CENTER FOR CYBERSIKKERHED

23. marts 2018

Trusselsvurdering: Danske universiteter er mål for cyberangreb

Et cyberangreb mod bl.a. danske universiteter understreger cybertruslen mod universiteter og forskningsinstitutioner i Danmark.

Hovedvurdering

- En statslig aktør har stået bag kompromitteringer af e-mailkonti tilhørende medarbejdere ved specifikke danske universiteter. Lignende cyberangreb fandt sted i udlandet.
- Angriberne har sandsynligvis været interesseret i en række bestemte fagområder.
- Angrebet afspejler cybertruslen mod danske offentlige forskningsinstitutioner. CFCS vurderer, at truslen fra cyberspionage mod forskningsinstitutionerne er **HØJ.**
- Tradition for stor åbenhed gør forskningsmiljøerne meget sårbare for cyberangreb.

Analyse

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) vurderer det meget sandsynligt, at flere e-mailkonti tilhørende nuværende eller tidligere ansatte ved universiteter i Danmark har været kompromitteret af en statslig aktør. CFCS har taget kontakt til relevante parter, som vi vurderer har været berørt i sagen.

Kompromitteringen var resultat af et stort antal fremsendte spearphishingmails målrettet ansatte på universiteter og andre organisationer verden over i perioden 2014-2016. Ifølge officielle udtalelser fra amerikanske myndigheder har angrebene tilknytning til Iran.

Cyberangrebet har i Danmark været målrettet medarbejdere ved specifikke danske universiteter med specialer inden for bl.a. økonomi, sundhed, kemi, fysik, geologi, miljø og transport. CFCS vurderer, at det er sandsynligt, at aktøren bag angrebene har været særligt interesseret i disse fagområder, men det er også muligt, at angriberne har forsøgt at misbruge adgange til medarbejdere på disse områder til at indsamle informationer på andre områder end de nævnte.

Cyberangrebene understreger den generelle cybertrussel mod danske universiteter og forskningsinstitutioner, som CFCS tidligere har beskrevet i trusselsvurderingen ”Hackere fra udlandet truer danske offentlige forskningsinstitutioner” fra 2016.

CFCS vurderer derfor fortsat, at truslen fra cyberspionage mod danske offentlige forskningsinstitutioner er HØJ, og at fremmede stater udfører cyberspionage mod danske offentlige forskningsinstitutioner. Universiteter og offentlige forskningsmiljøer har tradition for stor åbenhed. Det gør miljøerne meget sårbare for cyberangreb.

Mens det omtalte cyberangreb har været rettet mod forskningsinstitutioner i flere lande, kan det danske forskningsmiljø i sig selv være interessant for fremmede stater. Dansk forskning er i skarp international konkurrence om at komme først med forskningsresultater, sikre finansiering og rekruttere de bedste forskere og studerende. Danske forskere leverer også viden, som udgør en del af grundlaget for de politiske valg, regering og Folketing træffer. Fremmede stater kan også have interesse i at få adgang til eksempelvis it-infrastrukturer eller personfølsomme data, som forskningsinstitutionerne administrerer.

Anbefalinger

CFCS anbefaler, at ledelser på alle niveauer af danske universiteter og forskningscentre gør sig bevidst om cybertruslen og handler på baggrund heraf. Cybertruslen er ikke blot en it-teknisk udfordring, men også et spørgsmål om medarbejderes adfærd og viden om egne sårbarheder. Derfor er det vigtigt at involvere det strategiske niveau og forankre beslutninger hos ledelsen. Det kan f.eks. være en passwordpolitik, som, jf. CFCS' Passwordvejledning, anbefaler unikke passwords, som ikke genbruges.

CFCS anbefaler, at universiteternes ledelser vurderer risici og beslutter tiltag. Universiteterne bør arbejde målrettet med både processer, teknik og adfærd. Processer er bl.a. regelmæssigt at lave risikoanalyser og finde ud af, hvilken viden universiteterne vurderer vigtig at beskytte, og hvilke konsekvenser det har, hvis beskyttelsen fejler. Teknik kan f.eks. være at finde sårbarheder eller at afdække og beskytte it-infrastruktur og it-processer. Adfærd involverer tiltag, der skal øge bevidstheden om cybertruslen hos medarbejdere og uddanne dem til at begå sig hensigtsmæssigt og
sikkert.

CFCS anbefaler universiteter og andre forskningsinstitutioner at beskytte sig mod cybertruslen ved bl.a. at søge oplysninger og råd, f.eks. i disse publikationer:

- Cyberforsvar der virker
- Spear-phishing – et voksende problem
- Passwordvejledning
- Trusselsvurdering: Cybertruslen mod Danmark

FE bruger denne skala for sandsynlighed i analyser: