CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport:

Forsøg på kompromittering af netværks-udstyr

Statsstøttet hackergruppe forsøger at kompromittere net-værksudstyr i Danmark og resten af verden.

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave september 2019.

Formålet med denne undersøgelsesrapport er at beskrive forsøg på kompromittering af dansk internetvendt netværksudstyr. Rapporten gør opmærksom på en bestemt type af cyberangreb og indeholder forslag til tiltag, som kan hjælpe myndigheder og virksomheder til at beskytte sig mod lignende aktivitet. Målgruppen for denne rapport samt anbefalinger er it-ledelse og it-teknikere.

Hovedvurdering

- Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) har konstateret, at der har været rekognoscering mod og forsøg på kompromittering af danske myndigheders netværksudstyr.
- Det er sandsynligt, at hændelserne er udført af en statsstøttet hackergruppe, og at formålet har været cyberspionage.
- CFCS vurderer, at hændelserne er del af en global kampagne rettet mod netværksudstyr.
- CFCS har i 2019 fundet netværksenheder i Danmark, der er sårbare over for denne type angreb.

Indledning

CFCS har observeret aktivitet i Danmark fra det, der vurderes at være en statsstøttet hackergruppe, mod myndigheders internetvendte netværksudstyr. CFCS udsendte den 18. april 2018 et offentligt varsel i forbindelse med hændelserne. Varslet kan findes på CFCS' hjemmeside her: https://fe-ddis.dk/cfcs/nyheder/arkiv/2018/Pages/Varselangrebnetvaerksinfrastrukturer.aspx

CFCS har efterfølgende arbejdet videre og håndteret sagerne i samarbejde med relevante myndigheder.

CFCS undersøger og opsamler løbende viden omkring større cybersikkerhedshændelser. På baggrund af disse undersøgelser udgives offentlige undersøgelsesrapporter, så myndigheder og virksomheder kan drage nytte af erfaringerne og beskytte sig bedre.

CFCS har ved hjælp af open source-værktøjer i maj 2019 fundet knap 400 netværksenheder i Danmark med samme type sårbarhed, som er beskrevet i denne rapport. CFCS har i juni 2019 varslet de leverandører af internetforbindelser (ISP'er), som administrerer IP-adresser, hvor der er set sårbare netværksenheder.

Rekognoscering og indhentning mod Cisco-netværksudstyr

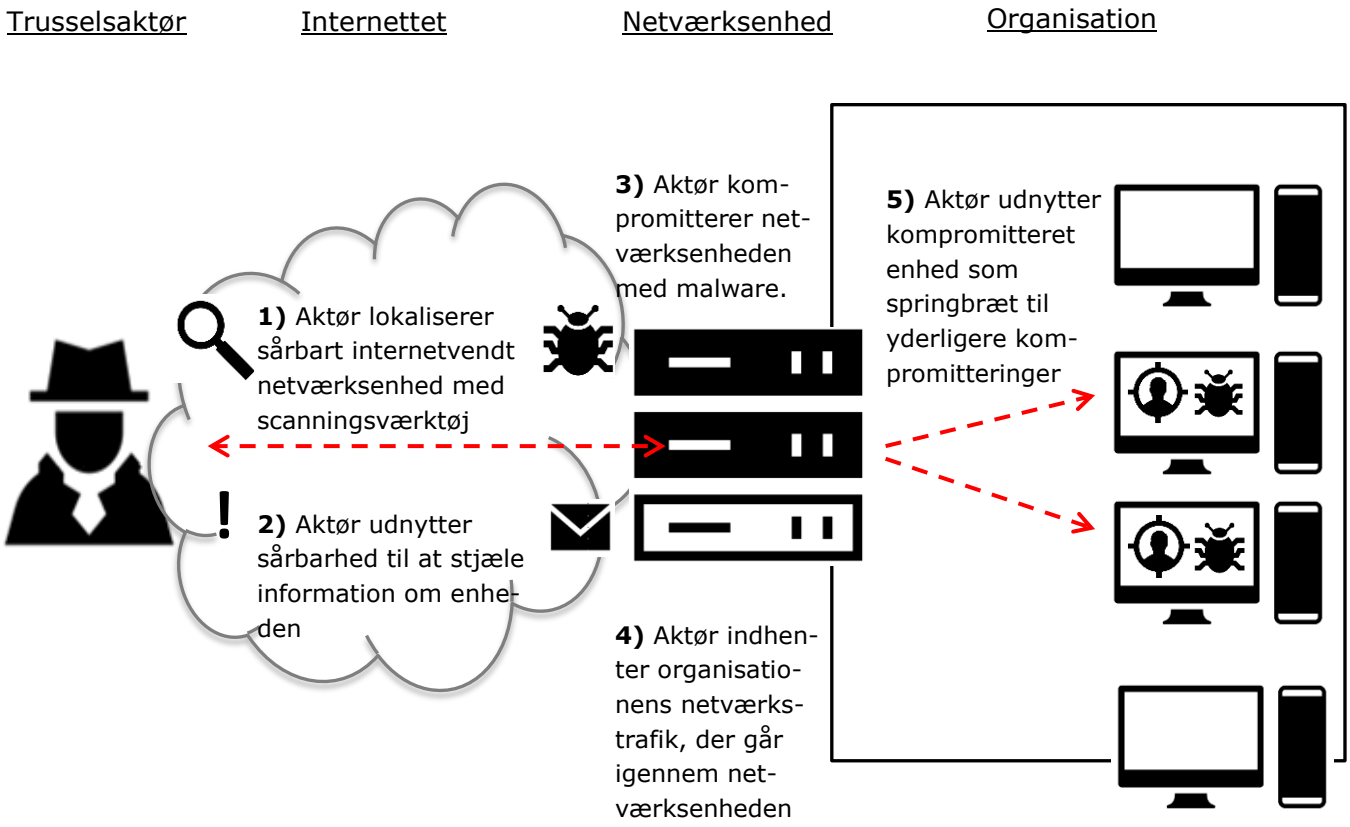
CFCS har konstateret, at en trusselsaktør i 2017 har forsøgt at indhente oplysninger fra internetvendt Cisco-netværksudstyr hos flere danske myndigheder. Flere af myndighederne har ansvarsområder, der kan have interesse for fremmede stater. Fælles for myndighedernes netværksudstyr er, at det har haft port 4786 eksponeret og åben imod internettet. Denne port håndterer en service kaldet Cisco Smart Install (SMI), som bruges til at opsætte og konfigurere netværksudstyr over internettet eller i et internt netværk. Det har gjort det muligt for aktøren at rekognoscere efter og dernæst lokalisere og kommunikere med udstyret.

Aktøren har udnyttet en kendt sårbarhed i myndighedernes Cisco-netværksudstyr til at indhente data fra enhederne. Dataene indeholder login-oplysninger til enheden i krypteret form - en såkaldt hash - samt information om enhederne og organisationernes netværksopsætning, som kan være relevant viden for fjendtlige aktører. Der er tegn på, at aktøren i enkelte tilfælde har kunnet udtrække hashes fra netværksenhederne. I de hændelser er der dog ikke tegn på, at aktøren efterfølgende har benyttet login-oplysningerne til at få adgang til netværkene. Kvaliteten af tilgængelige logs, der kan medvirke til at afdække hændelserne, er dog begrænset.

Redskaber til misbrug af sårbarheden er offentligt tilgængelige på internettet.

En stjålet hash kan udsættes for offline teknisk forcering. I et forceringsangreb forsøger aktøren på automatiseret vis at gætte kodeordet, der matcher den stjålne hash-værdi. Hvis forceringen lykkes, vil login-oplysningerne til netværksenheden fremgå i klar tekst. Med de stjålne login-oplysninger kan aktøren derefter logge ind på enheden over internettet og opnå kontrol med den.

Aktøren kan potentielt udnytte kompromitteret netværksudstyr til at overvåge, foretage cyberspionage eller ændre i trafik, der går ind og ud af en organisations netværk i et såkaldt man-in-the-middle-angreb. Dertil kan en kompromitteret netværksenhed potentielt fungere som trædesten til at trænge dybere ind i et netværk.



Figur 1: Illustration af hvordan sårbare internetvendte netværksenheder kan udnyttes til bl.a. at udføre spionage.

Kompromitteringen af netværksenheder kan potentielt misbruges til at lukke for adgangen til internettet, slette data og skabe driftsforstyrrelser for ramte organisationer, alt efter hvilke enheder aktøren har adgang til.

Der er sammenfald mellem den beskrevne aktivitet i Danmark og hændelser i udlandet. CFCS vurderer derfor, at der er tale om en global kampagne, der har ramt et stort antal netværksenheder globalt. Myndigheder i flere lande og sikkerhedsfirmaer har også beskrevet dette offentligt i rapporteringer. Se f.eks. US CERT's Alert (TA18-106A): https://www.us-cert.gov/ncas/alerts/TA18-106A

Attraktive mål

Netværksenheder, der forbinder et internt netværk i en organisation med internettet, er attraktive mål for hackere, herunder også statsstøttede hackergrupper.

Trusselsaktører kan ofte relativt nemt identificere internetvendt netværksudstyr bl.a. med offentligt tilgængelige værktøjer og online services. Med disse værktøjer, som også har legitime anvendelser, kan man finde frem til internetvendt hardware i hele verden, samt informa-

tion om den specifikke version af software, der er installeret på enhederne. Det betyder også, at man kan finde frem til netværksenheder, der har software med bestemte typer af sårbarheder. Når udstyret er lokaliseret, kan aktørerne interagere direkte med enhederne over internettet. CFCS vurderer, at statsstøttede hackergrupper generelt både scanner bredt og opportunistisk udnytter sårbare enheder, men også går målrettet efter netværksenheder hos specifikke organisationer.

Mange netværksenheder er desuden sårbare over for forsøg på kompromittering. Det kan bl.a. skyldes manglende installation af firmwareopdateringer, der lukker kendte sikkerhedshuller, fejl-konfiguration af udstyret ved opsætning, svage passwords eller brug og eksponering af sårbare protokoller og services på enheden. Dertil er netværksenheder sjældent beskyttet af antivirusprogrammer. Der offentliggøres jævnligt nye sårbarheder og metoder til at kompromittere internetvendte netværksenheder.

Sårbarhed: En (software) sårbarhed er en svaghed i et stykke software, der potentielt kan udnyttes til at få adgang til det it-system, hvor softwaren er installeret, eller påvirke systemets stabilitet eller integritet. Svagheden kan ligge i programkoden bag eller i konfigurationen af softwaren.

Exploit: Et exploit er selve udnyttelsen af den pågældende sårbarhed i et program eller konfigurationen af et system til at forårsage en hændelse, der bringer systemet i en usikker tilstand. Et exploit kan være et stykke programkode, som automatiserer udnyttelsen af en sårbarhed.

Endelig er det teknisk muligt at gennemføre kompromitteringer og spionage delvist automatiseret og i stor skala gennem sårbare netværksenheder. Trusselsaktører med den fornødne viden, infrastruktur og ressourcer kan ramme mange enheder på en gang.

Truslen

CFCS vurderer, at der i de omtalte hændelser rettet mod danske myndigheder er tale om forsøg på cyberspionage udført af en statsstøttet hackergruppe. Hackergruppen kan have forsøgt at kompromittere enhederne hos danske myndigheder for at understøtte deres cyberspionage på flere forskellige måder. Dels kan hackerne have haft til hensigt at kompromittere udstyret hos udvalgte myndigheder for at overvåge eller ændre i trafik, der går ind og ud af myndighedens netværk. Dels kan hackerne have haft en hensigt om at bruge det kompromitterede udstyr til at komme dybere ind i myndighedens netværk for at stjæle følsomme informationer.

Hændelserne i Danmark er som nævnt tidligere ikke isolerede, men sandsynligvis del af en kampagne, hvor hackerne har forsøgt at kompromittere netværksudstyr verden over. Flere lande har væsentlige

cyberkapaciteter, som benyttes til at spionere mod andre lande, herunder mod Danmark. Der er tale om en aktiv trussel fra stater, der vedholdende forsøger at stjæle informationer fra danske myndigheder og virksomheder. Truslen er især rettet mod de danske myndigheder, der ligger inde med oplysninger af strategisk, politisk og økonomisk betydning. Cyberspionage udgør en sikkerhedspolitisk og samfundsøkonomisk trussel mod Danmark og danske interesser.

Statsstøttede hackergrupper bruger ressourcer på at opbygge it-infrastruktur verden over. Fremmede stater har tidligere misbrugt dansk it-infrastruktur til at understøtte deres cyberoperationer mod danske og udenlandske mål. CFCS vurderer, at det er mindre sandsynligt, men teknisk muligt, at hackerne i denne sag har forsøgt at udnytte netværksenhederne til at rette cyberangreb mod andre mål i og udenfor Danmark.

Generelt kan cyberspionage mod myndigheder og virksomheder anvendes i forberedelsen af destruktive cyberangreb. CFCS vurderer dog, at det er usandsynligt, at formålet med kompromitteringen af netværksudstyret var at ødelægge data eller udstyr. CFCS vurderer samtidig også, at det er mindre sandsynligt, at fremmede stater på kort sigt vil rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark.

Anbefalinger

CFCS anbefaler i forhold til den beskrevne trussel at sikre, at Cisco Smart Install (SMI) er deaktiveret på internetvendt Cisco-udstyr, medmindre udstyret administreres af organisationens leverandør af internetforbindelser (ISP'en). For konkret vejledning hertil, se Ciscos egen vejledning her:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180409-smi

For de personer i organisationen, der skal begrænse adgangene til det internetvendte udstyr, er det nødvendigt at have et detaljeret kendskab til organisationens netværksinfrastruktur og de løsninger, der anvender udstyret. Det kan samtidig være nødvendigt at inddrage ISP'en, da netop gateway-udstyr ofte administreres af en ISP. I en dialog imellem organisationen og ISP'en kan følgende tiltag overvejes:

- Iværksæt en sårbarhedsskanning af perimeterudstyret. Eventuelt kan denne udføres af et eksternt (i forhold til ISP'en) firma. Husk at få alle relevante godkendelser og accepter, inden en sådan skanning påbegyndes, da skanninger kan påvirke udstyrets funktionalitet.
- Sørg for, at al internetvendt udstyr er opdateret med seneste firmware. Understøtter udstyret ikke en opdatering som følge af ældre teknologi, bør det udskiftes.

- Luk/bloker grænseflader, der ikke anvendes, samt forældede og usikre services/protokoller, herunder tftp (ofte port 69)og telnet (ofte port 23).
- Bloker for internetadgang til administrationsgrænsefladen og administrative protokoller (herunder SNMP) i videst muligt omfang.
- Adgangen til administrative funktioner på netværksenhederne skal beskyttes med nye og stærke passwords, og hver enhed bør have sit eget unikke password - alternativt bør der anvendes multifaktorautentifikation.
- Er der behov for, at flere brugerprofiler har adgang til menuerne i enhederne, bør der implementeres least-privileged-adgangsstyring i flere niveauer.
- Anvend i videst mulig omfang autentifikation og kryptering ved direkte kommunikation med udstyret.
- Fjern eller begræns "banner"-informationer, der potentielt afslører informationer om udstyrets type og version.
- Aktiver logning på alle internetvendte systemer, og sørg for, at disse logs overvåges for unormal aktivitet.

På længere sigt er der yderligere tiltag, som organisationen bør overveje, eventuelt i samråd med sin ISP. Ofte vil disse tiltag kræve flere ressourcer at implementere og måske betyde omstrukturering af det interne netværk (segmentering) samt opstilling af nye løsninger:

- Etabler en lagdelt sikkerheds-infrastruktur (løgstruktur). Dette kan reducere risikoen for, at en potentiel kompromittering af de yderste lag (perimetersikringen mv.) vil påvirke sikkerheden i de indre lag.
- Gennemgå og opdater om nødvendigt aftaler med ISP'en med henblik på at sikre, at netværksudstyret holdes opdateret og udskiftes, når dette ikke længere supporteres af producenten.

FE bruger denne skala for sandsynligheder i analyser