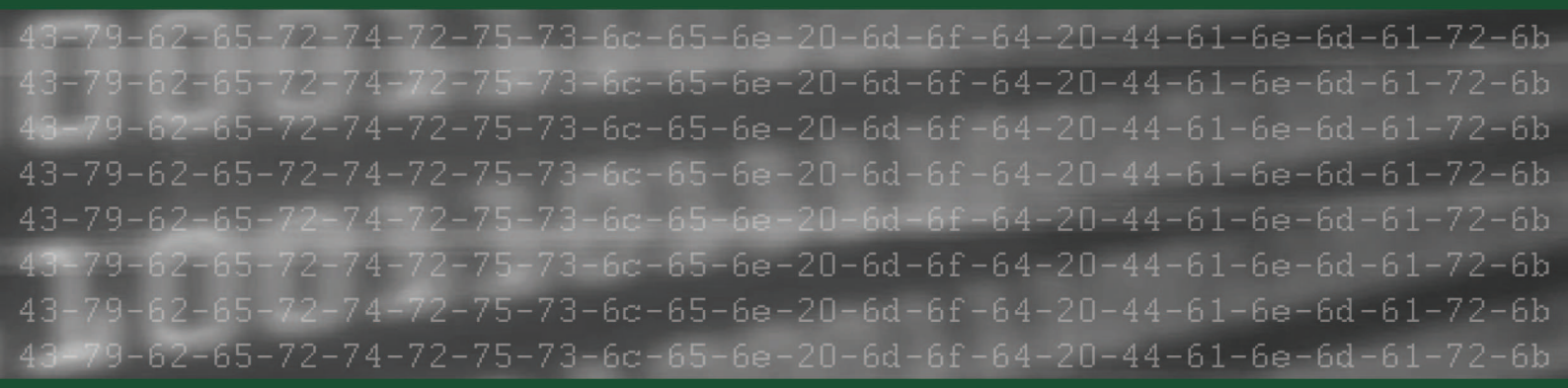
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod forsvars- og aerospaceindustrien i Danmark



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Maj 2016

CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cybertruslen mod forsvars- og aerospaceindustrien i Danmark

Formålet med denne vurdering er at informere om cybertruslen mod forsvars- og aerospaceindustrien i Danmark, hvor der er en vedholdende cyberspionagetrussel.

Hovedvurdering

- Der er en vedholdende trussel fra cyberspionage mod forsvars- og aerospaceindustrien i Danmark.
- Center for Cybersikkerhed vurderer, at trusselsaktørerne har tilknytning til fremmede stater, sandsynligvis fremmede sikkerheds- og efterretningstjenester.
- Truslen fra cyberkriminalitet, cyberaktivisme og cyberterror mod forsvars- og aerospaceindustrien svarer til den generelle trussel mod samfundet i Danmark.

Analyse

Trusselsvurderingsenheden ved Center for Cybersikkerhed (CFCS) vurderer, at der er en vedholdende cyberspionagetrussel mod forsvars- og aerospaceindustrien i Danmark. Truslen fra cyberspionage mod forsvars- og aerospaceindustrien i Danmark er **MEGET HØJ**, og CFCS vurderer, at der fra visse trusselsaktører aktuelt er særligt fokus på virksomheder, der beskæftiger sig med teknologier og tjenester med relevans for aerospace.

Truslen bliver understreget af viden om konkrete kompromitteringer og forsøg på kompromitteringer af virksomheder i industrien i både Danmark og udlandet. CFCS har inden for de sidste år undersøgt to større kompromitteringer af virksomheder i Danmark, hvor begge kompromitteringer blev opdaget og standset. CFCS vurderer, at begge kompromitteringer blev udført af trusselsaktører med tilknytning til samme fremmede stat.

Flere lande benytter systematisk cyberspionage som et middel til at opnå industrielle og forretningsmæssige fordele samt styrke deres egen politiske og økonomiske position. Spionagen mod forsvars- og aerospaceindustrien er sandsynligvis både økonomisk og sikkerhedspolitisk motiveret. Konsekvenserne for virksomheder, der er mål for cyberspionagen, kan både være tab af intellektuel ejendom og forringede vilkår i udbudsrunder og forhandlinger.

Trusselsaktørerne, der udgør en trussel mod forsvars- og aerospaceindustrien i Danmark, har meget væsentlige ressourcer og er bl.a. i stand til at iværksætte og udføre cyberspionage mod en lang række mål i flere lande på samme tid.

De enkelte forsøg på cyberspionage bliver gennemført meget målrettet med specifikke formål, men er samtidig ofte del af større kampagner udført af trusselsaktørerne, hvor angrebsmetoder og kapaciteter så som malware og infrastruktur ofte genanvendes på tværs af sektorer og industrier.

CFCS vurderer, at aktørerne er tilknyttet fremmede stater, i form af fremmede sikkerheds- og efterretningstjenester, som også har kapacitet til indhentning af oplysninger med andre efterretningsmidler end de digitale. Trusselaktørerne anser forsvars- og aerospaceindustrien for at være af strategisk betydning. De er derfor parate til at anvende meget væsentlige kapaciteter og vedholdenhed i cyberspionagen mod industrien.

For de enkelte virksomheder, hvor der er et fokus fra trusselsaktørerne, vil der typisk være tale om en vedholdende trussel, hvor aktøren gentagne gange forsøger at kompromittere virksomheden eller vedligeholder en gennemført kompromittering.

Virksomheder og organisationer i forsvars- og aerospaceindustrien anvendes også som platform for angreb mod andre. Trusselsaktører har i udlandet eksempelvis oprettet falske hjemmesider tilhørende flåde- og flyudstillinger og brancheorganisationer med henblik på at kompromittere andre. Der er også eksempler på kompromittering af virksomheder i industrien gennem underleverandører og servicevirksomheder.

Aktørerne benytter sig af forskellige angrebsteknikker mod forsvars- og aerospaceindustrien, blandt andet såkaldte spear-phishing mails, angreb via kompromittering af andre virksomheder og organisationers hjemmesider, såkaldt waterhole-angreb, og ved især at udnytte kendte sårbarheder i ikke-sikkerhedsopdaterede soft- og hardware benyttet af virksomheder i industrien. Aktørerne er også parate til at udnytte hidtil ukendte sårbarheder i soft- og hardware, såkaldte zero-day-sårbarheder.

Med spear-phishing mails forsøger trusselsaktørerne målrettet at angribe virksomhederne via deres medarbejdere. For at øge chancen for succes benyttes der såkaldt social engineering, hvor indsamlet viden om virksomheden og udvalgte medarbejdere bruges til at øge chancen for, at medarbejdere i god tro åbner mails og klikker på links til ondsindede sider, åbner vedhæftede inficerede filer eller afgiver brugernavne og passwords på eksempelvis falske hjemmesider.

Aktørerne forsøger at skjule deres aktiviteter og geografiske placering bl.a. ved hjælp af mellemled på internettet og navngivning af falske domæner og hjemmesider, der ved første øjekast virker legitime.

CFCS vurderer, at cybertruslen mod forsvars- og aerospaceindustrien i Danmark fra cyberkriminalitet, cyberaktivisme og cyberterror svarer til den generelle trussel mod Danmark. For yderligere oplysninger om den generelle trussel se trusselsvurdering "Cybertruslen mod Danmark" fra januar 2016, der er tilgængelig på CFCS' hjemmeside, der også forklarer anvendelsen af trusselsniveauer.

Anbefalinger

CFCS anbefaler, at topledelsen i virksomheder og organisationer i forsvars- og aerospaceindustrien med udgangspunkt i denne trusselvurdering erkender og handler på baggrund af det beskrevne trusselsbillede. Forankringen i topledelsen skal sikre, at der til det videre arbejde er de rette tekniske kompetencer i et nødvendigt omfang.

CFCS anbefaler endvidere, at der anvendes en risikobaseret tilgang i organisationens arbejde med cyberforsvar. Der bør foretages en risikovurdering med udgangspunkt i det aktuelle trusselbillede og de relevante angrebsvektorer (fx spear-phishing, waterhole-angreb og zero-day-sårbarheder). Risikovurderingen bør inddrage forhold omkring organisationens erkendte sårbarheder. Forudsætningen for i tilstrækkelig omfang at kunne erkende disse sårbarheder er, at organisationen har et godt overblik over egen it-infrastruktur, it-processer mv.

Baseret på erfaring er det gennemførelsen af de såkaldte top fire sikkerhedstiltag nævnt i vejledningen "Cyberforsvar der virker", og heriblandt især softwareopdateringerne, der er centrale for øget cybersikkerhed.

Endelig bør topledelsen sikre, at der gennemføres awarenes kampagner i organisationen på baggrund af det beskrevne trusselbillede og den udarbejdede risikovurdering.

CFCS har udarbejdet et antal vejledninger, der med fordel kan bidrage til organisationens generelle viden indsamling på området:

- Cyberforsvar der virker
- Spear-phishing – et voksende problem
- Logning – en del af et godt cyberforsvar

FE bruger denne skala for sandsynlighed i analyser: