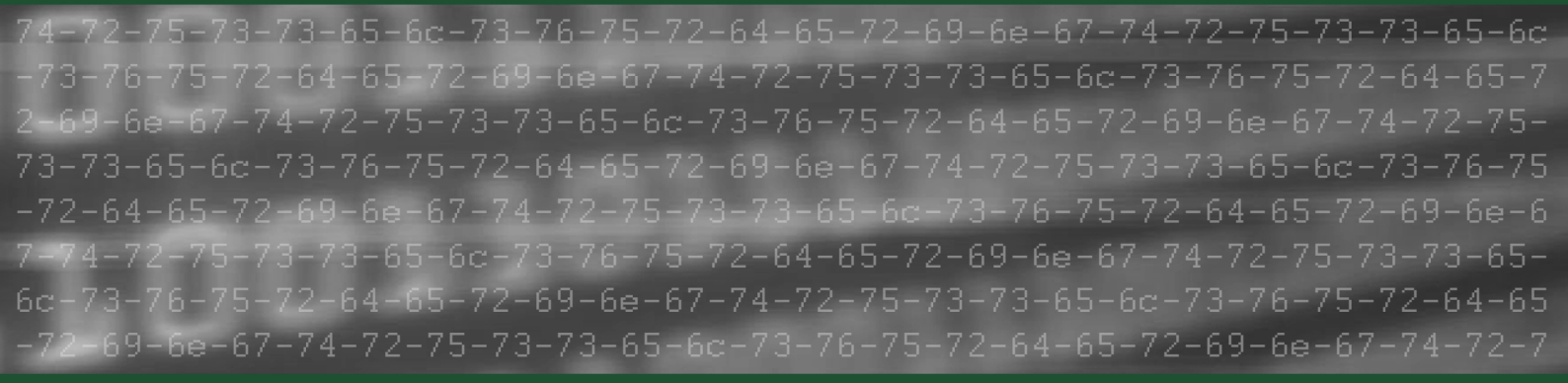
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Fremmede stater scanner danske virksomheder og myndigheder for sårbarheder i it-systemer



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Juni 2016

CENTER FOR CYBERSIKKERHED

29. juni 2016
Trusselsvurderingsenheden

Trusselsvurdering: Fremmede stater scanner danske virksomheder og myndigheder for sårbarheder i it-systemer.

Vurderingen gør rede for cybertruslen fra fremmede stater mod danske myndigheder og virksomheders it-systemer.

Hovedvurdering

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) vurderer, at fremmede stater scanner it-systemer i Danmark for at søge efter sårbarheder og installere bagdøre i systemerne. Ved at installere bagdøre i systemerne opbygger staterne et netværk af maskiner, som de senere kan angribe eller bruge til at angribe andre prioriterede mål.

CFCS har kendskab til angreb i Danmark og lignende aktiviteter i andre lande, hvor sårbarheder i it-systemer blev udnyttet.

Det er meget sandsynligt, at stater eller statsstøttede grupper fortsat vil scanne danske mål for at finde og udnytte kendte sårbarheder i it-systemer.

CFCS vurderer, at truslen fra cyberspionage mod danske myndigheder og private virksomheder fortsat er **MEGET HØJ**.

En uddybning af FE's brug af trusselsniveauer findes her

Analyse

Fremmede stater har både evner til og vedholdende intention om at angribe danske mål via internettet. Staterne er i stand til at gennemføre målrettede kampagner, hvor de scanner it-netværk bredt og systematisk for at finde sårbarheder i it-systemer. Angrebene bliver fortsat mere og mere avancerede.

Hackere udnytter virksomheder og myndigheder til at ramme andre mål
En virksomhed eller myndighed, der besidder viden andre stater har interesse i, kan udgøre et mål i sig selv, men kan også blive brugt som indgang til angreb på andre dele af samfundet, fx centraladministrationen eller andre virksomheder, den er leverandør til. Dens servere og pc'er kan også blive brugt som en del af et større netværk med det formål at opbygge stor maskinkraft og bevare anonymitet, når stater angriber andre mål end den enkelte virksomhed eller myndighed.

Fremmede stater gennemfører løbende disse kampagner, hvor de forsøger at udnytte kendte sårbarheder i virksomheders og myndigheders it-systemer.

Angreb mod sårbarheder i JBoss
I 2015-2016 har CFCS fx set flere angreb mod sårbarheder i it-systemet JBoss, som benyttes af flere danske virksomheder og myndigheder. CFCS vurderer, at hackerne er tilknyttet fremmede stater. Hackerne scanner internettet bredt og søger efter kendte sårbarheder på mange maskiner ad gangen. De udnytter, at virksomheder og myndigheder ikke altid har konfigureret og sikkerhedsopdateret deres systemer tilstrækkeligt. De konkrete angreb har ramt et bredt udsnit af mål, der ikke synes at have andet til fælles end brugen af JBoss.

Hackere kan altså, når de kender til et systems sårbarheder, lede målrettet efter dem for at skabe bagdøre ind i systemet. Adgangen kan de siden fx bruge til at installere malware eller til at opbygge et større netværk.

Malware
Malware er en overordnet betegnelse for forskellige typer software, der gør skade på den computer, de kører på. Det er en sammentrækning af ordene malicious software, og der er altså tale om ondsindede programmer

CFCS har kendskab til lignende aktiviteter foretaget mod maskiner i andre lande og mod andre typer it-systemer end JBoss, fx CMS-systemer, samt andre typer servere.

Særligt avancerede angreb
Spionage mod offentlige myndigheder og private virksomheder udgør fortsat den alvorligste cybertrussel mod Danmark og danske interesser. Gennem de seneste år er omfanget af cyberspionage mod Danmark steget betydeligt, og gruppernes metoder og teknikker er blevet mere avancerede. CFCS vurderer, at det især er stater og statsstøttede grupper, der står bag spionagen og har ressourcer og evner til at gennemføre såkaldte APT-angreb.

CFCS vurderer, at truslen fra cyberspionage mod danske myndigheder og private virksomheder fortsat er **MEGET HØJ**.

APT

APT står for Advanced Persistent Threat. Det er et særligt avanceret, målrettet og vedholdende hacker-angreb. Angriberne får adgang til et netværk via sårbarheder i den software, som en organisation bruger. APT-angreb kræver store ressourcer, teknisk indsigt og konkret viden om målet. Hackerne bruger specielle værktøjer, der gør dem i stand til at skjule, at de er til stede i et netværk, og de angriber hyppigt over lang tid. APT sker oftest med det formål at spionere. Det er meget sandsynligt, at det er stater eller statsstøttede grupper, der står bag.

De grupper af hackere, som har evner og ressourcer til at udføre APT-angreb, er gode til at skjule sig, så virksomheder og myndigheder har vanskeligt ved at opdage, at de bliver angrebet. Det er meget sandsynligt, at fremmede stater fortsat vil scanne danske mål for at opdage og udnytte sårbarheder som i JBoss og andre it-systemer. Derfor kan virksomheder og myndigheder, som endnu ikke er blevet angrebet, udgøre fremtidige mål.

Anbefalinger

På CFCS's hjemmeside kan man holde sig løbende orienteret om nye trusler og finde gode råd til, hvordan man kan imødegå cybertrusler. CFCS anbefaler myndigheder og private virksomheder at holde internetvendte maskiner opdaterede og følge de råd, der er beskrevet i vejledninger som fx *Cyberforsvar der virker*.

FE bruger denne skala for sandsynlighed i analyser: