CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod IoT-enheder

1. udgave oktober 2023

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk
1. udgave, oktober 2023

Formål

Formålet med trusselsvurderingen er at informere om cybertruslen mod IoT-enheder, der ligesom almindelige it-systemer rammes af cyberangreb. Vurderingen supplerer Center for Cybersikkerheds (CFCS) generelle vurdering af cybertruslen mod Danmark og kan f.eks. fungere som input til virksomheders og organisationers risikovurderinger.

Hovedvurdering

- Truslen fra cyberangreb mod IoT-enheder er **MEGET HØJ**.
- Både statslige og ikke-statslige hackere udfører løbende forsøg på cyberangreb mod IoT-enheder i Danmark og i udlandet. Det er meget sandsynligt, at det vil fortsætte på lang sigt.
- Det er meget sandsynligt, at hackere generelt anser IoT-enheder for at være attraktive mål, fordi de generelt er dårligere beskyttede end almindelige computere og dermed nemmere at kompromittere.
- CFCS vurderer, at hackere typisk kompromitterer IoT-enheder gennem udnyttelsen af sårbarheder eller bruteforce-angreb.
- CFCS vurderer, at hackere oftest kompromitterer IoT-enheder for at bruge dem i botnet. Botnet kan bl.a. anvendes til overbelastningsangreb (DDoS-angreb).
- Hackere kompromitterer dog også IoT-enheder for at bruge dem som en indledende angrebsvinkel i cyberangreb, eller fordi de udgør et selvstændigt mål for bl.a. cyberspionage.
- Brugen af IoT-enheder udviklet i lande uden for Danmarks normale sikkerhedspolitiske kreds kan øge risikoen for cyberspionage. Særligt hvis dem, de anvendes af, udgør et spionagemål for fremmede stater.

Brug af IoT-enheder medfører en sikkerhedsrisiko

Enheder kobles til internettet som aldrig før. Mange biler, elpærer, fjernsyn og lignende er i dag "smarte", idet de indeholder og styres af indbyggede computere. Når disse smarte enheder kobles til internettet, f.eks. for at give brugeren adgang til nye funktioner, betegnes de som Internet of Things-enheder (IoT-enheder).

IoT-enheder er blandt andet populære på arbejdspladsen. Det skyldes, at de gør hverdagen lettere. Ved at koble enhederne til internettet kan man eksempelvis tjekke videoovervågningen hjemmefra, og gennem mødelokalets konferenceudstyr kan kollegaer holde møder sammen, selvom de opholder sig vidt forskellige steder. Desuden kan printeren hurtigt fikses af virksomhedens it-leverandør gennem fjernadgang. Fordelene ved IoT-enheder er mange.

Men brugen af IoT-enheder medfører også en betydelig sikkerhedsrisiko. IoT-enheder er nemlig ofte dårligere beskyttede end almindelige computere. Og ligesom almindelige computere kan IoT-enheder også blive ramt af cyberangreb fra ondsindede hackere. Hackerne kan for eksempel kigge med på dit overvågningskamera eller udnytte en sårbar brandalarm til at stjæle sensitive data fra dit netværk. Med IoT-enhederne følger således en cybertrussel, som brugeren må forholde sig til.

Denne trusselsvurdering beskriver cybertruslen mod IoT-enheder. Det gør den dels ved at vurdere sandsynligheden for cyberangreb mod IoT-enheder i Danmark. Og dels ved at beskrive truslens karakter, såsom hvordan hackere typisk angriber IoT-enheder og med hvilke formål. Trusselsbilledet viser overordnet set, at truslen mod IoT-enheder er **MEGET HØJ**, samt at det er meget sandsynligt, at IoT-enheder i Danmark vil blive ramt af forsøg på cyberangreb.

Trusselsvurderingen er en af tre CFCS-udgivelser, som sætter fokus på sikkerheden i IoT-enheder. Ud over trusselsvurderingen udgives også en vejledning og en kort guide med anbefalinger om sikker brug af IoT-enheder.

Udgivelserne er udarbejdet efter dialog med Dansk Erhverv og Rådet for Digital Sikkerhed i rammen af "Aftale om et styrket cyberforsvar", og indholdet har bl.a. været drøftet med medlemmer af Dansk Erhvervs it-sikkerhedsnetværk. CFCS takker Dansk Erhverv, Rådet for Digital sikkerhed samt medlemmer af Dansk Erhvervs it-sikkerhedsnetværk for samarbejdet omkring udgivelserne.

Hvad er en IoT-enhed i denne trusselsvurdering?
IoT er en samlebetegnelse for alle enheder, der forbindes til internettet. IoT-enheder kan f.eks. være overvågningskameraer, køleskabe, smart-TV eller ladestandere, som kobles til internettet med henblik på bl.a. fjernstyring. Derudover betragtes netværksudstyr i denne trusselsvurdering også som IoT-enheder, da de i høj grad angribes og udnyttes på samme måde. Begrebet dækker i trusselsvurderingen ikke over almindelige computere, servere eller telefoner samt operationelle teknologier som f.eks. industrielle kontrolsystemer.

Foto: Shutterstock

IoT-enheder er attraktive mål for hackere og angribes løbende

CFCS vurderer, at den samlede trussel fra cyberangreb mod IoT-enheder er **MEGET HØJ**.

Truslen kommer både fra statslige og ikke-statslige aktører, der løbende forsøger at kompromittere IoT-enheder i Danmark og i udlandet. Det er meget sandsynligt, at det vil fortsætte på lang sigt.

Det er meget sandsynligt, at hackere generelt anser IoT-enheder for at være attraktive mål. Dels fordi de kan anvende dem til flere forskellige formål, som beskrives på de følgende sider. Men også fordi IoT-enheder typisk er mere eksponerede og dårligere beskyttede end f.eks. almindelige computere og dermed nemmere at kompromittere.

Særligt udsatte er IoT-enheder med kendte sårbarheder, der ikke beskyttes i relevant omfang. Det kan for eksempel være IoT-enheder hos privatpersoner samt små og mellemstore virksomheder, hvor ressourcerne til eller opmærksomheden på cybersikkerhed ofte er begrænsede. Det kan dog også være ved større organisationer med store netværk, hvor det kan være svært at holde et overblik over IoT-enheder og beskytte dem.

Derudover har de seneste års teknologiske udvikling medført en markant stigning i brugen af IoT-enheder, som i dag anvendes i alle dele af samfundet. Udviklingen har mange fordele, men betyder også, at antallet af potentielle mål bliver markant større.

Det er meget sandsynligt, at hackere udnytter denne udvikling til at kompromittere IoT-enheder i meget stor skala, eksempelvis med henblik på udviklingen af botnet. I nogle tilfælde er malwaren, som hackerne anvender til at kontrollere en kompromitteret IoT-enhed, f.eks. designet som en såkaldt orm, der efter at have inficeret en kompromitteret IoT-enhed automatisk vil forsøge at kompromittere andre enheder på samme netværk.

IoT-enheder kompromitteres oftest gennem sårbarheder og bruteforce-angreb
CFCS vurderer, at hackere typisk kompromitterer IoT-enheder gennem udnyttelsen af sårbarheder eller bruteforce-angreb.

Mange IoT-enheder indeholder kendte sårbarheder, der, på trods af at have været offentligt kendte i op til flere år, ikke er blevet lukket via sikkerhedsopdateringer. Desuden er det ikke usædvanligt, at nogle producenter stopper med at supportere en IoT-enhed efter få år, og at produkter derfor kan indeholde vedvarende sårbarheder. Disse kendte sårbarheder udnyttes løbende af hackere, der ved hjælp af forskellige programmer scanner internettet for sårbare IoT-enheder, hvorefter de kompromitterer dem.

Sårbarhed i Realtek chipsæt resulterede i millioner af angreb
Den taiwanesiske halvleder-producent Realtek offentliggjorde i forbindelse med en sikkerhedsopdatering i august 2021 en alvorlig sårbarhed (CVE-2021-35394) i deres SDK chipsæt, der anvendes i flere IoT-enheder. Sårbarheden gør det muligt at kompromittere IoT-enheder med dette chipsæt, der ikke er opdaterede. Fra offentliggørelsen og frem til december 2022 har cybersikkerhedsfirmaet Palo Alto Networks observeret mere end 134 millioner forsøg på at udnytte sårbarheden.

Både statslige og ikke-statslige hackere forsøger desuden løbende at identificere ukendte sårbarheder, såkaldte zero day-sårbarheder, i IoT-enheder, som de kan udnytte. Det kan derfor være nødvendigt at beskytte IoT-enheder med yderligere sikkerhedstiltag i tillæg til regelmæssige opdateringer.

Ved bruteforce-angreb forsøger hackere, ofte ved hjælp af computerprogrammer, at få adgang til IoT-enheden ved at gætte kodeordet til den med mange forskellige kombinationer af bogstaver, tal og tegn. Det er ofte nemt for hackerne, da nogle IoT-enheder leveres med svage passwords eller standardpasswords, som aldrig udskiftes. Hackerne kan dermed scanne internettet for IoT-enheder, der er kendt for at have svage passwords og dernæst forsøge at kompromittere dem.

Hackere udnytter IoT-enheder til mange formål

IoT-enheder kompromitteres oftest for at blive brugt i botnet
CFCS vurderer, at den største trussel mod IoT-enheder kommer fra hackere, som kompromitterer IoT-enheder for at bruge dem i botnet.

Botnet er netværk af et stort antal kompromitterede computere og IoT-enheder, som via malware udnyttes af tredjeparter, såsom cyberkriminelle og statsstøttede aktører, til at understøtte øvrige cyberaktiviteter. Hackerne stjæler dermed maskinkraft fra de kompromitterede enheder for selv at bruge den, hvilket i nogle tilfælde også kan reducere IoT-enhedens ydeevne. IoT-enheder er bl.a. attraktive at bruge i botnet, fordi de sjældent er slukkede og dermed altid er tilgængelige for hackerne.

CFCS vurderer, at de fleste typer IoT-enheder udgør potentielle mål for hackere, som ønsker at udnytte enhederne til at udvikle botnet. Det skyldes, at hackerne alene er interesserede i at udnytte IoT-enhedernes maskinkraft og derfor på opportunistisk vis kompromitterer IoT-enheder i meget stort omfang og på tværs af samfundet. Kompromitteringen af IoT-enheder, som skal bruges til botnet, er derfor også sjældent rettet mod en specifik slags IoT-enheder eller IoT-enheder hos specifikke virksomheder eller organisationer. I stedet går hackerne efter de IoT-enheder, som kan kompromitteres gennem f.eks. kendte sårbarheder.

Bagmændene blev fanget, men truslen fra Mirai lever videre
Amerikanske myndigheder anklagede i 2017 tre personer for at have udviklet og kontrolleret et botnet kendt under navnet Mirai. Ifølge anklagerne havde personerne scannet internettet for sårbare enheder, som de efterfølgende kompromitterede via sårbarheder og tog kontrol over ved hjælp af specialudviklet malware. Da botnettet var størst, bestod det af mere end 300.000 IoT-enheder inkl. kameraer, routere og digitale videooptagere, som de tiltalte bl.a. brugte til at udføre DDoS-angreb eller lejede ud til andre cyberkriminelle. Ifølge anklagen forsøgte en af bagmændene i mindst et tilfælde også at afpresse et DDoS-offer økonomisk for at stoppe angrebet. De tiltalte har alle erklæret sig skyldige i anklagerne.

Selvom Mirai-botnettets bagmænd blev stoppet, kompromitterer kriminelle aktører fortsat IoT-enheder via sårbarheder og tager kontrol over dem via af nye former for Mirai-malware. Det skyldes, at kildekoden blev gjort tilgængelig på diverse hackerfora og nu i vid udstrækning bruges og videreudvikles af andre kriminelle hackere.

Hackere anvender botnet af kompromitterede IoT-enheder til flere formål. For kriminelle hackere drejer det sig oftest om at tjene penge. Nogle cyberkriminelle bruger f.eks. kompromitterede IoT-enheders maskinkraft til at generere kryptovaluta eller til at udføre DDoS-angreb mod ransomware-ofre og dermed øge presset på offeret. Andre vælger i stedet at udleje eller sælge deres botnet til øvrige aktører eller at bruge dem til at udføre kriminelle services, såsom DDoS-angreb, mod betaling.

Nogle hackere, herunder både kriminelle og statsstøttede aktører, udvikler dog også botnet af IoT-enheder for at bruge dem som infrastruktur for deres egne cyberaktiviteter. Denne aktivitet er ikke i sig selv økonomisk motiveret, men har i stedet nogle operative fordele for hackerne.

Ved at inkorporere botnet af kompromitterede IoT-enheder i deres infrastruktur styrker hackerne både deres kapacitet og evne til at operere i det skjulte, hvilket også reducerer risikoen for, at deres bagvedliggende infrastruktur opdages. Samtidig kan hackerne, ved at dirigere ondartet trafik gennem kompromitterede IoT-enheder, nemmere camouflere deres digitale færden som legitim trafik, hvilket gør det sværere for ofre at opdage og forsvare sig imod cyberangreb. Brugen af botnet betyder derfor også, at det bliver vanskeligere at afgøre, hvem der står bag et cyberangreb.

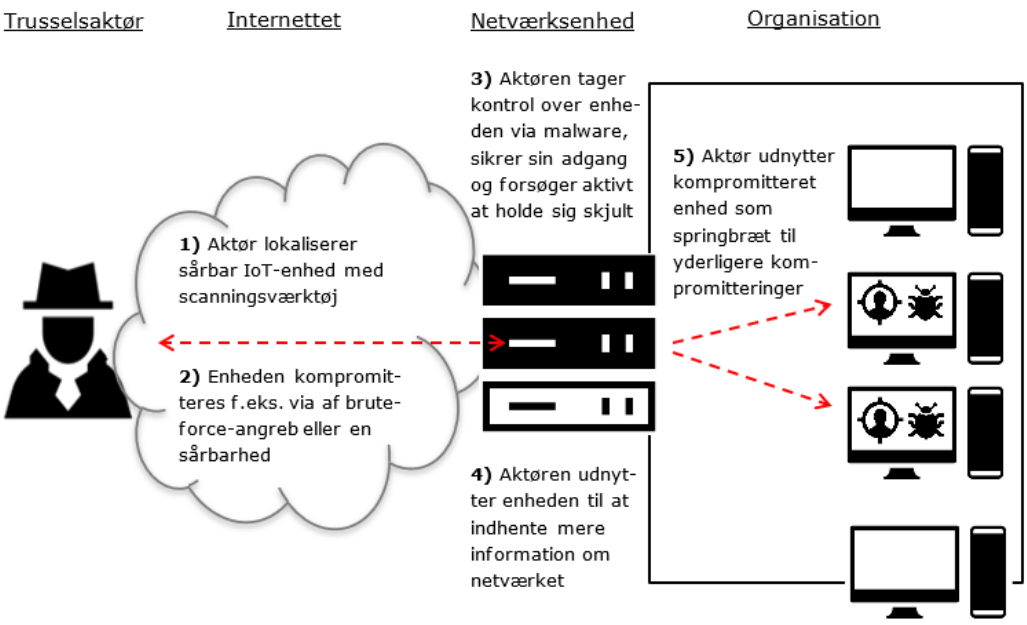
Kinesiske hackere udnyttede routere i Frankrig til at skjule aktiviteter
Den franske cybersikkerhedsmyndighed ANSSI offentliggjorde i 2021, at hackergruppen APT31 havde kompromitteret et meget stort antal routere i Frankrig. Routerne var af en type, der hovedsageligt blev anvendt i hjemmet eller på mindre kontorer. Ifølge rapporten om hændelsen var et af hovedformålene med kompromitteringen at samle de kompromitterede routere i et botnet, som kunne bruges til at udføre cyberaktiviteter i det skjulte. EU har tidligere attribueret cyberspionageaktiviteter fra APT31 til Kina's territorium.

Foto: Shutterstock

Cyberaktivister anvender hovedsageligt botnet til at udføre DDoS-angreb mod bl.a. hjemmesider, og det er muligt, at visse cyberaktivister kompromitterer IoT-enheder med det primære formål at udvikle botnet, som kan anvendes i cyberaktivistiske angreb.

Cyberkriminelle bruger IoT-enheder som indgangsvinkel i ransomware-angreb
Det er meget sandsynligt, at nogle kriminelle hackere kompromitterer IoT-enheder for at bruge dem som en indledende angrebsvinkel i deres cyberangreb.

Ved denne type angreb kompromitteres IoT-enheden ikke, fordi den i sig selv er interessant for hackerne, men derimod for at få adgang til det netværk, enheden er forbundet til. IoT-enheden bliver dermed en indgangsvinkel til et netværk, hvorigennem hackerne kan sprede sig til andre dele af netværket og eventuelt udføre flere cyberangreb. Det er ofte nyttigt for hackerne, da IoT-enheder typisk er mere eksponerede og dårligere beskyttede end almindelige computere og dermed udgør en relativt nem måde at få adgang til et netværk på.



Figur 1: Eksempel på hvordan IoT-enheder kan udnyttes som trædesten for yderligere cyberangreb.

Det er meget sandsynligt, at flere ransomware-grupper systematisk kompromitterer IoT-enheder med henblik på at etablere et indledende fodfæste i et offers netværk. Herfra kan ransomware-gruppen få mere viden om offerets netværk og dernæst bevæge sig til andre dele af netværket, inden de krypterer systemer og evt. stjæler de mest sensitive data, de kan finde, med henblik på afpresning.

Ransomware-gruppe brugte IoT-enheder som trædesten for angreb
I både 2021 og i 2022 blev ransomware-gruppen, der var kendt som Conti, udsat for et læk af gruppens interne informationer. Lækkene omfattede bl.a. interne chatbeskeder og trin-for-trin guides til at udføre ransomware-angreb. Af de trin-for-trin guides fremgår det blandt andet, at gruppens tilknyttede kriminelle blev opfordret til at undersøge, om et offer anvendte IoT-enheder, der kunne bruges til at få adgang til deres netværk. Samtidig viser de lækkede chatbeskeder, at gruppens medlemmer også ledte efter nye sårbarheder i netværksudstyr, de kunne anvende i cyberangreb.

Statsstøttede hackere bruger IoT-enheder som indgangsvinkel for spionage
Det er meget sandsynligt, at også statsstøttede hackere kompromitterer IoT-enheder med henblik på at bruge dem som indledende angrebsvinkler i cyberangreb. Årsagen er, som også nævnt i forrige afsnit, at IoT-enheder generelt er dårligere beskyttede end andre enheder i et netværk og derfor er en relativt nem vej ind i netværket.
CFCS vurderer, at hensigten med statsstøttede hackeres brug af IoT-enheder som indledende angrebsvektorer typisk er at udføre cyberspionage mod det netværk, som enhederne er forbundet til.

Truslen fra cyberangreb, hvor statsstøttede hackere anvender IoT-enheder som indgangsvinkler i cyberangreb mod et netværk, retter sig derfor særligt mod IoT-enheder anvendt af organisationer, der udgør et spionagemål for fremmede stater. For eksempel fordi organisationerne har en viden om udenrigs- og sikkerhedspolitiske forhold eller Forsvaret, eller fordi de har en særlig viden, som kan understøtte staternes teknologiske udviklingsmål og fremme økonomiske interesser.

Russiske hackere fik adgang til netværk gennem IoT-enheder
Ifølge Microsoft lykkedes det i 2019 statslige russiske hackere at kompromittere henholdsvis en IP-telefon, en printer og en videokoder hos tre af deres kunder med henblik på at etablere et indledende fodfæste i deres netværk. Herfra lykkedes det hackerne at få adgang til andre dele af netværket, som IoT-enheden var forbundet til, herunder brugerkonti med adgang til sensitive data.

Foto: Shutterstock

IoT-enheder kan udgøre et selvstændigt mål for cyberspionage
Udover at anvende IoT-enheder som en indledende angrebsvinkel for cyberspionage er det desuden meget sandsynligt, at statsstøttede hackere kompromitterer IoT-enheder, fordi de i sig selv kan udgøre et attraktivt cyberspionagemål. Det gælder særligt de IoT-enheder, der lagrer eller behandler data, som fremmede stater har en interesse i at få adgang til.

I undersøgelsesrapporten *Statsstøttet hackergruppe kompromitterer netværksudstyr i Danmark og resten af verden* har CFCS f.eks. beskrevet, hvordan statsstøttede hackere sandsynligvis forsøgte at kompromittere danske myndigheders netværksudstyr med henblik på at udføre cyberspionage. En aktivitet, der havde sammenfald med hændelser i udlandet og sandsynligvis var en del af en global kampagne.

Netværksudstyr, såsom routere og switches, kan bl.a. være interessante spionagemål for fremmede stater, fordi de kan give dem adgang til mails, filer og anden data, som sendes via enheden, hvis trafikken er svagt eller slet ikke krypteret. Samtidig kan statsstøttede hackere også anvende kompromitteret netværksudstyr til at få viden om det netværk, enheden er forbundet til. Viden som vil kunne anvendes i forbindelse med efterfølgende angreb. Eksempelvis har sårbarheder i netværksenheder før gjort det muligt for hackere at indsamle loginoplysninger i klar tekst fra netværket, som kan bruges til at få adgang til netværk.

Det er imidlertid ikke kun netværksudstyr, der kan være mål for cyberspionage. Overvågningskameraer kan bl.a. også udgøre et spionagemål, hvis de opsættes i nærheden af sensitive lokaliteter. For eksempel har det i internationale medier været fremme, at russiske hackere skulle have kompromitteret overvågningskameraer i Ukraine med henblik på at spionere mod Vestens støtte til landet.

Kompromitterede IoT-enheder muliggør destruktive cyberangreb

Selvom cyberspionage mod IoT-enhederne eller deres netværk oftest er formålet, når statsstøttede hackere kompromitterer IoT-enheder, kan kompromitterede IoT-enheder også anvendes i forbindelse med destruktive cyberangreb.

Ifølge britiske myndigheder var dette eksempelvis tilfældet, da statslige russiske hackere i 2018 anvendte malwaren VPN-filter, der udnytter sårbarheder i netværksudstyr, til at udføre destruktive cyberangreb mod enheder på tværs af Sydkorea i forbindelse med landets afholdelse af de Olympiske Lege. Angrebet medførte, at gennemførslen af de Olympiske Lege blev væsentligt forstyrret.

IoT-enheder kan også udgøre et selvstændigt mål for destruktive cyberangreb. For eksempel blev den amerikanske udbyder af sattelitkommunikation, Viasat, ramt af et såkaldt wiper-angreb på dagen for den russiske invasion af Ukraine. Ved wiper-angreb slettes, overskrives eller krypteres software og data, så det ikke længere er tilgængeligt. Angrebet medførte bl.a., at tusindvis af satellitmodemmer i særligt Europa blev sat ud af drift.

CFCS vurderer, at det generelt er mindre sandsynligt, at fremmede stater på nuværende tidspunkt har til hensigt at udføre destruktive cyberangreb mod mål i Danmark, herunder mod IoT-enheder. Det er dog sandsynligt, at statsstøttede hackergrupper forbereder sig på at kunne udføre destruktive cyberangreb med kort varsel, hvis hensigten skulle ændre sig. Dette sker bl.a. gennem cyberspionage. Det er muligt, at de også forbereder sig ved at kompromittere og spionere mod IoT-enheder og deres netværk.

Russiske hackere kompromitterer netværksudstyr verden over

Amerikanske og britiske myndigheder tilskrev i februar 2022 malwaren "Cyclops Blink" til den statslige russiske hackergruppe kendt som "Sandworm". Ifølge myndighederne var malwaren efterfølgeren til malwaren "VPNfilter", der ligesom Cyclops Blink havde til formål at kompromittere netværksudstyr i stor skala og samle dem i botnet med henblik på at muliggøre bl.a. cyberspionage, datamanipulation samt destruktive cyberangreb. VPNfilter-botnettet bestod ifølge amerikanske myndigheder i 2018 af flere hundredetusind kompromitterede enheder. Størstedelen var routere, som anvendes i hjemmet eller på mindre kontorer.

Cyberaktivister kompromitterer IoT-enheder for at levere et budskab

Det er meget sandsynligt, at nogle cyberaktivister udfører cyberangreb mod IoT-enheder med andre formål end at anvende dem i botnet. I disse tilfælde udnytter cyberaktivister oftest kompromitterede IoT-enheder til at dele deres budskab via et display på enheden eller gennem en anden af IoT-enhedernes funktioner.

Særligt pro-russiske og pro-ukrainske cyberaktivister har anvendt denne slags angreb til at sprede deres budskaber ifm. Ruslands invasion af Ukraine. Ifølge åbne kilder kompromitterede pro-ukrainske cyberaktivister i begyndelsen af krigen f.eks. en række ladestandere tilhørende den russiske energivirksomhed, Rosseti, for bl.a. at dele Putinkritiske budskaber på ladestandernes display.

Russiske printere ude af kontrol
I forbindelse med Ruslands invasion af Ukraine oplyste det cyberaktivistiske netværk, Anonymous, i marts 2022, at de angiveligt havde kompromitteret 156 printere på tværs af Rusland. Aktivisterne hævdede at have anvendt adgangen til at printe "anti-propaganda"-budskaber samt vejledninger, der skulle hjælpe russiske borgere med at omgå russisk statscensur.

Cyberaktivistiske angreb er generelt politisk eller ideologisk motiverede og har til formål at skabe mest mulig opmærksomhed omkring en specifik dagsorden. Angrebene er ofte rettet mod symbolske mål eller mål, der af cyberaktivisterne anses for at være modstandere af deres sag.

Angrebene har sjældent varige eller destruktive konsekvenser, men har i enkelte tilfælde haft en forstyrrende effekt. Dette var eksempelvis tilfældet i forbindelse med angrebet mod Rosseti's ladestandere, hvor cyberaktivister gjorde det umuligt at anvende ladestanderne i en periode.

IoT-enheder har også været ramt af hack-og-læk-angreb fra cyberaktivister. Ved denne type angreb kompromitterer cyberaktivister IoT-enhederne med henblik på at stjæle data og offentliggøre det på internettet sammen med et specifikt budskab. Ifølge åbne kilder kompromitterede en cyberaktivist i 2021 mere end 150.000 overvågningskameraer fra leverandøren Verkada. Efter kompromitteringen lækkede aktivisterne videooptagelser fra videokameraerne på internettet med et budskab om, at overvågning i samfundet fylder for meget.

Leverandører af IoT-enheder kan udgøre en sikkerhedsrisiko

En stor del af de IoT-enheder eller komponenter til IoT-enheder, der anvendes på verdensplan, produceres i lande uden for Danmarks normale sikkerhedspolitiske kreds. For eksempel er Kina dominerende på det globale marked for IP-forbundne overvågningskameraer.

Hvis en fremmed stats myndigheder har mulighed for at pålægge leverandører at bistå landets efterretningstjeneste, kan det gøre det muligt for disse stater at udnytte leverandører af IoT-enheder til bl.a. spionageformål. Som følge af Kinas efterretningslov fra 2017 kan den kinesiske regering eksempelvis kræve, at landets virksomheder bistår dets efterretningstjenester. IoT-enheder fra lande uden for Danmarks normale sikkerhedspolitiske kreds kan dermed udgøre en større sikkerhedsrisiko end udstyr fra andre lande. Særligt hvis enheden lagrer eller behandler data om personer eller organisationer, der udgør et spionagemål for de pågældende stater.

Derudover sælger nogle leverandører af IoT-enheder deres produkter til kunder i hele verden og leverer løbende opdateringer til disse produkter. Lykkes det for trusselsaktører at kompromittere en af disse leverandører, kan de derfor potentielt også få adgang til IoT-enhederne hos leverandørens kunder. Denne type angreb kaldes supply-chain-angreb og kan eksempelvis foregå ved, at trusselsaktører udnytter en kompromitteret leverandørs systemer til at indsætte en bagdør i et produkts firmware via en opdatering.

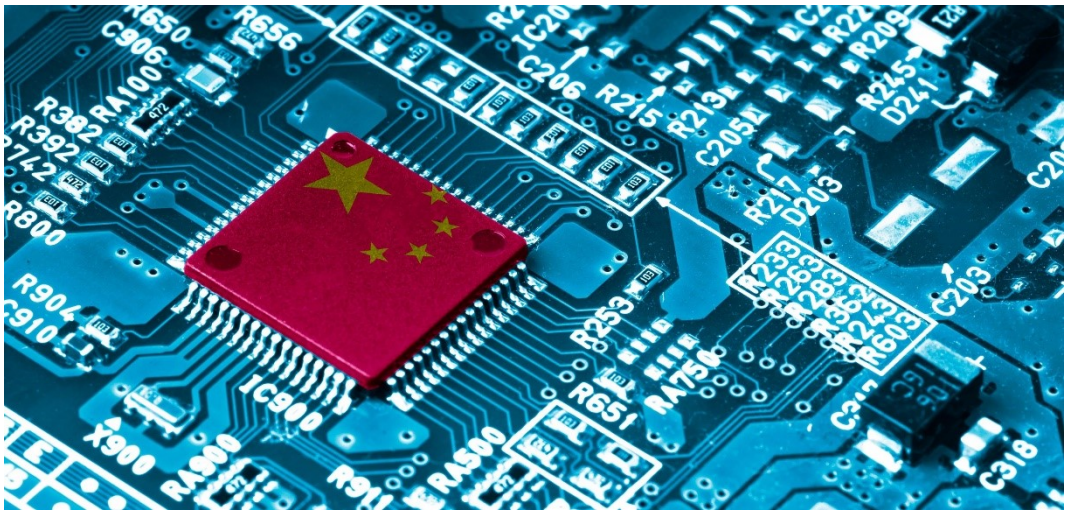


Foto: Shutterstock

Anbefalinger

Truslen mod IoT-enheder er **MEGET HØJ**, og det er meget sandsynligt, at IoT-enheder i Danmark vil blive ramt af forsøg på cyberangreb. Ligeledes kan alle IoT-enheder udgøre potentielle mål for cyberangreb. Det gælder uanset, om IoT-enheden bruges af privatpersoner, små og mellemstore virksomheder eller organisationer i den kritiske infrastruktur, som eksempelvis også udgør et spionagemål for fremmede stater.

Det er derfor vigtigt, at alle virksomheder og myndigheder er opmærksomme på den sikkerhedsrisiko, som følger af anvendelsen af IoT-enheder, og iværksætter mitigerende tiltag i relevant omfang. På den måde kan virksomheder og myndigheder bidrage både til egen sikkerhed og den nationale cybersikkerhed ved f.eks. at sikre, at overvågningskameraer eller routere ikke anvendes i botnet.

Få mere information og vejledning om, hvordan man kan øge sikkerheden i IoT-enheder i vejledningen "Beskyt IoT-enheder", som kan findes på www.cfcs.dk.

Andre CFCS-produkter

CFCS anbefaler alle til at følge udviklingen i trusselsbilledet i vores trusselsvurderinger på CFCS' hjemmeside: www.cfcs.dk. I forhold til emnet i dette produkt foreslår vi særligt at læse følgende:

- Trusselsvurdering: "Cybertruslen mod Danmark 2023".
- Undersøgelsesrapport: "Glemmer du, så husker hackerne".
- Undersøgelsesrapport: "Statsstøttet hackergruppe forsøger at kompromittere netværksudstyr i Danmark og resten af verden".

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer:

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, eller en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

FE bruger denne skala for sandsynligheder i analyser:

En sandsynlighedsgrad er udtryk for et skøn, ikke en beregnet statistisk sandsynlighed.
"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.