CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Truslen fra cyber-spionage mod dansk forskning og universiteter

1. udgave september 2021

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave september 2021

Truslen fra cyberspionage mod dansk forskning og universiteter

Formålet med trusselsvurderingen er at informere om cybertrusler rettet mod danske universiteter og forskningsinstitutioner. Trusselsvurderingen kan blandt andet bruges i institutionernes videre arbejde med risikovurderinger. Målgruppen for trusselsvurderingen er primært ledelsen og it-medarbejdere hos danske universiteter og forskningsinstitutioner.

Hovedvurdering

- Danske universiteter og forskningsinstitutioner er udsat for en **MEGET HØJ** trussel fra cyberspionage. Truslen er dermed steget fra **HØJ** til **MEGET HØJ** siden seneste vurdering i 2018**.**

- Der er en vedvarende trussel fra cyberspionage mod universiteter og forskningsinstitutioner. Truslen kommer fra flere fremmede stater, der angriber forskning verden over. Truslen fra cyberspionage er også rettet mod danske universiteter og forskningsinstitutioner, der i flere tilfælde er blevet forsøgt ramt af cyberangreb.

- Hackere forsøger ofte at få adgang til universiteters tværgående it-netværk, såsom mailsystemer. Det giver dem mulighed for at spionere mod flere fagområder inden for de enkelte universiteter på samme tid.

- Der er ikke et entydigt billede af, hvad fremmede stater går efter, når de udfører cyberspionage mod forskning. Konkrete sager i og uden for Danmark viser dog, at nogle fagområder sandsynligvis er udsat for en særlig interesse fra fremmede aktører.

- Fremmede stater har et særligt fokus på såkaldt dual-use teknologi og forskning i dual-use teknologi. Det betyder, at forskning inden for teknologier og anvendelse af teknologier, der kan benyttes til både civile og militære formål, er et særligt mål for cyberspionage.

- Danske universiteter og forskningsinstitutioner er også udsat for en **MEGET HØJ** trussel fra cyberkriminalitet. Universiteter kan f.eks., ligesom mål i mange andre sektorer, blive ramt af målrettede ransomware-angreb.

Analyse

Danske og udenlandske universiteter og forskningsinstitutioner bliver løbende udsat for cyberangreb fra statsstøttede og kriminelle hackere.

Denne trusselsvurdering fokuserer primært på truslen fra cyberspionage mod danske universiteter og forskning. CFCS har tidligere vurderet truslen fra cyberspionage mod danske universiteter i "Trusselsvurdering: Danske universiteter er mål for cyberangreb" fra 2018. CFCS hæver i denne vurdering trusselsniveauet fra **HØJ** til **MEGET HØJ.** CFCS hæver trusselsniveauet for cyberspionage, da universiteter og forskningsinstitutioner i og uden for Danmark er udsat for en vedvarende trussel fra cyberspionage, der bliver afspejlet i cyberangreb rettet mod forskning.

Det betyder, at det er meget sandsynligt, at danske universiteter og forskningsinstitutioner vil blive udsat for forsøg på cyberspionage inden for de næste to år.

Udover truslen fra cyberspionage er dansk forskning og universiteter også udsat for en **MEGET HØJ** trussel fra cyberkriminalitet. Truslen fra kriminelle hackere er beskrevet kort i slutningen af vurderingen.

Danske universiteter og forskningsinstitutioner er også udsat for en **LAV** trussel fra destruktive cyberangreb og cyberaktivisme. De to trusler bliver ikke yderligere beskrevet i denne trusselsvurdering.

Cybertruslerne mod dansk forskning og universiteter ligger på de samme trusselsniveauer, som truslerne mod Danmark samlet set. CFCS anbefaler alle danske universiteter og forskningsinstitutioner at følge beskrivelsen af trusselsbilledet på CFCS' hjemmeside og bl.a. læse den årlige vurdering af cybertruslen mod Danmark.

Forskning er et attraktivt og vedvarende cyberspionagemål

Der er en vedvarende trussel fra cyberspionage mod universiteter og forskningsinstitutioner. Truslen kommer fra flere fremmede stater, der angriber forskning verden over. Truslen fra cyberspionage er også rettet mod danske universiteter og forskningsinstitutioner, der i flere tilfælde er blevet ramt af forsøg på cyberangreb.

Fremmede stater har forskellige formål med at udføre cyberspionage mod forskningsinstitutioner og universiteter. Cyberspionage er i nogle tilfælde drevet af en interesse for at opnå konkurrencemæssige og strategiske fordele ved at stjæle sensitiv eller værdifuld viden. Nogle fremmede stater spionerer sandsynligvis også for at fremskynde national forskning og udvikling af samfundsmæssige ydelser, såsom bedre kritisk infrastruktur.

Hackere bruger flere forskellige angrebsmetoder i deres forsøg på at kompromittere danske universiteter og forskningsinstitutioner. I og uden for Danmark har forskningsinstitutioner og universiteter særligt været udsat for spearphishing og brute force-angreb.

Iran står sandsynligvis bag cyberangreb mod universiteter
Hackergruppen Silent Librarian (også kendt under andre navne, bl.a. Cobalt Dickens og TA407) har løbende siden 2013 udført cyberangreb mod universiteter verden over, bl.a. i Danmark. Hackergruppen benytter flere angrebsmetoder, primært omfattende spearphishing-kampagner og angreb, hvor hackerne opretter meget vellignende kopier af login-sider til forskellige it-systemer tilknyttet universiteter, der bruges til at høste brugeres login-oplysninger.

Det amerikanske justitsministerium anklagede i 2018 formodede medlemmer af Silent Librarian for at stå bag cyberangreb mod 144 amerikanske universiteter og for at have stjålet op mod 31.5 terabytes fra omtrent 340 universiteter verden over, inklusiv de amerikanske. Ifølge det amerikanske anklageskrift er hackerangrebene udført af iranske hackere på vegne af den iranske Revolutionsgarde (IRGC).

Hackere angriber ofte tværgående it-netværk og systemer

Hackere forsøger ofte at få adgang til tværgående it-netværk, såsom mailsystemer. Det giver dem mulighed for at spionere mod flere fagområder inden for de enkelte universiteter på samme tid.

I andre tilfælde har hackerne dog udført mere målrettede angreb, bl.a. i form af spearphishing-angreb rettet mod specifikke professorer.

GRU anklages for brute-force angreb mod universiteter
Amerikanske og britiske myndigheder udgav i juli 2021 en såkaldt Cybersecurity Advisory, hvor de hævdede, at den russiske militære efterretningstjeneste GRU står bag en omfattende kampagne af brute-force angreb mod bl.a. universiteter.

Ifølge rapporten har angrebene stået på siden midten af 2019 og foregår efter al sandsynlighed stadig. Angrebene har især været rettet mod Microsoft 365 cloud services, men har også ramt mailservere.

Nogle fagområder er udsat for særlig interesse fra fremmede stater

Der er ikke et entydigt billede af, hvad fremmede stater går efter, når de udfører cyberspionage mod forskning, idet hackerne ofte angriber tværgående mål, som f.eks. mailsystemer. Konkrete sager i og uden for Danmark, viser dog at nogle fagområder sandsynligvis er udsat for en særlig interesse fra fremmede stater.

Det gælder f.eks. forskningsinstitutioner, der beskæftiger sig med sikkerheds- og udenrigspolitiske forhold, og som har indflydelse på nationale beslutningstagere.

Det gælder også militære forsknings- og uddannelsesinstitutioner og universiteter samt forskningsinstitutioner, der beskæftiger sig med Arktis.

Der er således et sammenfald mellem de emner, som har fremmede staters strategiske opmærksomhed, og deres mål for cyberspionage inden for universiteter og forskningsinstitutioner.

Vigtige begivenheder påvirker også truslen fra cyberspionage
Under COVID-19-pandemien har der i udlandet også været interesse i forskning relateret til COVID-19. Det illustrerer, hvordan vigtige begivenheder påvirker, hvilken type forskning fremmede stater spionerer imod.

Fremmede stater har fokus på dual-use teknologi

Fremmede stater har et særligt fokus på såkaldt dual-use teknologi og forskning i dual-use teknologi. Det betyder, at forskning inden for teknologier og anvendelse af teknologier, der kan bruges til både civile og militære formål, er et særligt mål for cyberspionage.

Teknologiers mulige anvendelse til både civile og militære formål kan betyde, at fremmede stater potentielt opfylder både kommercielle og sikkerhedspolitiske behov på samme tid, hvis de kompromitterer dual-use mål.

Nogle lande med væsentlige cyberkapaciteter har et erklæret politisk mål om at have fokus på dual-use teknologi. Som et led i moderniseringen af Kinas forsvar er der eksempelvis et erklæret mål om "civil og militær fusion" ("junmin ronghe") med fokus på bl.a. dual-use teknologier. I Rusland er udviklingen af dual-use teknologier også et erklæret mål for landets militære udviklingsorganisation Fonden for Avanceret Forskning (FPI).

Cyberkriminalitet udgør en meget høj trussel mod danske universiteter

Danske universiteter er også udsat for en **MEGET HØJ** trussel fra cyberkriminalitet. Universiteter kan f.eks., ligesom mål i mange andre sektorer, blive ramt af målrettede ransomware-angreb.

Siden 2019 har flere cyberkriminelle grupper fokuseret på at udføre eller understøtte målrettede ransomware-angreb. Disse hackergrupper har i 2020 udvidet deres afpresning ved også at true med at lække følsomme oplysninger, stjålet i forbindelse med ransomware-angrebene.

Universiteter i udlandet er flere tilfælde blevet ramt af denne type målrettede ransomware-angreb. CFCS vurderer, at danske universiteter og forskningsinstitutioner også er udsat for truslen fra målrettede ransomware-angreb.

Universitetshospital i Tyskland blev ramt af målrettet ransomware

I september 2019 blev et universitetshospital i Düsseldorf angrebet med ransomwaren Doppelpaymer. Angrebet betød bl.a. at hospitalet kun kunne gennemføre ca. halvdelen af de behandlinger, det normalt gennemfører.

En kvinde, på vej til universitetshospitalet i en ambulance, blev omdirigeret til et andet hospital på grund af nedsat kapacitet, som følge af angrebet. Kvinden afgik efterfølgende ved døden. Tyske myndigheder undersøgte, hvorvidt dødsfaldet kunne kædes sammen med ransomware-angrebet. Konklusionen på undersøgelsen blev dog, at der ikke var tilstrækkeligt grundlag til at anklage de kriminelle hackere for at have ansvaret for kvindens død.

Den mest almindelige type cyberkriminalitet er fortsat baseret på brede cyberangreb rettet mod et stort antal potentielle ofre på tværs af samfundet. Det gælder bl.a. angreb gennem phishing, udnyttelse af kendte sårbarheder i udbredte it-systemer samt misbrug af usikre fjernadgange. Derfor kan danske universiteter og forskningsinstitutioner forvente at blive udsat for forsøg på cyberkriminalitet.

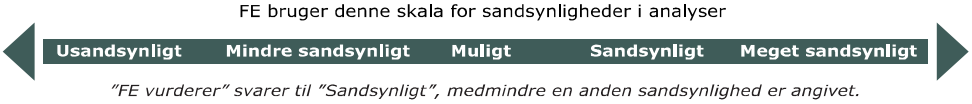
De kriminelle bruger værktøjer og angrebsteknikker, der typisk er udviklet til specifikke kriminelle formål, eksempelvis til tyveri af personlige oplysninger, afpresning gennem ransomware eller misbrug af it-systemer til kryptomining. Variationen i angrebene betyder, at cyberkriminalitet dækker over flere typer berigelseskriminalitet, herunder både tyveri, afpresning og bedrageri.

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



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

Andre relevante publikationer

Center for Cybersikkerhed (CFCS) udgiver løbende vejledninger og trusselsvurderinger. Nedenfor er fremhævet en række produkter af særlig relevans for denne trusselsvurdering. Alle produkterne er tilgængelige på CFCS' hjemmeside.

Truslen fra phishing-mails
Trusselsvurderingen "Cybertruslen fra phishing-mails" går i dybden med, hvordan hackere benytter phishing- og spear phishing-mails i deres forsøg på at kompromittere virksomheder eller franarre dem følsomme oplysninger. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/phishing/

Vejledning til at imødegå phishing
Vejledningen "Phishing: Beskyt organisationen mod phishingangreb" henvender sig til ledelsen og kommer med en række konkrete anbefalinger, der kan bidrage til organisationernes arbejde med at beskytte sig mod phishing-angreb. Læs vejledningen her: https://cfcs.dk/da/forebyggelse/vejledninger/phishing

Cybertruslen mod Danmark
Den årlige trusselsvurdering "Cybertruslen mod Danmark 2021" beskriver det samlede trusselsbillede for cybertrusler mod Danmark og indeholder kapitler om truslen fra cyberkriminalitet, cyberspionage, destruktive cyberangreb, cyberaktivisme og cyberterror. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

Samarbejde mellem cyberkriminelle
Trusselsvurderingen "Drømmer cyberkriminelle om tillidsfulde relationer?" beskriver, hvordan veletablerede samarbejdsrelationer, arbejdsdeling og udveksling af tjenester i det kriminelle miljø bidrager til den meget høje trussel fra cyberkriminalitet i almindelighed og målrettede ransomware-angreb i særdeleshed. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/organiseret-cyberkriminalitet/

Truslen fra målrettede ransomware-angreb
Trusselsvurderingen "Digitale gidseltagere på storvildtjagt" beskriver truslen fra såkaldte målrettede ransomware-angreb, der kan have alvorlige konsekvenser for en organisation. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

Hvordan målrettede ransomware-angreb foregår skridt for skridt
Undersøgelsesrapporten "Anatomien af målrettede ransomware-angreb" går i dybden med, hvordan sådanne angreb foregår. Rapporten indeholder konkrete råd til, hvordan angrebene kan imødegås. Læs rapporten her: https://cfcs.dk/da/cybertruslen/rapporter/anatomien-i-ransomware-angreb/

Vejledning til at imødegå ransomware-angreb
Vejledningen "Reducer risikoen for ransomware" giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-

angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket. Læs vejledningen her: https://cfcs.dk/da/forebyg-gelse/vejledninger/ransomware/

Trusselsvurdering om truslen mod leverandører
Trusselsvurderingen "Cyberangreb mod leverandører" beskriver cybertruslen mod leverandører. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/leverandorer/

Vejledning om leverandørstyring
Vejledningen "Informationssikkerhed i leverandørforhold" indeholder en række forslag til, hvordan styringen af forholdet mellem organisationer og leverandører kan varetages. Læs vejledningen her: https://cfcs.dk/da/forebyggelse/vejledninger/informations-sikkerhed-i-leverandorforhold/

Truslen fra bevidste og ubevidste insidere
CFCS og PET har udarbejdet trusselsvurderingen "Cybertruslen fra bevidste og ubevidste insidere". I trusselsvurderingen kan du læse mere om truslen og anbefalinger til mitigerende tiltag. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/insidertruslen/

Truslen mod Forsvarsindustrien
Trusselsvurderingen "Cybertruslen mod forsvarsindustrien" beskriver truslen fra forskellige typer cybertrusler mod forsvarsindustrien. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/forsvarsindustrien/

Cyberangreb mod HR-afdelinger
Trusselsvurderingen "HR-afdelinger rammes også af målrettede cyberangreb" belyser, hvordan hackere forsøger at bruge HR-afdelinger som en nem vej ind i organisationer. Vurderingen indeholder også anbefalinger til, hvordan organisationer kan understøtte deres HR-afdelinger med både tekniske tiltag og awareness. Læs vurderingen her: https://cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-hr-afdelinger/