationer på cyberområdet.”

Man ved stadig ikke, hvad formålet med hacket var, og det er stadig uvist, hvilken information, hvis nogen, de cyberkriminelle fik adgang til.

MS Exchange – Zero-day

En global bølge af cyberangreb og databrud begyndte i januar 2021, efter at fire zerodays sårbarheder blev opdaget på Microsoft Exchange Servers.

[2] https://heimdalsecurity.com/blog/russian-svr-solarwinds-hack/
[3] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Sårbarheden gav cyberkriminelle fuld adgang til bruger-e-mails og adgangskoder på de berørte servere, administratorrettigheder på serveren og adgang til tilsluttede enheder på det samme netværk.

Cyberkriminelle installerer typisk en bagdør, der giver dem fuld adgang til berørte servere, selvom serveren senere opdateres til ikke længere at være sårbar over for de oprindelige zero-day.

Det estimeres, at over 250.000 servere var ramt af denne type angreb

Vestas - Ransomware

Den 19. november 2021 blev Vestas ramt af Lockbit 2.0 ransomware-angreb, hvor kritiske systemer blev sat ud af funktion. Som en del af at lukke ned for angrebet var en af overvejelserne at lukke ned for 50.000 vindmøller, hvilket ville medføre, at store dele af landet ville stå uden strøm og potentielt medføre skade på vindmøllerne.

De cyberkriminelle har offentliggjort store mængder af fortrolige informationer, som de har stjålet under angrebet. Heriblandt finansielle dokumenter, tekniske tegninger af vindmøller samt meget personlige oplysninger på centrale medarbejdere.

Log4shell – Zero-day

Log4Shell var en zero-day sårbarhed i Log4j, som er et populær Java-logningsframework.

Sårbarheden det gjorde muligt at udføre vilkårlig kode. Sårbarheden har eksisteret ubemærket siden 2013 og blev anonymt anmeldt til Apache Software Foundations sikkerhedsteam den 24. november 2021 og blev offentliggjort den 9. december 2021. Apache gav Log4Shell en CVSS-score på 10, den højeste tilgængelige score. Udnyttelsen er enkel at udføre og anslås at påvirke hundreder af millioner af enheder.

Varsler udsendt fra varselssystemet

DCISsund overvåger og udsender løbende varsler til aktører i sundhedssektoren. Varslerne udsendes på baggrund af data fra kollegaer i sundhedssektoren globalt set. Disse triageres med information fra Center for Cybersikkerhed, risikovurderinger fra aktørerne i den danske sundhedssektor, åbne kilder samt andre sektorers DCIS'er.

Varslerne er med til at danne datagrundlaget for indeværende rapport, da de giver et udtryk for hvilke trusler og kritikalitet, DCISsund har varslet sektoren om.

Som det ses på grafen, har der været en stigning af udsendte varsler samt kritikaliteten i andet halvår 2021. I december kom årets første kritiske varsel, nemlig varslet angående log4shell.

Ransomware

Beskrivelse

Ransomware er ondsindet software eller kode, der krypterer filer og gør dem utilgængelige. Herefter kræver de cyberkriminelle løsepenge for at levere en nøgle, der kan åbne for adgang til eller dekryptere de filer, som er omfattet af angrebet. De cyberkriminelle er for det meste motiveret af potentialet for stor strategisk påvirkning og økonomisk afkast.

Løsesummens størrelse fastsættes ofte på baggrund af en konkret vurdering af, hvad angriberne vurderer, de kan få. De cyberkriminelle kræver typisk, at løsesummen betales i cryptovaluta, som ikke kan spores.

Ransomware-angreb kan forstyrre driften ved den enkelte aktør og have alvorlige konsekvenser. I værste fald kan konsekvenserne ramme sundhedssektorens væsentlige og/eller fælles infrastruktur og dermed forstyrre kontinuiteten af de samlede sundhedsydelser.

> Man regner med, at der i 2021 blev gennemført et ransomware-angreb hvert 11. sekund. Det svarer til en stigning på 151 % ift. 2020[4]

Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service er en forretningsmodel mellem ransomware-udviklere og cyberkriminelle, som ønsker et ransomware angreb iværksat. Den cyberkriminelle betaler for at iværksætte ransomware-angrebet, som ransomware-udvikleren har lavet. I sin opbygning ligner RaaS en variation af Software-as-a-Service (SaaS).

RaaS-kits gør det muligt for cyberkriminelle at gennemføre ransomware-angreb uden at have kompetencerne eller tiden til at udvikle egne ransomware-angreb. RaaS-kits er nemme at finde på the dark web, hvor RaaS-kits annonceres på samme måde som almindelige varer andre steder på internettet.

Et RaaS-kit kan indeholde 24/7-support, bundtede tilbud, brugeranmeldelser, fora og andre funktioner, præcis som dem, der tilbydes af almindelige SaaS-udbydere. Prisen på RaaS-kit varierer fra $40 om måneden til flere tusinde dollars – hvilket er små beløb taget i betragtning af, at de gennemsnitlige løsesumskrav i 2021 var $6 millioner.

[4] World Economic Forum - Global Cybersecurity Outlook 2022

Big Game Hunting (BGH)

Der er de seneste par år set et skifte i, hvor sofistikerede ransomware-angrebene er og hvilke mål, angrebene rettes mod. Hvor ransomware-grupper tidligere fokuserede på individer og små virksomheder, ser vi i dag, at fokus i højere grad er på de store organisationer.

Årsagen er sandsynligvis, at de større organisationer typisk har en bedre betalingsevne og ofte er dækket af en forsikring. Der benyttes dog ofte ikke forsikringer i den offentlige sektor i Danmark.

Double extortion og dark web

Ved ransomware-angreb indsamles der ofte fortrolige og følsomme oplysninger, som kan blive offentliggjort på hjemmesider på dark web[5] (Tor-netværket). Virksomheder, der måske allerede har betalt en løsesum for at genetablere adgangen til deres systemer, bliver nu afpresset endnu en gang, denne gang under truslen om offentliggørelse af de fortrolige og følsomme oplysninger.

Betaling er dog ikke en garanti for, at oplysninger ikke lækkes på et senere tidspunkt, eller at eventulle bagdøre ikke sælges videre til andre cyberkriminelle.

Quadruple (multi) extortion

I 2021 tog ransomware-grupperne afpresning til et nyt niveau, "firedobbelt eller multi afpresning" er en ny tendens set i 2021. Ransomware-grupperne bruger nu fire eller flere teknikker til at presse ofre til at betale flere penge:

1. Først krypteres data og backup forsøges slettet eller ødelagt. Herefter kræves der en løsesum for tilbagelevering af data.
2. Dernæst truer den kriminelle med at lække data, hvis der ikke betales en ny løsesum.
3. Trusler om at udføre et denial of service (DoS) angreb på hjemmesider. Igen kræves der løsesum for ikke at udføre angrebet.
4. Til sidst trues der med, at kunder, samarbejdspartnere, medarbejdere eller nyhedsmedierne vil blive kontaktet, hvis man ikke betaler en ny løsesum.

[5] https://www.avast.com/c-dark-web#topic-1

I 2021 steg løsesummen ved ransomware-angreb med 78 % til et gennemsnit på $570.000 pr. angreb. Den største løsesum, der er udbetalt i 2021, er på svimlende $40 millioner[6].

Angrebsvektorer

De mest hyppige angrebsvektorer for at igangsætte et ransomware-angreb synes at være:

Fjernadgange

- Remote Service Access, f.eks RDP, Citrix og VPN
- Social Engineering, f.eks. via phishing
- I forlængelse af Social Engineering anvendes mere generisk malware, som giver cyberkriminelle en etableret tilstedeværelse i netværket, som kan udnyttes til et ransomware-angreb på et senere tidspunkt.

Sårbare internetvendte services

- Eksempelvis legacy-systemer eller servere, som kan nås fra internettet, f.eks. via VPN, IIS, Oracle weblogic eller MS Exchange. Systemer, der ikke er patchede, eller som er fejlkonfigurerede, er særligt sårbare.

Mitigeringer

Mitigeringerne er ikke udtømmende, men skal ses som bedste praksis. Mange af dem tager afsæt i CIS securitys anbefalinger[7]:

Hav en beredskabsplan klar

- Planen skal inkludere, hvordan organisationen skal forholde sig under en ransomware-hændelse.

[6] https://www.mimecast.com/blog/the-biggest-ransomware-attacks-of-2021
[7] https://www.cisecurity.org/insights/blog/ransomware-facts-threats-and-countermeasures

Opdaterede sikkerhedskopier

- Brug et sikkerhedskopieringssystem, der gør det muligt at gemme flere iterationer i tilfælde af, at sikkerhedskopierne bliver krypterede af cyberkriminelle eller, at backuppen indeholder inficerede filer. Test rutinemæssigt sikkerhedskopier for dataintegritet og for at sikre, at de kan gendannes. Overvej offline backups samt at kryptere backuppen.
- Hold credentials, der har adgang til/styrer/kan slette backup, hermetisk adskilt fra alm AD.

Kryptér al data og trafik

- Sørg for at alt trafik krypteres, ikke kun trafik som transporteres over internettet, men også intern trafik.
- Data i hvile, særlig meget følsom data, bør ligeledes krypteres, således at cyberkriminelle ikke kan afpresse yderligere ved at true med læk af data.

Brug antivirus/spam/EDR

- Aktivér automatiske system- og netværksscanninger og sørg for, at antivirusprogrammer opdaterer signaturer automatisk. Implementer en anti-spam-løsning for at forhindre phishing-mails i at nå netværket.

Deaktiver brugen af makro i Office

- Overvej at bruge Office Viewer-software til at åbne Microsoft Office-filer, der sendes via e-mail, i stedet for den fulde version af Microsoft Office.

Hold alle systemer opdateret

- Det gælder al hardware, mobile enheder, operativsystemer, software og applikationer, cloudløsninger og CMS. Brug et centralt patch management system. Implementer en applikations whitelist og softwarerestriktionspolitikker (SRP) for at forhindre kørsel af programmer på typiske 'ransomware-placeringer' såsom midlertidige mapper.
- Benyt sårbarhedsscanninger på systemerne og prioriter opdatering ift. kritikalitet.

Begræns internetadgang

- Brug proxyserver til internetadgang og overvej annonceblokeringssoftware. Overvej at begrænse adgangen til typiske ransomware-indgange såsom personlige mailkonti (Gmail, yahoo-mail m.fl.) og sociale netværk (Facebook, Instagram m.fl.)

Privilegerede adgange

- Brug så få privilegerede og administratoradgange som muligt og sørg for at, adgangskoder skiftes jævnligt. Før log og gennemgå loggen med jævne mellemrum

Anvend segmentering og principperne for least privilege

- Segmenter fysiske og logiske netværk samt data. Virtualisér, hvor det er muligt. Og indfør princippet om administration med minimumsrettigheder (least privilege).

Overvåg tredjepartsadgange og før tilsyn

- Fjernadgange til organisationens netværk og/eller forbindelser til 3. parter bør overvåges. Før tilsyn med leverandører for at sikre, at de overholder bedste praksis for cybersikkerhed.

Videndeling

- Deltag i netværk hvor man deler information om hændelser, IoC'er, varsler mv, såsom MS-ISAC, DKCERT, DCISvarsel, MISP m.fl.

Awareness

- Tilbyd medarbejderne awareness-træning med særligt fokus på social engineering og phishing. Her undervises medarbejderne i at genkende mistænkelige e-mails, mistænkelige links eller vedhæftede filer og til at udvise forsigtighed, inden de besøger ukendte websteder.
- Overvej at tilføje et advarselsbanner til alle e-mails fra eksterne kilder, der minder brugerne om risiciene ved at klikke på links og åbne vedhæftede filer.
- Gennemfør derudover f.eks. phishing-kampagner, hvor medarbejdere bliver testet.

Incident response plan

- Udarbejd en hændelsesplan der sikrer, at personalet ved hvor og hvordan, de skal rapportere mistænkelig aktivitet eller hændelser. Gør opmærksom på, at det ikke er forkert at blive lokket i en fælde, men at det er afgørende, at medarbejderen hurtigt indberetter hændelsen.

Den gennemsnitlige nedetid for virksomheder, der gennemlever et ransomware-angreb, er 21 dage.

Reaktion på en hændelse/angreb

1. Afbryd øjeblikkeligt det inficerede system for at forhindre, at det spreder sig til andre systemer via netværket.
2. Undersøg de berørte data. Nogle følsomme data, såsom sundhedsoplysninger, kræver yderligere rapportering og/eller afbødende foranstaltninger. Hvis brugernavne, passwords eller persondata har været i risiko, skal et ransomwareangreb evt. meldes til Datatilsynet Undersøg om dekryptering er tilgængelig. Hjemmesiden www.nomoreransom.org[8] kan hjælpe med dette.
3. Gendan filer fra vedligeholdte sikkerhedskopier.
4. Del/anmeld hændelsen. Det anbefales at anmelde ransomware-angrebet til Politiets Landsdækkende Center for It-relateret økonomisk Kriminalitet (LCIK) og på virk.dk. Derudover er det en god idé at dele sin viden med DCISsund og andre organisationer, så de kan sikre sig mod lignende angreb.

Det anbefales, at man undlader at betale løsepenge eller gå i dialog med de cyberkriminelle. Start evt. med at undersøge, om der findes andre muligheder for at få data igen og søg råd og vejledning hos myndigheder eller private aktører[9].

[8] Retshåndhævende myndigheder og it-sikkerhedsfirmaer er gået sammen om at forstyrre kriminelle, som benytter ransomware.
[9] https://sikkerdigital.dk/virksomhed/naar-skaden-er-sket/hvad-skal-du-goere-hvis-du-er-ramt-af-ransomware

Observationer/hændelser

Januar	
Januar	
Februar	
Marts	
April	
Maj	› Colonial Pipeline • Darkside ransomware › Irske sundhedsvæsen • Conti ransomware
Juni	› Group Fleury • REvil ransomware › JBS • REvil ransomware
Juli	› Managed Service Providers • REvil ransomware
September	
Oktober	› REvil ransomware gruppen • Medlemmer bliver anholdt opg grup-pens aktiviteter stoppes (for en stund) › Canadiske sundhedvæsen • Unavngiven ransomware gruppe
November	› Vestas • LockBit ransomware
December	› Mærsk • Supply chain da leverandør rammes af ransomware.

Epilog

Under krigen i Ukraine har Rusland benyttet forskellige typer af malware forklædt som ransomware, heriblandt defacing af hjemmesider, hvor statsejede hjemmesiders forside fjernes og erstattes af andet indhold. Metoden bruges taktisk for at fjerne statens kommunikation til borgerne. Derudover er der set en del wipermalware, som udelukkende er designet til at ødelægge/kryptere uden mulighed for gendannelse af data.

APT-gruppen Wizard Spider, som står bag Conti-ransomwaren og menes at være finansieret af den russiske stat, har gentagne gange angrebet Ukraine og landets allierede. Derudover har de offentlig givet udtryk for deres loyalitet over for Rusland.

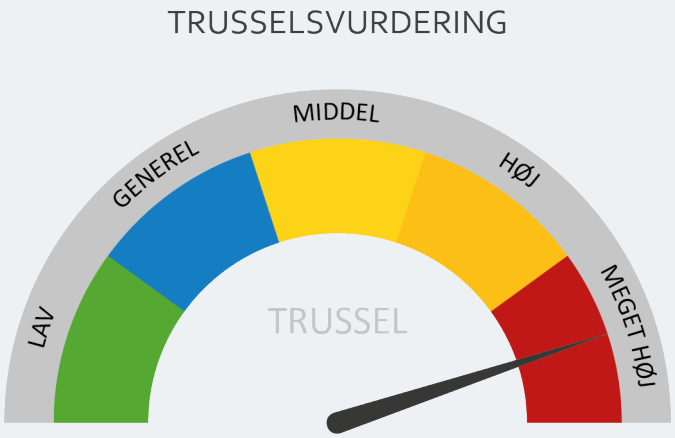
Det antages at, grundet vestens sanktioner mod Rusland er der sket et fald i ransomware angreb generelt, da det er blevet mere besværligt for cyberkriminelle (fra Rusland) at hvidvaske løsesummene.

Gruppen Wizard Spider der står bag Conti-ransomwaren, har under COVID19-pandemien meldt ud at bl.a. sundhedssektoren er fredet, men under krigen i Ukraine har de nu officielt meldt ud, at sektorer, som tidligere var 'fredet', ikke længere kan vide sig sikre.

Trusselsvurdering - Ransomware

I 2021 blev der endnu engang observeret en øget tendens til dobbeltafpresninger, hvor cyberkriminelle efter udlevering af nøgle til dekryptering, efterfølgende truede både virksomheder og borgere med at lække information, der var stjålet i forbindelse med ransomware-angrebet. Tendensen til at gennemføre flere afpresninger i forlængelse af et ransomware-angreb kommer også til udtryk i firdobbelte afpresninger, hvor de cyberkriminelle udnytter lækket yderligere f.eks. med trusler om gennemføre DoS-angreb samt at kontakte samarbejdspartnere, kunder, medarbejdere, medier mv., hvilket øger konsekvensen radikalt.

Sammenholdt med den MEGET HØJE hyppighed af angreb og den KATASTROFALE konsekvens vurderes det, at ransomware-angreb udgør en MEGET HØJ trussel mod sundhedssektoren.



Phishing

Beskrivelse

Phishing er i dag meget mere end dårligt formulerede e-mails. I takt med at brugerne er blevet bedre til at gennemskue den slags cyberkriminalitet, har de kriminelle også taget ved lære. Nu gennemføres phishingforsøg også via SMS, sociale medier og endda telefonopkald. Samtidig er de cyberkriminelles tekster blevet bedre oversat, logoer og links ligner det, de udgiver sig for, og generelt set er deres teknikker blevet forfinede. Dette gælder i særdeleshed de former for phishing, der ikke kommer på e-mail.

36% af alle cybersikkerhedsbrud med datatab involverer phishing[10]

SMS, sociale medier og telefonopkald

Angreb via SMS, kontakt på sociale platforme og direkte telefonopkald er metoder, der bliver mere og mere udbredte.

Det kan f.eks være opkald, hvor den kriminelle forsøger at franarre modtageren oplysninger. Eller SMS'er med links til malware, hvor beskeden udgiver sig for at være fra firmaer eller institutioner, medarbejderne generelt har tillid til, såsom Microsoft, GLS eller Sundhedsstyrelsen.

Der er også eksempler på, at medarbejdere bliver ringet op af en person, der udgiver sig for at være fra it-support. Den kriminelle oplyser, at der er sket et sikkerhedsbrud, og at de skal bruge medarbejderens login-oplysninger for at undersøge, om bruddet har bredt sig til medarbejderens konto.

Flere oplever også at blive kontaktet på de sociale platforme af fremmede, der er underligt interesserede i at lære dem at kende. I virkeligheden er der ofte tale om kriminelle, der forsøger at lokke medarbejderen til at sende penge, eller som forsøger at franarre borgeren materiale eller oplysninger, der senere kan bruges til at afpresse borgeren.

De fleste ransomware-angreb initieres med et phishing-angreb, hvor en medarbejder lokkes til at trykke på et link eller åbne et "lure document". Et "lure document" er bevidst designet til at

[10] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

lokke en person til at åbne dokumentet. I nogle tilfælde kan det være nok til, at systemer inficeres med en trojan, der kommunikerer med en command-and-control (C2) server[11], som senere udnyttes af den ondsindede aktør til at øge sin tilstedeværelse, eskalere privilegier og bevæge sig på tværs af net-og informationssystemer, og herved er ransomware-angrebet initieret.

Spear phishing

Spear phishing er et målrettet forsøg på at narre et eller flere specifikke ofre til at videregive personlige eller andre fortrolige oplysninger, som kan give de cyberkriminelle adgang til blandt andet it-systemer.

Spear phishing anvender ofte avanceret social engineering for at målrette indholdet til det enkelte offer. Kommunikationen er typisk udformet til at være særligt relevant eller særligt overbevisende for modtageren ved f.eks. at bruge modtagerens navn eller andre oplysninger, der er fundet ved forudgående analyse af ofret.

Spear phishing adskiller sig især ved, at ofrene er nøje udvalgte og ikke er tilfældige.

Smishing

Smishing er phishing-forsøg, der finder sted via sms. De cyberkriminelle vil typisk forsøge at lokke modtageren ind på en webside, hvor medarbejderen skal oplyse sin adgangskode eller kreditkortoplysninger eller downloade en ondsindet applikation. Offeret kan også blive lokket til at ringe til et telefonnummer, hvor gerningsmanden vil fortsætte sit svindelnummer.

Vishing

Vishing er phishing-forsøg som foregår via telefonopkald. Den cyberkriminelle fortæller f.eks., at man har vundet en konkurrence, og man derfor skal udlevere personlige oplysninger for at modtage præmien. Den cyberkriminelle kan også påstå, at man har sikkerhedsproblemer med sin computer, betalingskort eller bankkonto og derfor skal udlevere personlige oplysninger eller adgangskoder for at få løst problemet.

> Der sendes ca. 3 milliarder spoofede e-mails hver dag

[11] https://en.wikipedia.org/wiki/Command_and_control

Phishing-as-a-Service (PhaaS)

Phishing-as-a-Service er en tjeneste, hvor cyberkriminelle kan få adgang til phishing-kampagner uden selv at skulle konfigurere dem. Mod betaling forsyner servicen de cyberkriminelle med de e-mails, som skal bruges, kits til at efterligne forskellige kendte mærker og derudover tilbydes hosting og support.

Processen bag PhaaS er ret simpel; En cyberkriminel kontakter det firma, der leverer denne service, og betaler for at oprette og implementere en phishing-kampagne mod den entitet, de vil angribe. Servicen inkluderer defekte login-sider, hosting og ressourcer til at holde og distribuere stjålne oplysninger.

> FBI vurderer, at Business E-mail Compromise (BEC) kostede virksomheder ca. 80 milliarder kroner i 2020[12]

Angrebsvektorer

De mest hyppige angrebsvektorer for at igangsætte et phishing-angreb er:

- E-mail (Phishing/Spear phishing)
- Cyberkriminelle der sender en e-mail direkte eller indirekte til en organisation.
- SMS (Smishing)
- Cyberkriminelle der sender en SMS med et link, hvor man skal dele fortrolige oplysninger som NemID eller lignende.
- Telefon (Vishing)
- Cyberkriminelle ringer op og forsøger at lokke en til at gå ind på et website og downloade malware

Mitigeringer

Mitigeringerne er ikke udtømmende, men skal ses som bedste praksis.

Awareness

- Træning af medarbejdere med fokus på at spotte phishing-mails.

[12] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Mailfiltrering og anti-spam-løsning

- Brug mailfiltrering og anti-spam løsninger for at forhindre, at phishing-e-mails når mailboksen og derved potentielt kan inficere klienten med malware.

Advarselsbannere på e-mails

- Brug advarselsbannere på e-mails fra eksterne kilder, som minder brugerne om farerne ved at klikke på links og åbne vedhæftede filer fra ukendte kilder.

Opdateret antivirus/EDR-software

- Skulle der komme e-mails med malware, evt. ved brug af private tredjepart mailudbydere, er det essentielt, at man har antivirus/EDR installeret og opdateret. Det kræver dog også, at malwaren er kendt af antivirus/EDR.

DMARC e-mail autentifikation

- DMARC[13] beskytter mod, at cyberkriminelle misbruger organisationens domain til phishing.

Luk ned for private e-mails

- Luk ned for adgang til tredjeparts e-mail (private e-mails, f.eks. gmail, yahoo-mail m.fl.) Disse er services er en vej ind i organisationen, hvor mitigeringer som f.eks. DMARC, mailfiltrering og Anti-spam ikke rammer.

Reaktion på en hændelse/angreb

1. Afbryd øjeblikkeligt det inficerede system for at forhindre, at virussen spreder sig via netværket til andre systemer.
2. Få hurtigt adviseret it-support/helpdesk om hændelsen.

Awarenesstræning handler om at reducere ”The Human Risk Element” til et acceptabelt niveau og ikke om at blive perfekt!

[13] https://dmarc.org/

Observationer/hændelser

Sundhedssektoren er hver eneste dag mål for et utal af phishing-angreb. Det vurderes, at der er en meget høj hyppighed, og cyberkriminelle forventes også fremadrettet at anvende phishing, især via e-mails, i deres angreb mod sektoren. I nogle tilfælde spoofer[14] en angriber en aktør i sektoren og sender e-mails, der udgiver sig for at være legitime e-mails, til borgere og andre aktører.

Under COVID-pandemien skete der en markant stigning i phishing-angreb, hvor cyberkriminelle angreb både borgere og organisationer i dække af køb af værnemidler, vacciner mv.

Phishing-angreb er altid i bevægelse og tilpasser sig altid til verdenssituationen. Cyberkriminelle vil altid udnytte muligheder som pandemier, krig eller andet, som kan lokke folk til at hoppe i fælden.

Epilog

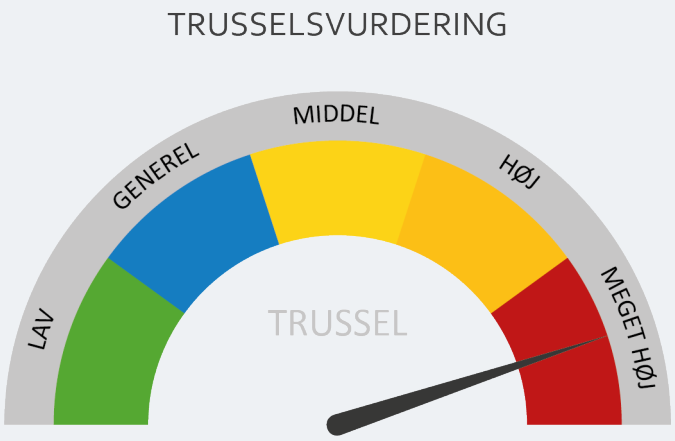
Under krigen i Ukraine har Rusland flittigt benyttet phishing-angreb mod entiteter i den kritiske infrastruktur i Ukraine. Dette har medvirket til, at Rusland har kunne deface statslige ukrainske hjemmesider for at sprede desinformation, ydermere har de haft held med at inficere systemer med wiperware og initiere ransomware-angreb.

[14] https://en.wikipedia.org/wiki/Spoofing_attack

Trusselsvurdering - Phishing

Mange af de hacking- eller malwareangreb, som målrettes eller rammer sundhedssektoren, anvender phishing til indledningsvis at få adgang til sektorens net- og informationssystemer, hvorfor de mulige konsekvenser vurderes at være alvorlige.

Sammenholdt med den MEGET HØJE hyppighed af angreb og de meget KATASTROFALE konsekvenser vurderes det, at phishing-angreb udgør en MEGET HØJ trussel mod sundhedssektoren.



Insider-truslen

Beskrivelse

En insidertrussel er en person inden for organisationen eller en leverandør, der har adgang til aktiver eller intern viden omkring organisationens sikkerhed, data og it-systemer. Disse oplysninger kan anvendes på en måde, der negativt påvirker organisationen.

Nogle af de risici og udfordringer, som sundhedssektoren står over som følge af insidertrusler, er:

- Bedrageri
- Datatyveri
- Sabotage
- Spionage
- Fejl og utilsigtede hændelser

En insidertrussel kan opdages gennem mistænkelig adfærd, herunder forskellige indikatorer for ulovlig adfærd, som bør igangsætte yderligere undersøgelser. Nogle indikationer på ondsindet aktivitet fra en insider kan ses i nedestående tabel:

En analyse[15] fra 2021, der omfattede 58 organisationer og i alt 3 milliarder filer, viste at:

- Hver medarbejder havde adgang til 20 % af alle filer.
- 31.000 følsomme sundhedsfiler var åbne for alle.
- Mere end 1 ud af 10 følsomme filer var åbne for alle medarbejdere.
- 77 % af virksomhederne havde 500 eller flere konti med adgangskoder, der ikke udløb.
- Skiftet mod cloud-tjenester gjorde insidertrusler 53 % sværere at opdage.

[15] Varonis '2021 Healthcare Data Risk Report

Tabel 5 Insider indikationer

Adfærdsmæssige indikatorer	Indikatorer for it-sabotage	Indikatorer for datatyveri
Straffeattester med sikkerhedsbrud eller forbrydelser Tilfælde af uprofessionel adfærd Tilfælde af mobning af andre medarbejdere Personlige konflikter Misbrug af rejser, tid eller udgifter Konflikter med kolleger eller ledere	Oprettelse af bagdørskonti Ændring af alle adgangskoder, så ingen får adgang til data Deaktivering af systemlogs Installation af et fjernadministrationsværktøj Installation af malware Tilgå andre medarbejderes systemer eller maskiner	Massiv download af organisationens data Afsendelse af fortrolig data til adresser uden for organisationen Afsendelse af e-mails med mange vedhæftede filer til adresser uden for organisationen Omfattende brug af virksomhedsprintere Fjernadgang til en lokal server uden for arbejdstiden

Skødesløse eller uagtsomme medarbejdere

Mens de fleste organisationer bruger penge på at beskyttes sig mod insidertrusler med ondsindet hensigt, er uagtsomme insidertrusler mere almindelige. Rapporter[16] viser, at 61 % af databrud, som involverer en insider, er utilsigtede og forårsaget af uagtsomme medarbejdere. Denne type databrud skyldes ofte:

- Manglende bevidsthed om sikkerhedspolitikker og manglende uddannelse i sikkerhedsbevidsthed.
- 27 % af medarbejderne læste organisationens sikkerhedspolitikkerne igennem mindre end en gang om året
- 39 % af medarbejderne modtog awareness-træning mindre end én gang om året.

[16] Ponemons 2020 Insider Threats Report

Misbrug af administrative privilegier udgør 20 % af alle angreb med alvorlige datatab til følge[17]

Ondsindede insidere

Ondsindede insidere er insidere, som har til hensigt at skade organisationen. Det kan f.eks. være en medarbejder, der har set sig sur på organisationen og derfor bevidst handler til skade for organisationen. Undersøgelser viser dog, at denne type trussel udgør en mindre trussel mod organisationer end den uagtsomme medarbejder[18]. Det er vigtigt at nævne, at der er forskellige undersøgelser af dette med varierede målinger.

- Ondsindede insidere er involverede i 14 % af alle insider-hændelser,
- Uagtsomme medarbejdere er skyld i 61 % af alle insider-hændelser,

Uagtsomme medarbejdere, der får stjålet deres legitimationsoplysninger, udgør 25 % af alle insider-hændelser[19].

Et mål for mange cyberangreb er misbrugen af administrative rettigheder.

Indvendige agenter

En indvendig agent er en medarbejder, som arbejder på vegne af en ekstern aktør for at kompromittere en organisations netværk og udføre et databrud eller andre angreb. Denne type trussel er særlig farlig, fordi det giver den eksterne aktør adgang og privilegier på medarbejderniveau.

For eksempel kan statsstøttede aktører via indvendige agenter udføre spionage på organisationer for at få strategisk insiderviden eller for at stjæle informationer, der kan fremme deres egen industri og økonomi.

[17] IBM The Cost of a Databreach 2021
[18] https://h-isac.org/annual-threat-landscape-report/
[19] https://h-isac.org/annual-threat-landscape-report/

Utilfredse medarbejdere

Utilfredse medarbejdere kan udgøre en betydelig trussel på grund af deres adgang til organisationens it-systemer. Det er en følelsesmæssig trusselsaktører, der har til formål at skade organisation, og i nogle tilfælde føler medarbejderen, at organisationen skylder medarbejderen noget. Denne type medarbejderutilfredshed skyldes normalt en uopfyldt forventning eller en uheldig begivenhed. I 2021 var 80 % af hændelserne med misbrug af privilegier økonomisk motiverede[20].

Tredjeparter/leverandører

Insidertrusler er ikke kun interne medarbejdere, men kan også være tredjeparter som f.eks. leverandører. Omkring 94 % af organisationerne i sundhedssektoren på global plan giver tredjeparter adgang til deres systemer. I 72 % af tilfældene har tredjepartsleverandører oven i købet privilegerede adgange til systemerne[21].

Angrebsvektorer

Nogle angrebsvektorer for insider-angreb er:

Forkert administreret adgang

- Manglende kontrol over medarbejdernes adgange og procedurer om nedlukning af konti f.eks. når medarbejdere skifter stillinger internt.
- For brede adgange til medarbejdere, særligt priviligerede og admin adgange er kritiske sårbarheder.

Skygge-it

- Alt it-udstyr som ikke er registreret i en CMDB (Configuration Management Data Base), eller anden for dokumentation går ofte under radaren og er ofte sårbare for indgang til organisationens infrastruktur.

Bring Your Own Device (BYOD)

- Manglende politikker om medarbejdernes egne enheder og grundet den manglende kontrol over disse enheder kan disse udgøre en sårbarhed for organisationen.

[20] Verizons databrudsrapport for 2021
[21] https://h-isac.org/annual-threat-landscape-report/

Ved 61 % af alle angreb misbruges administrative rettigheder[22]

Mitigeringer

At identificere en insidertrussel bør være en holdindsats mellem ledelse, it og HR-afdelingen. Inden for organisationen skal der samarbejdes om at implementere overvågning og opdage ondsindede insidere i tide, før de forårsager skade.

Der er en række foranstaltninger, man kan implementere for at værne sin organisation mod de forskellige typer insidertrusler.

Mitigeringerne er ikke udtømmende, men skal ses som bedste praksis.

Revidering og opdatering af sikkerhedspolitikker og retningslinjer.

- Sørg for altid at have opdaterede sikkerhedspolitikker og retningslinjer og kommuniker dem til medarbejdere med faste intervaller

Begræns privilegeret adgang og etabler rollebaseret adgangskontrol.

- Sørg for at lukke af for brede adgange, giv kun medarbejdere adgang til hvad der er behov for og gennemgå jævnligt hvilke adgange, de har. Vær opmærksom på, at medarbejdere, der skifter stillinger internt i en organisation, kan have en tendens til at overføre adgange, der ikke er relevante, fra den ene stilling til den anden.
- Sørg for at følsomme oplysninger kun er tilgængelige for dem, der har et arbejdsrelateret behov for adgang.

Implementering af multifaktor autentifikation (MFA).

- Beskyt adgangen til data og apps ved at implementere MFA.

Adgangskode og kontoadministration

- Implementer arbejdsgange der sikrer overholdelsen af organisationens retningslinjer for adgangskode- og kontoadministration.

[22] Verizon DBIR 2021

Backup

- Sikkerhedskopier data og implementer værktøjer til forebyggelse af datatab.

USB og andre flytbare medier

- Administrer USB-enheder på tværs af virksomhedens netværk. Aktiver automatisk antivirus scan på USB-porte eller luk for portene på arbejdsstationer, der ikke er under opsyn.

Cloud-tjenester

- Udarbejd specifikke databehandleraftaler for alle cloud-tjenester og leverandører, vær især opmærksom på adgangsbegrænsninger og overvågningsfunktioner i aftalerne.

Logning

- Sørg for at logge adgange og gennemgå logs jævnligt.

SIEM

- Benyt et SIEM-system (Security Information and Event Management) til at logge, overvåge og gennemgå medarbejdernes aktivitet.

Fakta

For at få privilegeret adgang kræver det en insider, som f.eks. en uagtsom medarbejder eller en indvendig agent. Det typiske angrebsmønster er privilegie-eskalering på kompromitterede klienter, som efterfølges af traversering af netværket for at opnå domain admin rettigheder. Opnår de cyberkriminelle domain admin rettigheder har de fuld kontrol over virksomhedens infrastruktur og data.

Den tid, der går fra angrebet påbegyndes til ofret opdager det, Dwell time, varierer meget fra land til land. I EMEA er dwell time i gennemsnit 66 dage mod et globalt gennemsnit på 24 dage[23].

[23] Mandiant M-Trends 2021

Reaktion på en hændelse/angreb

1. Hav en proces for at undersøge og dokumentere en hændelse.
2. Sørg for at jeres Incident Response Plan har politikker og bestemmelser om insidertrusler.
3. Vær forberedt på at handle hurtigt ved at lukke for adgange og samle beviser.
4. Vær forberedt på at gendanne fra backups.

Observationer/hændelser

DCISsund erfarer, at der dagligt er hændelser, som omhandler insidere i sundhedssektoren. Det drejer sig primært om uagtsomme medarbejdere, der laver fejl, eller som har for brede adgange og derfor behandler information, som ikke er relevant i arbejdssammenhænge. Medarbejdere, som er uopmærksomme ved for eksempel ikke at låse sin skærm, når man forlader sin pc, eller omgår sikkerhedsforanstaltninger som besværliggør hverdagen, er en konstant trussel og sker jævnligt.

Epilog

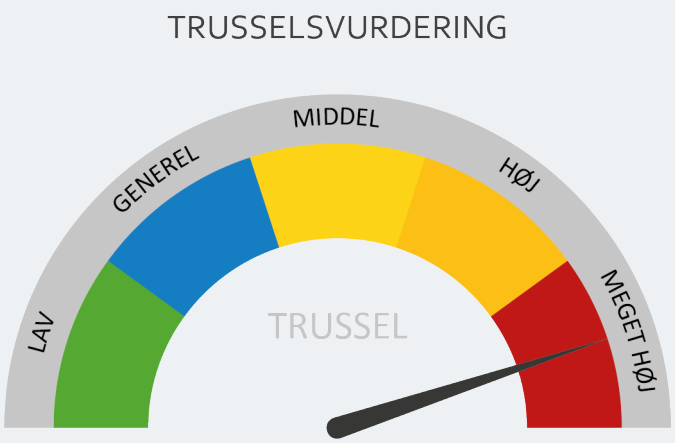
Krigen i Ukraine har sat insidertruslen, herunder spionage meget højt på dagsordenen.

Danmark udviste i starten af april 2022 15 russiske (formodede) spioner, der ifølge regeringen var efterretningsofficerer, som har arbejdet under diplomatisk dække på ambassaden og spioneret på dansk jord.

Trusselsvurdering - Insider

Der er en meget høj hyppighed af brud relateret til insidertruslen. Dette skyldes primært antallet af utilsigtede hændelser, hvor en medarbejder tilgår eller deler data på grund af uagtsomhed i arbejdsprocessen. I tilfælde hvor det er teknisk personale, som handler uagtsomt eller laver fejl, kan det have alvorlige konsekvenser for den fortsatte drift.

Grundet det MEGET HØJE antal forekomster af brud relateret til insidertruslen og de potentielt KATASTROFALE konsekvenser ved hændelser i denne kategori vurderes det, at insidertruslen udgør en MEGET HØJ trussel mod sundhedssektoren.



Supply-chain angreb

Beskrivelse

Ved et Supply-chain angreb forsøger de cyberkriminelle at kompromittere net- og informationssystemer i en forsyningskæde for at nå deres egentlige mål. Baggrunden for denne type angreb kan være, at cyberkriminelle vurderer, at leverandører til en virksomhed er mere sårbare over for angreb end det primære mål, og dermed forsøger de cyberkriminelle at finde og udnytte et svagt punkt i kæden af leverandører til det egentlige mål.

> Supply-chain angreb steg med faktor 4 fra 2020 til 2021[24]

Der er fire nøgleelementer i et Supply-chain angreb:

1. Leverandør: En entitet, der leverer et produkt eller en tjenesteydelse til en anden entitet.
2. Leverandør aktiv: Værdifulde aktiver, som leverandøren anvender til at producere produktet eller tjenesteydelsen.
3. Kunde: Den entitet, der forbruger det produkt eller den tjeneste, der produceres/leveres af leverandøren.
4. Kundeaktiver: Værdifulde elementer, der ejes af kunden.

En entitet kan være enkeltpersoner, grupper af enkeltpersoner eller organisationer.

Aktiver kan være mennesker, software, dokumenter, økonomi, hardware eller andet.

Spill-over-Effect og Colatteral Damage

Fænomenerne ”Spill-over-Effect” og ”Colatteral Damage” dækker over angreb, der er målrettede leverandøren, men hvor en organisation som en afledt effekt bliver ramt af, at leverandøren bliver angrebet. Enten ved at en service er nede eller ved, at cyberkriminelle bevæger sig videre til organisationen via forbindelser, som f.eks. fjernadgange (RDP) til og fra leverandøren.

[24] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Angrebsvektorer

Legacy systemer og Zero-days

- Uopdaterede systemer og zero-days er aårbarhder som cyberkriminelle udnytter til at skabe adgang til leverandører eller organisation.

Fjernadgange

- Remote Service Access, f.eks RDP, Citrix og VPN.

Administratorrettigheder og priviligerede adgange

- Manglende kontrol over medarbejdernes adgange og procedurer om nedlukning af admin-konti f.eks. når medarbejdere skifter stillinger internt.
- For brede adgange til medarbejdere, særligt priviligerede og admin adgange er kritiske sårbarheder.

Open Source og Usikker kodning af software

- Open source kan være inficeret med malware eller generelt dårlig skrevet kode, som derfor ikke er sikker.
- Kode som ikke er valideret af andre med fokus på sikker kode udgør en markant trussel.

Kompromitteret leverandør

- En kompromitteret leverandør udgør en stor sårbarhed, særligt hvis de har priviligerede eller admin konti som forbinder ind til organisationens infrastruktur.

Mitigeringer

Listen er ikke udtømmende, men skal ses som generelle bedste praksis mitigeringer.

Privilegerede adgange

- Luk ned for priviligerede adgange og adminkonti, der ikke er nødvendige.

Patch Management

- Sørg for at have tydelige og dokumenterede patch management-processer.

Segmentering

- Segmenter netværk og systemer så der kun kan etableres adgange, hvor der er et forretningsmæssigt behov.

Logning

- Sørg for at logge adgange og gennemgå logs jævnligt.

Leverandørstyring

- Stil høje sikkerhedskrav til leverandøren og sørg for, at der føres audit på leverandørens sikkerhed evt. i form af revisionserklæringer.

Udvikling af software

- Udvikling med fokus på sikker kodning (brug code review).
- Undgå at bruge open source
- Open source kan være inficeret med malware eller generelt dårlig skrevet kode, som derfor ikke er sikker.

62% af angrebene var malware den anvendte angrebsteknik[25]

Observationer/hændelser

SolarWinds

I februar 2020 injicerede cyberkriminelle tilknyttet Ruslands SVR (udenlandsk efterretningstjeneste) ondsindet kode til en opdatering til SolarWinds Orion, som er en netværksovervågningssoftware, der bruges af flere organisationer verden over. Den ondsindede kode gik uopdaget indtil december 2020 og inficerede over 18.000 maskiner gennem forsyningskæden. Flere organisationer i Danmark blev ramt.

[25] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Kaseya

I juli 2021 udnyttede ransomware-gruppen REvil en sårbarhed i Kaseyas RDP-værktøj til at få adgang til Kaseyas systemer. Kaseya er et netværksovervågnings- og sårbarhedsstyringsværktøj og en Software-as-a-Service (SaaS) udbyder. REvils adgang til Kaseyas netværk resulterede i den potentielle infektion af tusindvis af downstream-kunder, herunder Managed Service Providers (MSP'er). For nogle kunder tog det måneder at komme tilbage til normal drift.

Accenture

I august 2021 blev konsulent- og sikkerhedsfirmaet Accenture angrebet af LockBit ransomware.

De cyberkriminelle afpressede Accenture ved at true med at publicere fortrolig information på dark web. Selvom Accenture hævder, at der ikke var nogen af deres kunder, som blev ramt, er der stadig mulighed for, at de vil blive ramt af spill-over-effect, eller at de cyberkriminelle har bevæget sig dybere ind og afventer for at udføre et mere sofistikeret angreb.

Omkring 50% af alle supply-chain angreb er blev tilskrevet kendte APT-grupper[26].

Epilog

Under krigen i Ukraine har der indtil videre været flere eksempler på 'collataral damage'. I den danske sundhedssektor har en leverandør, der benytter Ukrainsk udviklet software, været ramt af ransomware, der fik berørte aktører til at lukke for alle forbindelser til leverandøren. Det har heldigvis vist sig, at den danske sundhedssektor ikke var ramt i dette tilfælde. Det formodes, at de cyberkriminelle ikke vidste, hvilke adgange de havde og derfor ikke udnyttede angrebet fuldt ud.

[26] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Trusselsvurdering – Supply-chain

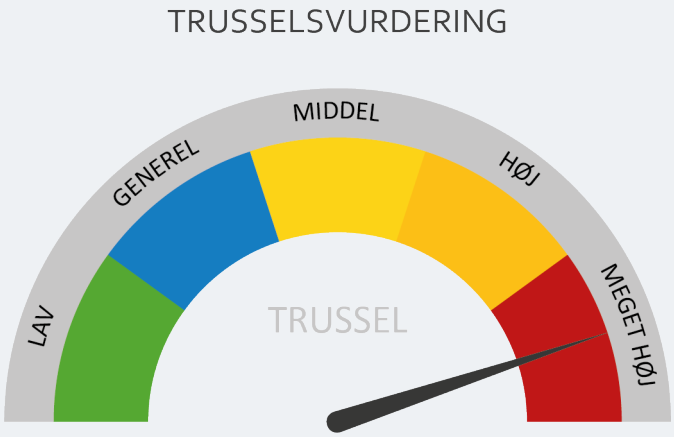
Over de seneste par år er der opstået en trend, hvor hackere målrettet går efter Managed Service Providers (MSP) for at kompromittere en leverandør, der giver adgang til mange forskellige ofre. Angrebene mod en MSP udføres ofte af APT'er (avancerede og vedvarende trusselsaktører), som bruger tid på at rekognoscere, undvige detektering, eskalere privileger, bevæge sig på tværs af miljøer, indsamle data, opnå kontrol, lække data og kryptere data.

Cyberkriminelle vil sandsynligvis fokusere på forsyningskæder som en levedygtig angrebsvektor, særligt i betragtning af de vellykkede brud på SolarWinds, Kaseya og udnyttelsen af Apache's Log4j i slutningen af 2021. De cyberkriminelle ved, at et brud i forsyningskæden vil give dem adgang til en større målflade end ved at angribe individuelle mål.

Det vurderes, at der en MEGET HØJ hyppighed af Supply-chain angreb, og cyberkriminelle forventes også fremadrettet at forsøge at udnytte sektorens leverandører i angreb mod sektoren.

Sundhedssektoren anvender mange leverandører, der forsyner sektorens aktører med både it-systemer og infrastruktur, og den fortsatte drift af nationale og andre større net- og informationssystemer er direkte afhængig af disse leverandører. Et angreb mod forsyningskæden vurderes at kunne have ALVORLIGE konsekvenser, hvis it-understøttelsen af sundhedsydelserne kompromitteres.

Supply-chain angreb vurderes at udgøre en MEGET HØJ trussel mod sundhedssektoren.



Legacy systemer

Beskrivelse

Et legacy-system er et forældet (upatchet) operativsystem, applikation eller hardwareplatformen, som det kører på. Mens mange systemer i disse dage kører på enten Linux, Unix eller Windows, kan nogle applikationer også køre på en mainframe eller Tandem-hardwareplatform, og det placerer dem ligeledes som et legacy system. En anden kategori af legacy systemer har at gøre med forældede programmeringssprog.

Sundheds-it består af mange specialiserede systemer, både hardware og software, og der er derfor en meget bred vifte af systemer, der kan udgøre en sårbarhed, hvis ikke de er patchede, segmenteret eller sikret på anden vis.

Upatchede systemer åbner op for en række sårbarheder, herunder ransomware, RCE (fjernkode eksekvering), blandt flere.

Angrebsvektorer

Legacy systemer og Zero-days

- Uopdaterede systemer og zero-days er aårbarhder som cyberkriminelle udnytter til at skabe adgang til leverandører eller organisation.

Supply-chain angreb

- Via leverandører kan cyberkriminelle få adgang til interne systemer, særligt hvis leverandøren har for brede adgang som privilegerede- og admin konti.

Phishing-angreb

- Phishing angreb med malware er en kritisk sårbarhed, særlig hvis man har legacystemer som ikke er sikret tilstrækkeligt.

Mitigeringer

Leverandørstyring

- Stil høje sikkerhedskrav til leverandøren og sørg for, at der føres audit på leverandørens sikkerhed evt. i form af revisionserklæringer.

WAF

- Implementer Web Application Firewall (WAF[27]) foran legacy-systemerne for at sikre systemet yderligere.

OWASP

- Mitiger sårbarheder jf. OWASP top 10[28], som er top 10 sårbarheder på webapplikationer.

Segmentering

- Segmenter netværk og systemer så der kun kan etableres adgange, hvor der er et forretningsmæssigt behov.

Internet

- Minimer adgang til internet; er der ikke et forretningsmæssigt behov, skal systemet ikke have adgang.

Integrationer

- Minimer integrationer til andre systemer; malware kan komme via integrationer eller sprede sig til andre systemer fra et sårbart system.

Patch Management

- Sørg for at have tydelige og dokumenterede patch management-processer.

Observationer/hændelser

Der er i dag mange legacy-systemer i sundhedssektoren. Størstedelen er 'hegnet' ind ved segmentering og WAF-løsninger, men der er stadig sårbarheder på mange systemer, det gælder både kendt it og såkaldt skygge-it.

Sundheds-it er dyrt, og udbudsprocessen er lang og tidskrævende. Man skifter ikke bare et system ud som er dyrt og komplekst at implementere. Dette medvirker også til, at der er mange legacy-systemer i sundhedssektoren.

[27] https://www.f5.com/services/resources/glossary/web-application-firewall
[28] https://owasp.org/www-project-top-ten/

Epilog

Krigen i Ukraine og Ruslands konstante ransomware- eller wiperware-angreb gør truslen omkring legacy-systemer endnu større. Det er huller, som legacy-systemer eller zero-days, de cyberkriminelle forsøger at udnytte til at udføre angreb.

Trusselsvurdering – Legacy systemer

Mærkninger som CE og GXP er dyre for leverandører at få lavet. Derfor ønsker udviklere og leverandører også at få længst mulig levetid ud af mærkningerne. Det går desværre ud over cybersikkerheden i disse specialiserede it-systemer. Sundhedssektoren arbejder dagligt med at sikre legacy-systemer via WAF-løsninger eller segmentering.

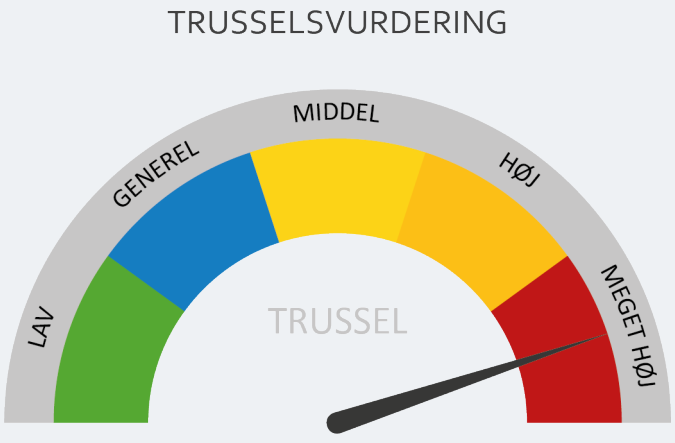
Der vil altid være et spørgsmål, om hvorvidt kritiske sundhedssystemer skal være præcise og redde liv, eller om de skal overholde best-practice patch-standarder for, at systemet er sikkert.

For at opnå den ønskede effekt med systemer, der er sikre og præcise at bruge for sundhedssektoren samtidig med, at cybersikkerheden følges, bør der fremadrettet stilles meget højere krav til leverandører af løsningerne om at overholde gængse patch management standarder.

Det vurderes, at der en MEGET HØJ hyppighed af legacy-systemer, og cyberkriminelle forventes også fremadrettet at forsøge at udnytte sektorens sårbarhed i angreb mod sektoren.

Et angreb mod et eller flere legacy vurderes at kunne have ALVORLIGE konsekvenser.

Angreb mod legacy-systemer vurderes at udgøre en MEGET HØJ trussel mod sundhedssektoren.



Øvrige væsentlige trusler

Fejl

Beskrivelse

Fejl omfatter dårlig proces, uforudsete fejl, fejlkonfigurering, tryk på forkert funktion/knap eller utilsigtet adgang til oplysninger, f.eks. pga. fejlindtastning eller fejljournalisering af oplysninger.

Fejl kan også opstå, hvis medarbejderen i god tro vælger at dele sit password med kolleger, undlader at følge koncernens regler for udformning af sikre passwords eller overfører følsomme data via private e-mailkonti eller usikre medier. Det kan f.eks. være forretningsdata, der sendes til en privat e-mail for, at medarbejderen kan arbejde hjemme på egen pc.

Trusselsvurdering - Fejl

De fleste alvorlige hændelser skyldes fejl begået af teknisk personale under ændringer eller

opdateringer af net- og informationssystemer. Der er set eksempler på, at fejl kan lede til en

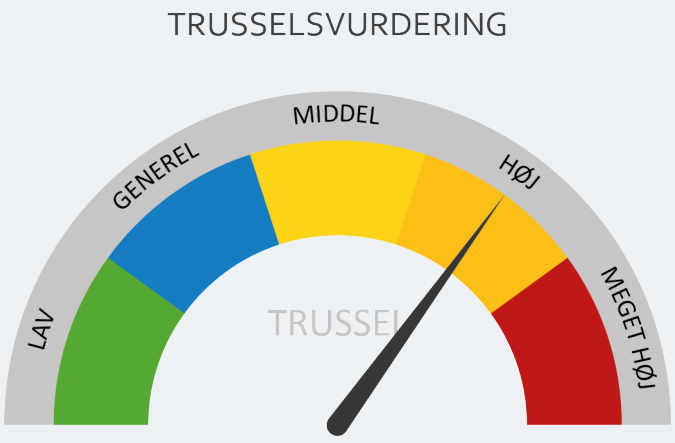
kompromittering af både fortrolighed, integritet og tilgængelighed, ligesom der er set eksempler på, at fejl både kan ramme nationale sundhedsløsninger og centrale løsninger ved aktørerne.

Ved hændelser med integritetsfejl er der ofte gået et par dage, inden hændelsen er kendt, og det kan tage lang til at opklare hændelsens omfang.

Ved hændelser med tab af tilgængelighed påvirker fejl ofte kontinuiteten af sundhedsydelserne.

Det vurderes, at der er en MEGET HØJ hyppighed af fejl. Fejl begået af teknisk personale, både ved aktører i sundhedssektoren og leverandører, vurderes at kunne lede til hændelser med ALVORLIGE konsekvenser, men det vurderes at være mest sandsynligt, at en fejl leder til en hændelse med begrænsede eller ingen konsekvenser.

Fejl vurderes at udgøre en HØJ trussel for sundhedssektoren.



Malware

Beskrivelse

Malware eller "ondsindet software/kode" er et begreb, der dækker over et ondsindet program eller kode, som er skadelig for net- og informationssystemer eller anvendes til at få uautoriseret adgang.

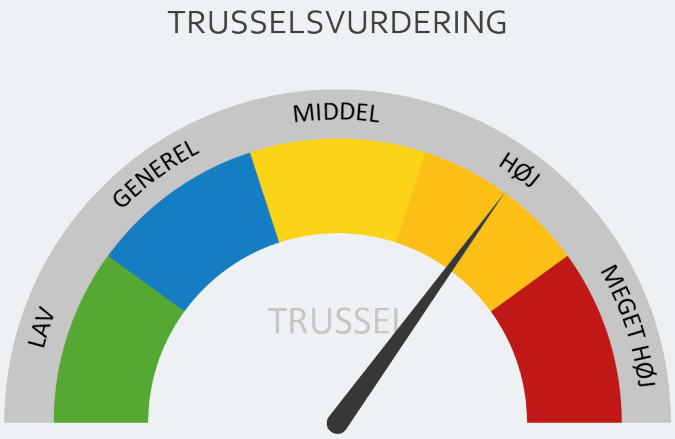
Malware kan have særlige egenskaber, f.eks. er der malware, der fungerer uden at placere eksekverbar programkode. Denne type malware er kendt som "Fileless malware". Der er en øget tendens til, at denne type malware indgår i cyberkriminelles angreb.

Malware kan også have egenskaber som en virus, hvilket vil sige, at den spreder sig fra enhed til enhed. Malwaren kan også have trojanske egenskaber, hvilket vil sige, at den er i stand til at udgive sig for at være legitim, mens den spreder sig selv fra enhed til enhed. Noget af den mest avancerede malware er polymorf eller metamorfisk i den forstand, at malwaren løbende ændrer signatur for at undgå detektering.

DCISsund vurderer, at ved databrud er malware ofte involveret, og der er ofte blevet anvendt en kombination af flere forskellige typer af malware. Et angreb kan fx involvere PowerShell (Fileless malware) til at få adgang, Emotet (Botnet og modular downloader) til opnå kontrol og downloade anden malware såsom TrickBot (oprindelige banking Trojan) til at undgå detektering, samt indsamling og læk af data og til sidst Ryuk (ransomware) til at kryptere filer.

Trusselsvurdering - Malware

Det vurderes, at der er en MEGET HØJ hyppighed af malware. Sundhedssektoren rammes hver dag af angreb, hvor der indgår malware, og det vurderes, at angreb eller skadevoldende aktivitet også fremadrettet er forventeligt. Malware anvendes ofte i hændelser, der er forbundet med ALVORLIGE konsekvenser for den organisation, der bliver ramt, og de borgere, hvorom der behandles oplysninger. Malwareangreb vurderes at udgøre en HØJ trussel for sundhedssektoren.



Remote Code Execution

Beskrivelse

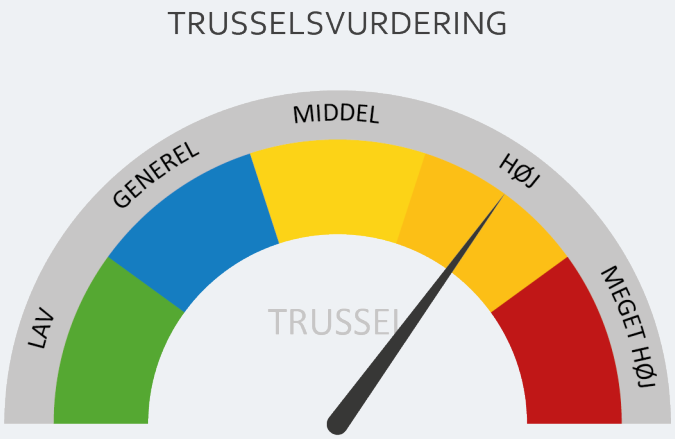
Remote Code Execution (RCE) er en hændelse, hvor angriberen på afstand, typisk over internettet, udnytter en sårbarhed til at eksekvere ondsindet kode eller software i det miljø, der angribes.

En angriber kan anvende en teknik kaldet ”code injection” til at eksekvere ondsindet kode i et RCE-angreb. Herved er angriberen begrænset af de muligheder, der er med den kode, der anvendes. Angriberen kan også anvende ”command injection”, hvorved en angriber kan eksekvere ondsindet kode i operativsystemet gennem en sårbar applikation. Ved denne type angreb får angriberen mulighed for at eksekvere system commands uden at skulle introducere egen kode.

Trusselsvurdering - RCE

Der opdages løbende nye sårbarheder, der kan udnyttes af angribere til at eksekvere ondsindet kode eller software i et offers net- og informationssystemer. Det vurderes, at hyppigheden er MEGET HØJ. Angreb, der anvender denne teknik, er ofte meget alvorlige, da denne form for angreb kan give angriberen fuld kontrol med store dele af det miljø, der angribes. Det vurderes, at de mulige konsekvenser ved RCE-angreb er ALVORLIGE.

RCE-angreb vurderes at udgøre en HØJ trussel for sundhedssektoren.



Webapplikationer

Beskrivelse

Angreb mod webapplikationer er direkte eller indirekte forsøg på at udnytte en sårbarhed i tjenester og applikationer på nettet. Dette kan være udnyttelse af API'er, runtime eller tjenester/services på internettet.

Webbaserede angreb er hændelser, hvor en angriber udnytter browsere og tjenester som primær vektor til at nå sit mål i et angreb. Webbaserede angreb omfatter udnyttelse af sårbarheder i browsere, tilføjelser til browsere, websteder, indhold og Content Management System (CMS) til at udføre drive-by kompromittering, watering-hole angreb, url redirection og man-in-the-browser angreb.

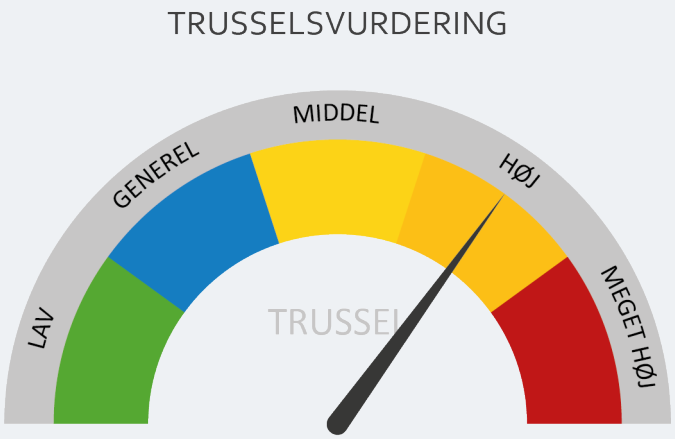
Trusselsvurdering - Webapplikationer

Det vurderes, at der en HØJ hyppighed af disse typer af angreb. The European Union Agency for Cybersecurity (ENISA) vurderer dog, at angreb mod sundhedssektoren, der involverer webapplikationer, er en faldende trend.

Generelt vurderes det, at webbaserede angreb indgår i få af de angreb, der målrettes sundhedssektoren, men at sundhedssektoren er sårbar, da Internet Explorer er en af de mest anvendte browsere i sektoren. DCISsund kender ikke til angreb i den danske sundhedssektor, hvor denne teknik har haft betydning for forløbet af et angreb.

I angreb mod webapplikationer og web-baserede angreb er formålet ofte tyveri af personhenførbare informationer. Det vurderes, at denne teknik kan anvendes i angreb med ALVORLIGE konsekvenser.

Denne type af angreb vurderes at udgøre en HØJ trussel for sundhedssektoren.



Botnets

Beskrivelse

En 'bot' er kode eller software, der kører nogle automatiske processer, der typisk er simple. Et 'botnet' er en sammenkobling af flere enheder over internettet, der sammen eller uafhængigt kører en eller flere bots.

Der findes mange forskellige bots og botnets, der anvendes til forskellige formål i forbindelse med angreb mod sundhedssektoren. Bots anvendes til Denial-of-Service (DoS) angreb, at stjæle data, sende spam og til at give angriberen adgang til en enhed og dens forbindelser.

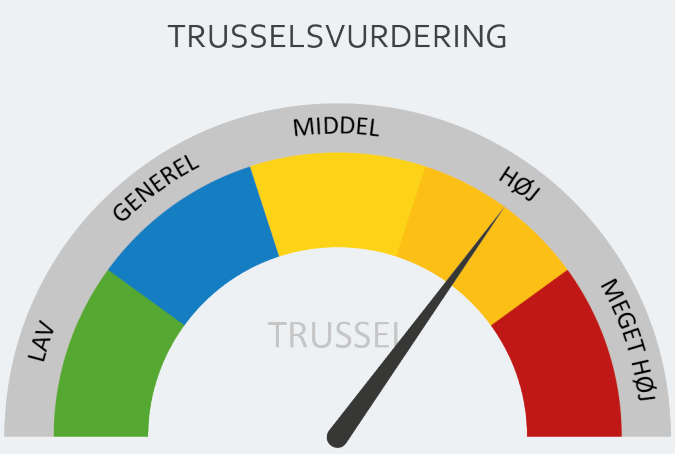
Trusselsvurdering - Botnets

Det vurderes, at der en MEGET HØJ hyppighed af denne type angreb, og at ondsindede aktører fremadrettet vil anvende botnets i angreb mod den danske sundhedssektor.

Det vurderes, at sundhedssektorens sikkerhedsforanstaltninger overordnet set er delvist effektive.

Mange af de hacking- eller malwareangreb, som målrettes eller rammer sundhedssektoren, anvender botnets til at stjæle data, sende spam og til Command and Control, hvorfor de mulige konsekvenser vurderes at være ALVORLIGE.

Botnets vurderes at udgøre en HØJ trussel for sundhedssektoren.



Misbrug af legitime adgange

Beskrivelse

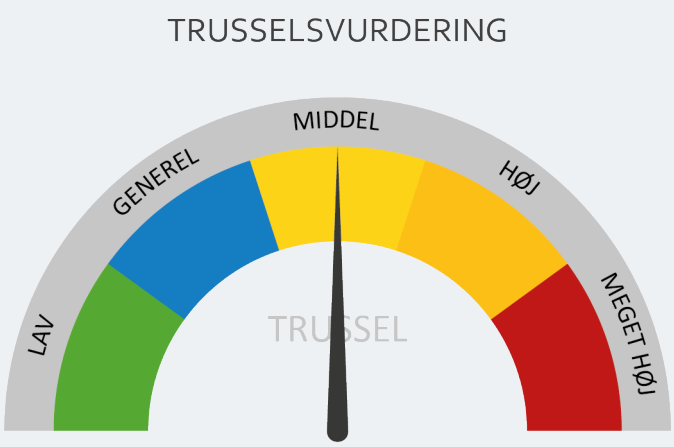
Medarbejdere kan af flere grunde vælge at handle imod behandlingsinstrukserne og således behandle data til usaglige eller ulovlige formål. Der er især en risiko i forbindelse med behandlingen af helbredsoplysninger og ved økonomisystemer.

Trusselsvurdering – Misbrug af legitime adgange

Der er flere gange set eksempler på uberettigede opslag, og det vurderes, at der er en MEGET HØJ hyppighed heraf. Der er ikke nye eksempler på misbrug af legitime adgange til økonomisk svindel i sektoren, og det vurderes, at der er en meget lav sårbarhed. På grund af sektorens foranstaltninger, fx Min Log, eller når aktører laver kontrol af behandlerrelationer, opdages det ofte, når en medarbejder har lavet uberettigede opslag.

Det vurderes, at der kan forekomme hændelser med MINIMALE konsekvenser.

Misbrug af legitime adgange vurderes at udgøre en MIDDEL trussel for sundhedssektoren.



Cryptomining

Beskrivelse

Cryptomining er generering af en ny kryptovaluta, og cryptojacking er uautoriseret udnyttelse af systemressourcer til at generere kryptovaluta.

Cryptomining er forbundet med ekstremt høj processoraktivitet og tilhørende strømforbrug. Cryptomining er blevet påvist på flere forskellige platforme, og da cryptomining-software udnytter de samme muligheder og sårbarheder som anden malware, er det noget, der rammer både enkeltpersoner og større organisationer.

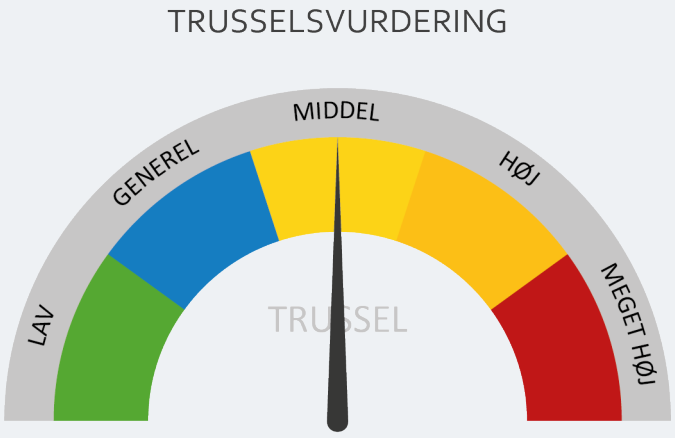
Trusselsvurdering - Cryptomining

følge ENISA var 2018 året for cryptomining, hvor eksisterende botnets og trojans blev udnyttet til at sprede cryptomining-software. Siden 2017 har angribere anvendt en teknik kendt som Drive-by cryptomining, hvor angribere anvender et simpelt JavaScript til at foretage et browserbaseret angreb. Denne metode gør det muligt at udføre den ondsindede aktivitet direkte i ofrets browser uden at installere nogen software.

Siden 2018 har der været en nedadgående trend, og DCISsund har ikke kendskab til angreb, hvor computerkræften i den danske sundhedssektor har været udnyttet af kriminelle til cryptomining. Det vurderes dog, at der fortsat er en MEGET HØJ hyppighed.

Det vurderes, at cryptojacking, som det udføres i dag, ikke vil lede til væsentlige konsekvenser for den fortsatte drift af sektorens ydelser eller sundhedssektoren som helhed. Det kan dog lede til mindre konsekvenser for den enkelte aktør. Det vurderes, at der kan forekomme hændelser med MINIMALE konsekvenser.

Cryptomining vurderes at udgøre en MIDDEL trussel for sundhedssektoren.



Denial of Service

Beskrivelse

I et Denial of Service-angreb (DoS-angreb) udnytter en angriber kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside (web-server) eller et netværk, således at hjemmesiden eller netværket overbelastes. Imens angrebet står på, er hjemmesiden eller netværket utilgængelig for legitim trafik.

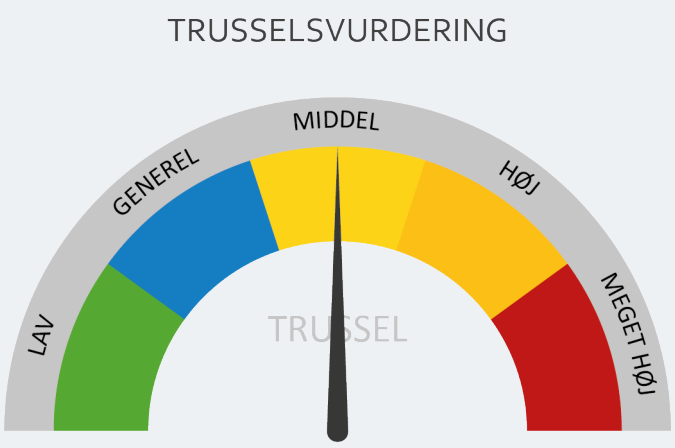
Trusselsvurdering – Denial of Service

Der har både været indrapporteret informationer om Distributed Denial of Service-angreb (DDoS-angreb) og Telephone Denial of Service-angreb (TDoS-angreb) mod sundhedssektoren, og der er flere eksempler på DDoS-angreb i andre sektorer. Det vurderes, at der er en MEGET HØJ hyppighed.

Borgernes adgang til sundhedsoplysninger kunne blokeres i et DDoS-angreb, og en avanceret aktør kunne i et målrettet angreb gå efter specifikke dele af sundhedssektorens infrastruktur. Det vurderes, at der er en generel trussel, og at cyberkriminelle eller aktivister har kapacitet og/eller interesse i at foretage et angreb.

Et DoS-angreb vurderes at kunne lede til en mindre nedgang i sektorens serviceniveau. Forpligtelser over for borgeren vurderes at kunne overholdes. Det vurderes, at skulle sektoren blive ramt af et DoS-angreb, er det mest sandsynligt, at det vil lede til MINIMALE konsekvenser.

DoS-angreb vurderes at udgøre en MIDDEL trussel for sundhedssektoren.



Business E-mail Compromise

Beskrivelse

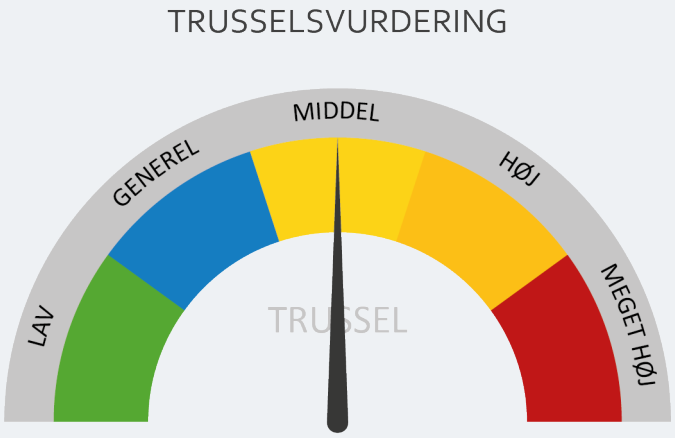
Business E-mail Compromise (BEC) er, når en angriber i en e-mail udgiver sig for at være direktøren i en kommune, region eller styrelse. Disse angreb sker oftest op til og/eller under sommerferien eller helligdagene omkring jul. Disse angreb er oftest rettet mod enkeltpersoner og er ofte dårligt udført.

Trusselsvurdering - BEC

Sundhedssektoren rammes ofte af simple BEC-angreb fra e-mails, der nemt genkendes som ondsindede. Det vurderes, at der er en MEGET HØJ hyppighed.

Der har været mere komplicerede angreb, hvor en angriber kompromitterede en e-mailkonto hos en leverandør til sektoren og over flere måneder fulgte med i kommunikationen for at kunne slå til og ændre eksisterende fakturaer eller oprette/målrette nye fakturaer med henblik på økonomisk vinding. Typisk er der tale om mindre beløb for sektoren, men for medarbejderen, der nogle gange overfører egne penge, kan det udgøre et større problem. I de mere avancerede angreb kan der være tale om større beløb, men her er sektoren på grund af finansielle kontroller mere robust. Det vurderes, at der kan være tale om hændelser med MINIMALE konsekvenser.

BEC-angreb vurderes at udgøre en MIDDEL trussel for sundhedssektoren.



Deepfake og AI

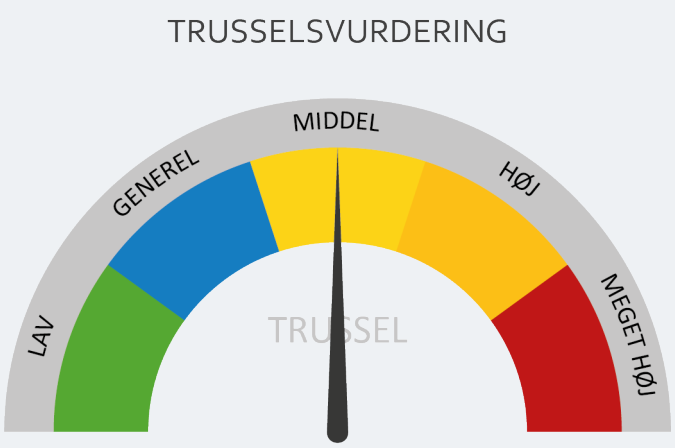
Beskrivelse

Identitetssvindel er bestemt ikke nyt, idet cyberkriminelle bliver mere og mere dygtige til at kombinere lækkede personlige oplysninger med tilgængelige data på internettet og sociale medieprofiler. Fremskridt inden for AI-teknologi gør det muligt for cyberkriminelle effektivt at efterligne menneskers stemmer og ansigter og dermed omgå verifikationskontroller. De kan derefter bruge tilgængelig information og AI til at generere nye syntetiske profiler med dokumenter, ansigtsbilleder og stemmekloning for at ansøge om lån og kræve sociale ydelser. Dette skaber ikke kun yderligere udfordringer for virksomheder til at autentificere deres kunder, men det kan også udgøre alvorlige økonomiske og personlige risici for enkeltpersoner. For eksempel vælger mange trusselsaktører at målrette mod mindreårige internetbrugere for at udføre syntetisk identitetssvindel.

Trusselsvurdering – Deepfake og AI

Deepfake-indhold er meget overbevisende, og den igangværende udvikling af deepfake-teknologi har gjort det vanskeligere at skelne mellem ægte og falsk indhold. Mens deepfake-teknologi stadig er relativt ny, ses dens rolle i nye tendenser til svig og cyberkriminalitet. Dette er blevet en voksende bekymring blandt forbrugere og organisationer, da deepfake udnyttes af kriminelle til at udføre social engineering-angreb, spredning af misinformation og svindel.

Det vurderes, at der er LAV, men stigende hyppighed inden for deepfake og sammenholdt med den potentielle MEGET HØJE konsekvens, vurderes deepfake-teknologien at udgøre en MIDDEL trussel for sundhedssektoren.



Konklusion og anbefalinger

I Trusselsbillede 2022 for sundhedssektoren giver DCISSund sit bud på de væsentligste trusler for sektoren baseret på en trendanalyse af cyberkriminelles taktik, teknikker og procedurer (TTP'er) samt rapporter fra en række lukkede og åbne kilder giver. På baggrund af indeværende rapport og de findings, den har afstedkommet, anbefaler DCIS følgende mitigeringer til sundhedssektoren, som går på tværs af alle de største trusler, som er bekrevet i rapporten.

Anbefalingerne tager hovedsageligt afsæt i hændelser og tendenser set i 2021, men da særligt en storpolitisk begivenhed, krigen i Ukraine, har forrykket rammerne for hvilke lande og institutioner, der må anses som særligt sårbare, har DCIS også haft denne konflikt med som fokus i anbefalingerne.

Beredskab

- Gennemgå beredskabsplaner, herunder nødplaner, med henblik på at sikre at beredskabsplaner er opdaterede. Sørg for at kontaktoplysninger og -lister er opdaterede, samt at alle relevante personer er bekendt med beredskabsplanen og deres ansvar og rolle i beredskabet.
- Beredskabsplaner og tilhørende dokumenter bør være tilgængelige offline, og krisestaben bør have en fysisk kopi på kontoret og hjemme.
- Test at sekundære kommunikationsmidler fungerer i tilfælde af, at it-systemer er utilgængelige.
- Overvej jeres procedure for aktivering af beredskab; kan krisestabens medlemmer for eksempel blive hentet af politiet for at kunne møde i krisestaben, såfremt der ikke er telefonkontakt?

Patch Management

- Patch Management gælder al hardware, mobile enheder, operativsystemer, software og applikationer, cloudløsninger og CMS. Anvend et centralt patch management-system. Implementer en applikations whitelist samt softwarerestriktionspolitikker (SRP) for at forhindre kørsel af programmer på typiske 'ransomware-placeringer' såsom midlertidige mapper.
- Benyt sårbarhedsscanninger på systemerne og prioriter opdatering ift. kritikalitet.

Backup / Restore

- Tag backup af de mest kritiske systemer og data og anvend et sikkerhedskopieringssystem, der gør det muligt at gemme flere iterationer i tilfælde af, at sikkerhedskopierne bliver krypterede af cyberkriminelle eller, at backuppen indeholder inficerede filer. Test rutinemæssigt sikkerhedskopier for dataintegritet og for at sikre, at de kan gendannes. Overvej offline backups samt at kryptere backuppen.

- Hold credentials, der har adgang til/styrer/kan slette backup, hermetisk adskilt fra almindeligt AD.
- Sørg for at teste backups jævnligt ved at køre en restore og test indholdets integritet.

Segmentering og principperne for least privilege

- Segmenter fysiske og logiske netværk samt data. Virtualisér hvor det er muligt, og indfør princippet om administration med minimumsrettigheder (least privilege).

Leverandørstyring

- Stil høje sikkerhedskrav til leverandøren og sørg for, at der føres audit på leverandørens sikkerhed evt. i form af revisionserklæringer.

Awareness

- Tilbyd medarbejderne awareness-træning med særligt fokus på social engineering og phishing. Her undervises medarbejderne i at genkende mistænkelige e-mails, mistænkelige links eller vedhæftede filer og til at udvise forsigtighed, inden de besøger ukendte websteder.
- Overvej at tilføje et advarselsbanner til alle e-mails fra eksterne kilder, der minder brugerne om risiciene ved at klikke på links og åbne vedhæftede filer.
- Overvej derudover at gennemføre f.eks. phishing-kampagner, hvor medarbejdere bliver testet.

Videndeling

- Deltag i netværk hvor man deler information om hændelser, IoC'er, varsler mv, såsom MS-ISAC, DKCERT, DCISvarsel, MISP m.fl.

Sundhedssektorens decentrale cyber- og informationssikkerhedsenhed

I 2018 udgav regeringen "National strategi for cyber- og informationssikkerhed 2018-2021", som skulle bidrage til at øge den tekniske robusthed og sikre bedre beskyttelse af statens kritiske it-systemer, øge viden og kompetencer hos borgere, virksomheder og myndigheder samt styrke den nationale koordinering og samarbejdet om informationssikkerhed.

Her blev seks kritiske sektorer udpeget til at etablere en decentral cyber- og informationssikkerhedsenhed (DCISsund) samt udarbejde deres egen sektorspecifikke strategi for cyber- og informationssikkerhed, som herefter skulle udmøntes gennem den pågældende sektors DCISsund.

Sundhedssektorens DCISsund blev oprettet i januar 2019. Siden oprettelsen har enheden arbejdet målrettet med 17 initiativer (projekter). Formålet med initiativerne er at styrke arbejdet med cyber- og informationssikkerhed i sektoren ud fra et helhedsorienteret perspektiv.

Initiativerne er fordel på fire spor; Forudsige, Forebygge, Opdage, Håndtere. Sammen med sektorens aktører arbejder DCISsund med udmøntningen af initiativerne med fokus på at skabe værdi både lokalt og nationalt.

Samarbejdet har været frugtbart, og der er i løbet af de første tre år blevet løst mange opgaver af betydning for sektorens cyber- og informationssikkerhed. DCISsund ser derfor frem til også i de kommende år at fortsætte samarbejdet om at udmønte og designe løsninger, der kan øge kapacitet og kapabilitet i sektoren.

DCISsund er kontaktpunkt for sektorens aktører og Center for Cybersikkerhed (CFCS) ift. håndtering af varsler, hændelser samt koordinering på tværs. I den forbindelse har DCISsund bl.a. løst følgende opgaver:

- Udvikling af et varselssystem, hvor aktører kan få akutte varsler hurtigt og målrettet.
- Etablering af en vagtordning, som CFCS og sektorens aktører kan kontakte 24/7, såfremt der er hændelser eller indikationer på et igangværende angreb.
- Opbygning af et beredskab der kan understøtte indsatser, der rammer på tværs af aktører.
- Opbygget en indsigt i tværgående kritiske systemer og sektorens risikobillede via andre initiativer i strategien. DCISsund kan på den baggrund rådgive om hvilke indsatser, der bedst hjælper sektoren samt vejlede, når der skal prioriteres ud fra en risikobaseret tilgang.