CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien

Formålet med denne trusselsvurdering er at opdatere trusselsbilledet for de alvorligste cybertrusler, cyberkriminalitet og cyberspionage, i lyset af den nuværende COVID-19-pandemi.

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. udgave april 2020

Hovedvurderinger

- Cybertruslen er fortsat en alvorlig trussel mod Danmark.
- Hackere forsøger at udnytte COVID-19-pandemien til deres fordel. Det udgør et nyt element i det samlede trusselsbillede, mens de generelle cybertrusler ikke har ændret sig markant. Pandemien har således primært påvirket trusselsbilledet ift. hvilke angrebsmetoder, hackerne vælger.
- De ændringer, som pandemien har medført for arbejdsvilkårene for mange myndigheder og virksomheder, kan dog samtidig øge risikoen for, at hackere lykkes med deres cyberangreb.
- Truslen fra cyberkriminalitet er **MEGET HØJ**. Truslen er rettet mod alle. Der er uafhængigt af COVID-19-pandemien en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder, og såfremt de rammer vitale dele af det danske samfund, som for eksempel sundhedssektoren, kan de få alvorlige konsekvenser.
- Truslen fra cyberspionage er **MEGET HØJ**. Truslen er især rettet mod myndigheder, der arbejder med udenrigs- og sikkerhedspolitik, samt virksomheder med viden, som andre stater har interesse i. Blandt andet sundhedssektoren har en sådan viden.

Indledning

Truslen fra hhv. cyberspionage og cyberkriminalitet er fortsat **MEGET HØJ**. Cybertruslen er dermed en alvorlig trussel mod Danmark. Det vil den blive ved med at være i fremtiden i takt med den fortsatte digitalisering og afhængighed af digitale tjenester.

Der er altid hackere, der forsøger at udnytte aktuelle begivenheder, udviklinger eller vilkår til deres fordel. Det er også tilfældet med COVID-19-pandemien, som hackere eksempelvis har udnyttet ved at sende phishing-mails med COVID-19 som tema. Udnyttelsen af COVID-19 udgør et nyt element i det samlede trusselsbillede, men truslerne har på nuværende tidspunkt derudover ikke ændret sig markant. COVID-19 har primært påvirket trusselsbilledet ift. hvilke angrebsmetoder, hackerne vælger.

De ændringer, som pandemien har medført for arbejdsvilkårene for mange myndigheder og virksomheder, kan dog øge risikoen for, at hackere lykkes med deres cyberangreb. Dette adresseres i følgende afsnit.

Der er en øget risiko for, at cyberangreb lykkes under COVID-19 pandemien

Myndigheder og virksomheder kan være mere sårbare under den igangværende COVID-19-pandemi. It-sikkerheden i mange myndigheders og virksomheders netværk er under pres fra det ændrede brugsmønster i form af nye hjemmearbejdspladser, og fordi tilgængeligheden af systemerne prioriteres højt. De nye arbejdsvilkår kan give hackere lettere adgang til organisationernes systemer og gøre det sværere at opdage hackerne i systemerne.

Selvom trusselbilledet grundlæggende er uændret, kan myndigheder og virksomheder derfor stå over for et ændret risikobillede.

Et af de forhold, der kan gøre organisationer mere sårbare, er, hvis sædvanlige sikkerhedsforanstaltninger ikke opretholdes eller gennemføres rutinemæssigt. Det kan f.eks. dreje sig om system- og softwareopdateringer, fravalg af VPN-forbindelse eller flerfaktorgodkendelse. Herudover kan begrænsninger i ressourcer også være et problem, f.eks. i forhold til at opdage og effektivt håndtere cyberangreb.

Hvis danske myndigheder eller virksomheder, der leverer samfundsvigtige ydelser, bliver ramt af f.eks. et ransomware-angreb under pandemien, vil det kunne medføre særligt store konsekvenser for hele Danmark.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) har udarbejdet en række vejledninger til, hvordan man kan styrke cybersikkerheden. De kan findes på CFCS' hjemmeside, www.cfcs.dk.

Cyberkriminalitet

Truslen fra cyberkriminalitet er **MEGET HØJ.** Det betyder, at det er meget sandsynligt, at danske virksomheder og myndigheder vil blive udsat for forsøg på cyberkriminalitet på kort sigt.

Cyberkriminalitet er i denne vurdering en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, som er motiveret af ønsket om økonomisk berigelse.

Cyberkriminalitet udgør en vedvarende og aktiv trussel mod alle danske myndigheder, virksomheder og borgere.

Cyberkriminelle udfører oftest relativt simple angreb mod mange potentielle ofre på én gang, bl.a. gennem phishing-angreb. Der findes dog også netværk med kapacitet til at udføre mere komplekse og tidskrævende cyberangreb, herunder målrettede ransomware-angreb.

Cyberangreb fra kriminelle grupper starter typisk, uden at aktøren på forhånd har udset sig et specifikt offer. De fleste cyberangreb starter som opportunistiske angreb, hvor eksempelvis phishing-mails bliver spredt til tusinder af ofre, eller hvor kriminelle misbruger it-systemer og enheder med kendte sårbarheder.

Cyberkriminelle forsøger at udnytte danskernes interesse i COVID-19

CFCS har viden om, at der under COVID-19-pandemien bliver sendt flere phishing-mails til danske myndigheder og virksomheder end normalt. Flere sikkerhedsfirmaer rapporterer også om en stigning i phishing i andre lande den seneste måned.

Mange af disse phishing-mails misbruger COVID-19 som tema for at øge sandsynligheden for, at modtageren åbner mailen og klikker på links eller vedhæftede filer. Hackerne forsøger dermed at udnytte danskernes efterspørgsel på viden om COVID-19 og den nuværende sundhedskrise.

Under COVID-19-pandemien er der blevet oprettet en relativt stor mængde falske domæner, som bl.a. udnyttes af hackere til at franarre danske borgere deres NEMID-oplysninger og andre loginoplysninger. En del af de falske domæner lægger sig tæt op ad legitime sundhedsmyndigheders hjemmesider og navne. CFCS samarbejder med andre aktører på at få nedtaget erkendte falske domæner.

Der er ydermere set falske applikationer og malware rettet mod mobile enheder, som udnytter COVID-19 som tema. De falske apps kan eksempelvis stjæle informationer fra den mobile enhed.

CFCS vurderer, at kriminelle fremadrettet også vil forsøge at udnytte statslige kompensationsordninger som tema i deres phishing-mails.

Cyberkriminelle udnytter sårbarheder og at mange arbejder hjemme

Cyberkriminelle udnytter løbende nye sårbarheder. Der går ofte ikke mere end et par uger fra en teknisk sårbarhed bliver offentligt kendt, til den bliver brugt til at forsøge at hacke danske mål med.

Det høje angrebstempo stiller store krav til, at it-afdelingerne i danske myndigheder og virksomheder opdaterer systemer og programmer i tide eller får opsat kompenserende foranstaltninger i de tilfælde, hvor det ikke er muligt at lukke en sårbarhed. Det er også gældende under COVID-19-pandemien. Blandt andet i relation til at sikre fjernadgange,

såsom VPN-løsninger, samt de klienter, som kan bruge disse fjernadgange.

Der er medierapporter om, at hackere under COVID-19-pandemien forsøger at udnytte, at der er et øget behov for fjernadgange, VPN-løsninger samt samarbejds- og kommunikationsplatforme.

Cyberkriminelle har eksempelvis udviklet et nyt modul til den meget udbredte malware TrickBot. Modulet er specifikt designet til at foretage brute-force angreb mod Remote Desktop Protocol-adgange (RDP-adgange). Trickbot benyttes til flere forskellige typer angreb, herunder målrettede ransomware-angreb.

Der er ifølge it-sikkerheds-selskaber hackere, der udbyder decideret falske VPN-løsninger. Der er også rapporter om, at der er blevet oprettet falske domæner, der lægger sig tæt op ad samarbejds- og kommunikationsplatformen Zoom.

Der er derudover set eksempler på, at medarbejdere og borgere bliver ringet op af kriminelle, der udgiver sig for eksempelvis at være it-personel. De kriminelle forsøger at lokke følsomme informationer fra medarbejderne eller at få dem til at downloade filer inficeret med malware.

Udover ændringer i angrebsmetoder er det muligt, at der sker stigninger i visse angrebsformer, som hackerne tror vil være mere effektive, fordi mange arbejder hjemmefra. Det kan f.eks. være BEC-svindel, også kendt som direktørsvindel, hvor hackere forsøger at franarre virksomheder og organisationer penge gennem falske anmodninger om pengeoverførelser. Hackerne udgiver sig i denne type angreb for at være f.eks. chefer eller kollegaer for at lokke ansatte til at agere i den tro, at det er efter ordre fra ledelsen.

En anden angrebsform, der kan stige, er overbelastningsangreb, herunder DDoS-angreb, hvor hackerne forlanger betaling for at stoppe angrebene. Mange myndigheder og virksomheder er lige nu mere afhængige af internettet, hvilket kan øge hackeres interesse i den angrebsmetode.

CFCS vurderer, at de fleste DDoS-angreb dog udføres af enkeltpersoner, hvor formålet primært er spænding eller chikane. Selvom de fleste angreb er små og ikke truer samfundsvigtige funktioner, så findes der i denne gruppe også aktører, som er i stand til selv at udføre kraftige DDoS-angreb eller købe dem af andre.

Truslen fra målrettede ransomware-angreb er stigende
Der er en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder. Denne stigning finder sted uafhængigt af COVID-19-pandemien.

Et målrettet ransomware-angreb mod danske myndigheder og virksomheder vil ikke kun påvirke den enkelte organisation, men kan potentielt også påvirke samfundsvigtige ydelser. Det har f.eks. været tilfældet i forbindelse med ransomware-angreb mod sundhedssektoren i

bl.a. USA og Storbritannien, hvor nedetid i administrative systemer medførte, at patientaftaler måtte aflyses. Et vellykket målrettet ransomware-angreb mod sundhedssektoren i Danmark vil kunne øge det pres, som sektoren oplever lige nu pga. COVID-19.

I målrettede ransomware-angreb forsøger kriminelle at afpresse myndigheder og virksomheder for store pengebeløb ved at kryptere centrale dele af offerets it-systemer ved hjælp af ransomware.

Siden slutningen af 2019 er der eksempler på, at hackere, der står bag målrettede ransomware-angreb, nu også lækker følsomme data indsamlet fra det ramte system, hvis offeret ikke betaler løsesummen.

Målrettede ransomware-angreb har ramt enkelte danske virksomheder. I efteråret 2019 har to danske virksomheder, Demant og Global-Connect, eksempelvis været udsat for separate ransomware-angreb. Angrebet på Demant medførte ifølge virksomheden et tab på op mod 650 mio. kr. I februar 2020 blev den internationale servicevirksomhed ISS ramt af et ransomware-angreb, der også påvirkede den danske del af virksomheden, med store økonomiske konsekvenser til følge.

Kriminelle sælger adgange, der bliver brugt i målrettede angreb
Der er et samarbejde mellem de kriminelle, der udfører mere målrettede angreb, og de kriminelle, der rammer tusindvis af ofre gennem bl.a. phishing. Målrettede ransomware-angreb udføres ofte efter en indledende opportunistisk kompromittering af offeret med malware spredt gennem phishing. Videregivelse og salg af disse indledende kompromitteringer kaldes for access-as-a-service.

Massekompromitteringer gennem phishing udgør derfor ikke kun en trussel i sig selv, men understøtter også den stigende trussel fra målrettede cyberangreb udført af kriminelle.

Cyberspionage

Truslen fra cyberspionage er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at danske myndigheder og virksomheder vil blive udsat for forsøg på cyberspionage inden for kort sigt.

Danmark er udsat for både politisk og kommercielt motiveret cyberspionage fra fremmede stater.

Det er en vedvarende trussel, der også gælder under den nuværende COVID-19-pandemi. Fremmede stater misbruger ligesom cyberkriminelle COVID-19 som tema i deres phishing- og spear phishing-mails.

Fremmede stater ved, at danske myndigheder og virksomheder har andre arbejdsvilkår under krisen, der kan gøre dem sårbare, og fremmede stater er hurtige til at udnytte sårbarheder.

Truslen er også under COVID-19-pandemien især rettet mod danske myndigheder, der arbejder med udenrigs- og sikkerhedspolitik, samt virksomheder med viden, som andre stater har interesse i.

Leverandører og samarbejdspartnere til disse myndigheder og virksomheder kan også blive udsat for forsøg på cyberspionage med det formål at misbruge dem som trædesten i forsøg på at opnå adgang til myndighederne og virksomhederne. Visse underleverandører eller samarbejdspartnere har måske ikke en viden, der er interessant for fremmede lande, men de kan til gengæld have en adgang eller troværdighed, hackerne kan udnytte til at kompromittere deres egentlige mål.

Cyberspionage kan føre til pres på danske beslutningstagere
Det er sandsynligt, at fremmede stater forsøger at bruge cyberspionage som et middel til at opnå viden om danske interesser, overvejelser og beslutninger i forbindelse med større internationale sager eller udenrigspolitiske forhandlinger. Den viden kan staterne bl.a. udnytte til at modarbejde danske interesser eller sætte danske forhandlere og beslutningstagere under pres.

Særligt Rusland og Kina råder over meget væsentlige cyberkapaciteter og begge lande bruger deres kapaciteter aktivt på globalt plan. Det er sandsynligt, at bl.a. Iran også udfører cyberspionage og andre typer cyberangreb mod mål i og uden for deres nærområde.

Cyberspionage kan skade dansk konkurrenceevne og økonomi
Stater bruger også cyberspionage med det formål at styrke deres nationale udvikling og konkurrenceevne. Den form for cyberspionage retter sig især mod virksomheder og institutioner, der har en viden, som fremmede stater har interesse i.

Staterne kan bruge den stjålne information til at understøtte udviklingen af deres nationale sektorer, som kan springe flere led af deres innovations- og udviklingsproces over.

Det kan skade Danmarks konkurrenceevne og derved dansk økonomi, hvis danske virksomheder udsættes for cyberspionage, især inden for områder hvor danske virksomheder besidder en konkurrencestærk viden.

Forskning relateret til COVID-19 er et eksempel på viden, der kan have værdi for fremmede stater. CFCS vurderer, uafhængigt af COVID-19-pandemien, at fremmede stater særligt har interesse i de dele af sundhedssektoren, der har adgang til forskningsdata eller intellektuel ejendom. Det er f.eks. virksomheder og universiteter, der bl.a. beskæftiger sig med biokemi, biotek og lægemidler.

Grænsen mellem denne kommercielt motiverede og den sikkerhedspolitisk motiverede cyberspionage kan være overlappende.

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