CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Hackere scanner dit netværk for sårbarheder hver dag året rundt

1. udgave juli 2021

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave juli 2021

Hackerne scanner dit netværk for sårbarheder hver dag året rundt

Formålet med denne trusselsvurdering er at orientere myndigheder og virksomheder om, at hackere konstant afsøger internettet for udstyr med sårbarheder, de kan udnytte til at kompromittere organisationen. Viden om truslen og hackernes metoder skal bl.a. bruges til at hjælpe myndigheder og virksomheder til at imødegå truslen fra hackernes scanninger.

Hovedvurdering

- Scanninger kan afsløre sårbarheder, som hackere kan udnytte, og udgør en vedvarende cybertrussel mod myndigheder, virksomheder og borgere. Truslen fra ondartede scanninger er **MEGET HØJ**.
- Alle, som benytter en offentlig IP-adresse, er et potentielt mål, fordi scanningerne ofte afsøger hele internettet for sårbarheder.
- En ondartet scanning kan føre til et målrettet cyberangreb. Det kan f.eks. ske, hvis en scanning afslører sårbarheder, som giver adgang til et særlig attraktivt mål.
- Nye enheder, der forbindes til internettet, bliver ofte opdaget af hackere inden for få minutter. Det betyder, at selv en kortvarig udsættelse af en softwareopdatering udgør en sikkerhedsrisiko.
- De fleste ondartede scanninger udføres af cyberkriminelle, men metoden anvendes også af statslige aktører.
- Selvom en scanning kan være et tegn på et forestående cyberangreb, er det som regel umuligt at afgøre, om en scanning er ondartet. Resultatet fra scanninger udført i en god mening, f.eks. af tjenester på internettet, kan imidlertid også udnyttes af hackere.

Analyse

Denne trusselsvurdering handler om hackeres vedvarende scanninger af internettet. Hackerne scanner efter enheder, som anvender en tjeneste eller software, der kan kompromitteres. Når de sårbare enheder er fundet, kan hackere få uautoriseret adgang til udstyret og de data og netværk, som udstyret er forbundet til. CFCS vurderer, at truslen fra ondartede scanninger er **MEGET HØJ**.

Alt udstyr, som er tilgængeligt fra internettet, er i farezonen. De ondartede scanninger er blevet dagligdag for mange it-sikkerhedsfolk. Derfor opfatter flere dem som forholdsvis uskadelige. Det er imidlertid kun tilfældet for de organisationer, som løbende sikrer sit udstyr og netværk.

Mængden af internetforbundne computere, servere, netværksenheder og apparater i virksomheder og hjemmet er konstant stigende. Hvis udstyret ikke er sikkert, kan det skabe huller i det digitale hegn, som beskytter adgangen til organisationers og almindelige borgeres lokale it-netværk.

Det er ikke muligt at afgøre det præcise antal enheder, der er forbundet til internettet, og tallene fra forskellige analysefirmaer varierer meget. I den lave ende af skalaen vurderer selskabet IOT Analytics, at der ved udgangen af 2020 var tale om cirka 20 mia. enheder, og at tallet vil stige til det dobbelte i løbet af de kommende fem år.

Netværksscanninger indgår typisk også i de indledende faser af cyberangreb, hvor hackere går efter et bestemt mål. Her vil scanningen ofte være mere avanceret og vedholdende samt sværere at opdage, fordi den foregår langsomt og fra flere IP-adresser. Formålet er at skabe et detaljeret billede af det it-netværk, som er mål for angrebet, så hackerne kan planlægge deres næste trin.

I den slags angreb vil hackerne typisk fortsætte, selvom scanningen ikke afslører åbenbare sårbarheder.

Sådan fungerer en scanning af internettet

En scanning sker altid ved hjælp af et computerprogram, som er specielt designet til at lave scanninger. Programmet kan scanne mange IP-adresser samtidigt.

1. I programmet angives, hvilke IP-adresser og porte der skal scannes, samt hvor avanceret eller aggressiv scanningen skal være.

2. Når scanningen starter, undersøger programmet først hvilke af de angivne IP-adresser, der reelt er i brug. Det begrænser den efterfølgende port scanning til kun at omfatte de aktive IP-adresser.

3. Programmet forsøger herefter at etablere forbindelser til de angivne porte på de aktive IP-adresser. Svarene, der sendes retur fra IP-adresserne, gemmes af programmet.

Efter scanningen vises hvilke IP-adresser, porte og tjenester, der kan skabes forbindelse til. Nogle programmer kan også vise, hvilken software der kører på servere, som programmet har kunnet oprette forbindelse til.

Omfanget af ondartede scanninger er enormt

Fordi der er mange, som scanner internettet, og fordi scanningerne foregår automatisk, hurtigt og vedvarende, er omfanget enormt. Det betyder, at der er en konstant baggrundsstøj af ondartede scanninger, som tester enhver IP-adresse for udstyr med sårbarheder.

Greynoise.io er en organisation, som klassificerer de IP-adresser, hvorfra scanninger foretages, som enten ondartede eller godartede. De ondsindede aktører er kendetegnet ved, at de forsøger at udnytte fundne sårbarheder, mens de godartede IP-adresser typisk tilhører kendte organisationer, som scanner uden ond hensigt.

Alene i februar 2021 registrerede Greynoise.io scanninger fra 1,3 mio. IP-adresser, der med sikkerhed kunne klassificeres som ondartede. Derudover var der scanninger fra mere end 10 mio. IP-adresser, som kunne være ondartede. Kun scanninger fra 12.000 IP-adresser blev med sikkerhed klassificeret som godartede.

AbuseIPDB.com er en anden hjemmeside, som registrerer IP-adresser, der har været anvendt til skadelig aktivitet. På siden kan enhver anmelde IP-adresser, hvorfra de er scannet eller forsøgt hacket. Hjemmesiden modtager tusindvis af anmeldelser hver time døgnet rundt. I 2020 modtog siden lige under 120 mio. anmeldelser i alt.

Offentlige IP-adresser

Alt udstyr, som er forbundet til internettet, har en offentlig IP-adresse. Det er et unikt nummer, svarende til en adresse, der gør det muligt at kommunikere med enheden over internettet.

Private IP-adresser

Private IP-adresser anvendes til kommunikation mellem enheder i lokale it-netværk. De reducerer behovet for offentlige IP-adresser, fordi samme private IP-adresse kan anvendes samtidig i forskellige lokale it-netværk.

IPv4

IPv4-protokollen er blevet anvendt siden internettets begyndelse. IPv4 kan håndtere godt 3,7 mia. offentlige IP-adresser. Det er de offentlige IPv4-adresser, som hackerne scanner.

I et lokalt netværk kan mange enheder på skift dele få offentlige IP-adresser. På den måde kan der være flere enheder tilknyttet internettet, end der er IPv4-adresser

IPv6
IPv6-protokollen er tiltænkt at skulle afløse IPv4. I praksis anvendes IPv6 parallelt med IPv4, og udstyr på internettet kan have både en IPv4- og en IPv6-adresse. IPv6 kan håndtere 3,4 x 10^{38} IP-adresser.

De mange IP-adresser betyder, at det ikke er praktisk muligt at scanne IPv6.

Alt udstyr, som kan tilgås fra internettet, er i farezonen
Enhver enhed, som kan nås fra internettet, bliver regelmæssigt, og måske flere gange i døgnet, gransket for kendte sårbarheder, som hackere kan udnytte.

Hvorvidt scanningen vil føre til et forsøg på en kompromittering afhænger alene af, om udstyret eller adgangen til udstyret er sårbar, og hvor let der er at udnytte sårbarheden. De fleste hackere går efter de lavest hængende frugter, så jo lettere en sårbarhed kan udnyttes, desto flere hackere vil lede efter den.

En konsekvens af de mange scanninger er, at blot en kortvarig udsættelse af en sikkerhedsopdatering, eller en midlertidig usikker konfiguration, måske med en usikker adgangskode, hurtigt findes af hackerne. Det kan medføre, at udstyret bliver kompromitteret. Ved at kende egen infrastruktur og løbende opsøge information om kendte sårbarheder kan en organisation forsøge at komme hackerne i forkøbet.

Enhver bruger af internettet er et potentielt mål for hackere
Mange brugere af internettet opfatter sig ikke som et interessant mål for hackere. De fleste hackere interesserer sig imidlertid ikke for, hvem de angriber, men afsøger internettet bredt efter udstyr, de kan kompromittere. Først når den indledende kompromittering er lykkedes, afgør hackeren, hvordan de kan udnytte adgangen. Det betyder, at enhver bruger af internettet kan blive mål for de ondartede scanninger.

Hacker kompromitterede hjemmeroutere via port 7547
I 2017 tilstod en britisk hacker, at det var ham, som i 2016 kompromitterede 900.000 hjemmeroutere hos kunder ved Deutsche Telecom.

Ved at scanne efter IP-adresser med port 7547 åben fandt hackeren hjemmeroutere, som på grund af en sårbarhed kunne tilgås fra internettet. Derefter var det let at få adgang, fordi mange ikke havde ændret standard brugernavnet og adgangskoden.

Målet var at inficere routerne med Mirai malware for at indlemme dem i hackerens botnet, som blev anvendt til DDoS-angreb.

Myndigheder og virksomheder er særlig udsat
Myndigheder og virksomheder er mest udsat for hackernes scanninger. Det skyldes at de ofte stiller tjenester til rådighed på internettet, hvilket private sjældent gør. Nogle eksempler er fjernadgang til servere og kontorarbejdspladser, hjemmesider, mailservere, IP-telefoni, og loginportaler til diverse kundetjenester.

It-udstyr i private hjem er som standard ofte beskyttet mod de ondartede scanninger. Det skyldes, at de hjemmeroutere, internetudbydere leverer til deres kunder, typisk spærrer for indgående datatrafik. Teknisk kyndige brugere kan dog vælge at åbne for adgang fra internettet til f.eks. en server i hjemmenetværket. Det medfører en risiko for, at hackere finder eventuelle sårbarheder i udstyret.

Ondartede scanninger kan føre til målrettede cyberangreb
Hvis en hacker efter en succesfuld scanning kompromitterer et særlig interessant mål, såsom en myndighed eller virksomhed, er der risiko for, at kompromitteringen følges op af et målrettet cyberangreb med eksempelvis ransomware.

Risikoen forstærkes af, at nogle hackere specialiserer sig i at finde og kompromittere netværk, for bagefter at sælge adgangene til andre hackere med kapacitet til at udføre mere målrettede cyberangreb.

Virksomhed ramt af ransomware og datalæk via hacket fjernadgang
I august 2020 blev den svenske virksomhed Gunnebo AB, som bl.a. leverer løsninger til adgangskontrol og kontanthåndtering, ramt af ransomware. Hackerne fik sandsynligvis adgang via en RDP-fjernadgang. Hackerne havde købt brugernavn og adgangskode til RDP-adgangen fra andre hackere, som tidligere havde fundet og kompromitteret adgangen.

Ifølge selskabet lykkes det at inddæmme angrebet uden at betale løsesummen, men interne data fra selskabet blev senere lækket af hackerne.

Hvem scanner internettet og hvorfor?
Der er mange, som scanner internettet, og de gør det med forskellige motiver. De fleste scanninger udføres af:

- Cyberkriminelle
- Stater eller statsstøttede hackere
- Internettjenester som Shodan og Censys
- Sikkerhedsfirmaer
- Universiteter og forskningsinstitutioner
- Script kiddies og andre, som primært er drevet af spænding

De ondartede scanninger udføres især af cyberkriminelle, og for dem er målet altid at få en økonomisk gevinst.

Kriminelle hackere kan enten selv udnytte eller videresælge en adgang til en server eller et netværk. Adgangen kan udnyttes til at kryptere data med ransomware, og stjålne data kan udnyttes eller sælges. Hacket udstyr kan f.eks. anvendes som en

proxy-server, der skjuler hackerens rigtige IP-adresse, inficeres med en kryptominer, eller inddrages i et botnet, som hackeren selv anvender eller lejer ud til andre hackere.

Statslige aktører scanner også internettet for udstyr eller adgange med kendte sårbarheder. Formålet kan være at kompromittere it-infrastruktur, som senere kan udnyttes i andre cyberangreb. En kampagne kan være målrettet et bestemt land, eller en specifik sektor.

Internettjenester som Shodan.io og Censys.io scanner internettet kontinuerligt og stiller resultaterne til rådighed via hjemmesider på internettet. På siderne kan brugerne se, hvilke IP-adresser, porte, tjenester og softwareversioner der er synlige på internettet. Hjemmesiderne kan også fortælle, om udstyret ser ud til at indeholde kendte sårbarheder.

Tjenesterne opfattes af nogle som kontroversielle, fordi informationen ikke kun kan bruges af organisationer til at sikre sårbare systemer, men også af hackere, som vil udnytte sårbarhederne.

Sikkerhedsfirmaer scanner generelt internettet med gode intentioner. Formålet vil ofte være at finde og fortælle offentligheden eller ejeren af IP-adresserne om sårbarheder, inden hackerne udnytter dem.

Universiteter og forskningsinstitutioner bruger typisk scanninger til at indsamle data, som anvendes i forskningsprojekter.

Portnumre og scanningsværktøjer gør det let for hackerne
Brugen af standard portnumre er nødvendig for at gøre tjenester generelt tilgængelige på internettet. Det gør det imidlertid også let for hackerne at scanne efter kendte sårbare tjenester, fjernadgange eller applikationer.

Hvis en hacker f.eks. ønsker at scanne efter fjernadgange, der anvender telnet-protokollen på standard portnummeret, er det kun nødvendigt at scanne efter port 23.

I januar 2020 delte en hacker telnet adgangsoplysninger for mere end 515.000 servere, hjemmeroutere og IoT-enheder i et populært hackerforum. Ved at scanne internettet for telnet-forbindelser, som anvendte standard eller svage adgangskoder, var det muligt for hackeren at gætte de korrekte adgangsoplysninger.

Der findes på internettet mange værktøjer, som hackere kan anvende til at scanne internettet. Masscan er populært, når mange IP-adresser skal scannes hurtigt, mens NMAP ofte anvendes til mere avancerede scanninger. I NMAP er det muligt med en enkelt parameter at angive, hvor mange af de mest anvendte portnumre man ønsker at scanne. Hvis der ikke angives andet, søger NMAP efter de 1000 mest anvendte portnumre.

Portnumre
Kommunikation over internettet kræver ikke kun kendskab til IP-adressen. Ligesom når man sender et brev, er det også nødvendigt at oplyse, hvem på adressen, man ønsker at tale med.

Ved at kombinere IP-adressen med et portnummer fortæller den afsendende computer, hvilken tjenester eller hvilket program der ønskes forbindelse til på den modtagende computer.

Der findes 65.353 mulige portnumre. For at sikre en effektiv kommunikation over internettet er mange netværksprotokoller og kommercielle produkter tildelt et standard portnummer.

Standard portnumrene betyder, at computere på forhånd ved, hvilken port der skal anvendes til en bestemt tjeneste eller applikation.

Uden åbne porte fungerer internettet ikke
En åben port er ikke nødvendigvis et problem. Uden åbne porte ville internettet ikke fungere, og det ville f.eks. ikke være muligt at besøge en hjemmeside eller sende en mail. Fordi en IP-adresse optræder i værktøjer som Shodan og Censys, betyder det altså ikke automatisk, at der er et sikkerhedsproblem.

En åben port er kun et problem, hvis den tjeneste eller applikation, som porten giver adgang til, er sårbar. Den kan være sårbar, fordi den er designet eller konfigureret på en usikker måde, eller fordi softwaren ikke er opdateret.

Nedenfor er eksempler på porte, som hackere ofte scanner, samt antallet af åbne porte ifølge Shodan pr. juni 2021.

22 (SSH)	Anvendes til krypteret fjernadgang til servere. Er meget brugt med cirka 15 mio. åbne porte på internettet, og er derfor et typisk mål for hackere.
23 (Telnet)	Protokol til fjernadgang. Selvom den ikke længere bør anvendes, fordi brugernavn og adgangskode sendes ukrypteret, er den stadig meget brugt. Cirka 2,7 mio. IP-adresser har denne port åben.
445 (SMB)	Anvendes til fildeling i Windows systemer. Wannacry, som var et verdensomspændende ransomwareangreb i 2017, udnyttede en sårbarhed i denne protokol. Mere end én mio. IP-adresser har porten åben.
3389 (RDP)	Anvendes til fjernadgang til en Windows computer. Sårbare RDP-adgange, som anvendes ved hjemmearbejde, har fået en del omtale under Covid-19 pandemien. Cirka fire mio. IP-adresser har denne port åben.

Bluekeep

Bluekeep er en sårbarhed i RDP-protokollen, som anvendes til fjernadgang. Sårbarheden blev offentliggjort i maj 2019, og eksisterede i flere versioner af Windows, før de blev opdateret.

Kort efter offentliggørelsen rapportede sikkerhedsfirmaer, at hackere scannede efter sårbare RDP-forbindelser på port 3389, der som standard anvendes til RDP. De værktøjer, som hackerne anvender, blev også opdateret med moduler, der kunne udnytte sårbarheden.

I dag er der globalt stadig tusindvis af Windows systemer, som indeholder Bluekeep sårbarheden.

En enkelt hacker kan scanne hele internettet på en time

Ligesom en indbrudstyv leder efter ulåste døre, eller vinduer der let kan brydes ind af, afsøger hackere konstant alle offentlige IP-adresser for at finde tjenester eller software med sårbarheder, som kan give hackeren uautoriseret adgang til udstyret.

Modsat indbrudstyven, som på en dag kun kan nå at undersøge få huse for sårbarheder, kan den digitale indbrudstyv ved hjælp af en computer, et effektivt scanningsprogram og en god internetforbindelse nå at scanne en enkelt port på alle offentlige IP-adresser inden for en time. Det betyder, at hvor husejeren kan være heldig ikke at få besøg af tyven, så er held ikke noget, man kan satse på i det digitale domæne.

I praksis tager en scanning fra en enkelt computer ofte længere tid. Det kan skyldes, at der scannes flere porte på hver IP-adresse, at åbne porte testes for hvilken tjeneste, der anvender porten, eller at scanningen forsøger at hente information ud om det operativsystem og den software, der kører på fundne servere. Firewalls kan også forsinke en scanning, da filtrerede porte ofte scannes flere gange for at afgøre, om et manglende svar skyldes en firewall eller en netværksfejl.

En scanning kan også være bevidst langsom for at undgå opdagelse, eller fordi den bliver sløvet af den løsning, som hackeren anvender til at skjule sin identitet. Det kan f.eks. være Tor-nettet.

Hackere kan øge hastigheden af en scanning ved at udføre scanningen med flere computere eller et botnet.

En ny fjernadgang scannes for sårbarheder inden for minutter

Hackere scanner ofte internettet for at finde sårbare fjernadgange. Særlig telnet-, RDP- og SSH-forbindelser er populære mål.

SSH-protokollen (Secure Shell) anvender som standard port 22. Fjernadgangen kan beskyttes med en adgangskode eller et kryptografisk nøglepar. De adgange, som kun er beskyttet med en adgangskode, er eftertragtede af hackere, fordi de kan kompromitteres blot ved at gætte brugernavn og adgangskode.

Statistik fra honeypots viser, at der ofte kun går sekunder eller minutter, før hackere opdager og forsøger at kompromittere en nyoprettet SSH-fjernadgang. Når en SSH-fjernadgang først er oprettet, kan adgangen være udsat for tusindvis af loginforsøg fra hackere hver dag.

Honeypot
En honeypot er en internetforbundet server, som er indrettet til at tiltrække hackere. Formålet er at analysere omfanget af hackerangreb og hackernes metoder. En honeypot kan simulere forskellige typer udstyr, tjenester og applikationer, afhængig af hvilke cyberangreb brugeren ønsker at indsamle data om.

Fordi en nyoprettet fjernadgang meget hurtigt opdages af hackere, vil selv fjernadgange, som kun åbnes kortvarigt, eksempelvis i en supportsituation, være i fare for at blive hacket, hvis den oprettes med standard eller svage adgangsoplysninger. Kritiske adgange bør derfor være sikret med en unik og sikker digital nøgle eller adgangskode, allerede inden der åbnes for adgangen fra internettet.

Ovenstående viser, at hvis en IP-adresse giver adgang til en kendt sårbar tjeneste, så er det sandsynligt, at hackere finder og udnytter sårbarheden inden for kort tid. Det gælder i særdeleshed, hvis tjenesten anvendes bredt, er kendt for let at kunne kompromitteres eller er i fokus i medierne på grund af sårbarheder.

Standard adgangskoder er en guldgrube for hackere
Meget netværksudstyr leveres fra fabrikken med et standard brugernavn og en standard adgangskode. Det gør det lettere at installere udstyret, men betyder også, at hackere kan få adgang til udstyret, hvis brugeren ikke ændrer standard adgangskoden.

”Admin” er en populær standard adgangskode
Meget udstyr anvender standard brugernavnet ”admin” eller ”root” og adgangskoden ”admin” eller ”password”.

Data fra en honeypot, der simulerede en SSH fjernadgang, viste at 97% af forsøgene på at logge ind, anvendte netop de brugernavne, og at de mest testede adgangskoder var ”admin”, ”password”, ”1234” og ”123456”.

Hackeren kan som regel finde standard brugernavnet og adgangskoden på leverandørens hjemmeside eller i en af de mange lister, som findes på internettet.

Problemet med standard koderne bliver yderligere forværret af, at forskellige leverandører ofte anvender de samme standard brugernavne og adgangskoder til deres udstyr.

Statistik fra honeypots viser, at hackere først går efter de lavthængende frugter. Når de har fundet en fjernadgang, vil de som det første forsøge at logge ind med udstyrets standard brugernavn og adgangskode.

Selv hvis en bruger skifter adgangskoden, lader de i mange tilfælde brugernavnet forblive standard. Ofte er det slet ikke muligt at ændre brugernavnet. Det gør det betydeligt lettere for hackeren, da det så kun er adgangskoden der skal gættes.

Hackere stjæler eller krypterer indhold i MySQL databaser
Hackere har i årevis scannet efter port 3306 for at finde MySQL databaser på internettet. Efterfølgende har de forsøgt at logge ind med typiske brugernavne og adgangskoder. Hvis hackeren får adgang, stjæler de indholdet eller krypterer det med ransomware.

I december 2020 opdagede sikkerhedseksperter, at data fra 85.000 MySQL databaser var sat til salg via en portal på dark web. Hackerne havde efterladt en note til ofrene om, at de indenfor ni dage kunne købe deres data tilbage via portalen, hvorefter dataene ville blive solgt til højestbydende.

Hackere skjuler deres identitet, når de scanner
Hackerne skjuler typisk deres identitet når de scanner. Det er derfor sjældent muligt at identificere oprindelsen af en scanning ud fra afsender IP-adressen.

Hackeren kan gemme sig ved at anvende proxyservere eller et botnet. På internettet findes lister med IP-adresser på proxyservere i forskellige lande, som enhver internetbruger kan anvende gratis. Tor-nettet, offentlige VPN-tjenester eller wifi-hotspots kan også skjule hackerens identitet. Hackere scanner også fra servere, de har lejet anonymt ved en cloud- eller hostingudbyder.

En anden mulighed er at benytte en udbyder, som ikke interesserer sig for, hvad kunderne anvender deres servere til, og som ikke svarer på henvendelser fra myndigheder.

Hollandsk hostingudbyder lejede servere ud til kriminelle
I oktober 2019 lukkede hollandsk politi hostingselskabet KV Solutions. Udbyderen havde tilladt kriminelle at leje selskabets servere. De kriminelle brugte bl.a. serverne til at scanne danske organisationers it-netværk.

I dette tilfælde skjulte gerningsmændene ikke deres spor, og det var derfor muligt at se den korrekte oprindelse af scanningerne. Det betød, at myndighederne kunne finde gerningsmændene.

Det er vanskeligt at afgøre, om en scanning er ondartet
En scanning kan indikere et forestående cyberangreb, men er i sig selv sjældent skadelig. Meget aggressive scanninger kan dog, ligesom et DDoS-angreb, overbelaste f.eks. en firewall.

Medmindre en scanning følges op af forsøg på at udnytte en sårbarhed, kan det være umuligt at afgøre, om den er ondartet eller blot harmløs indsamling af data. Det skyldes, at hackere, og de som scanner med gode intentioner, bruger de samme værktøjer og metoder.

Hensigten med den enkelte scanning er dog mindre væsentlig i forhold til risikoen for efterfølgende kompromittering. Dels er omfanget så stort, at alle organisationer jævnligt vil være mål for ondartet scanning. Dels er der altid en risiko for, at resultatet af en godartet scanning ender hos hackerne, eksempelvis via værktøjer som Shodan.

Det er derimod vigtigt ikke at eksponere software eller tjenester med kendte sårbarheder eller fjernadgange med svage adgangskoder på internettet.

Ønsker man at undersøge om en scanning er ondartet, kan man eventuelt få en indikation via de tidligere omtalte internettjenester, Greynoise.io og AbuseIPDB.com, eller lignende tjenester.

Hackere scanner efter sårbare Microsoft Exchange servere

Den 2. marts 2021 udsendte Microsoft sikkerhedsopdateringer til Microsoft Exchange servere. Årsagen var, at hackere havde udnyttet fire nul-dags-sårbarheder til at kompromittere mailservere. En af hackergrupperne, der har udnyttet sårbarhederne, har Microsoft kaldt Hafnium.

Efter offentliggørelsen begyndte flere hackere at scanne efter sårbare Exchange servere, og de udviklede værktøjer, der automatisk kunne udnytte sårbarhederne. Det medførte, at mange organisationer, også i Danmark, fik kompromitteret deres mailserver.

Den 4. marts oplyste Shodan på Twitter, at de havde fundet mere end 260.000 potentielt sårbare Exchange servere på internettet. De sårbare servere findes typisk på port 443, som er den standardport, der anvendes til krypterede forbindelser til webservere.

Det stigende antal internetforbundne enheder øger angrebsfladen

Den globale udvikling går mod en stadig øget digitalisering. Eksisterende og nye trådløse teknologier til internetkommunikation betyder bl.a., at der i 2025 vil være mindst 40 mia. digitale enheder i f.eks. virksomheder, hjemmet, byer, transportmidler og dagligdags apparater, som vil være forbundet til internettet.

Det er sandsynligt, at størstedelen af de mange nye internetforbundne enheder vil være sårbare over for angreb fra hackere. Det vil medvirke til at øge angrebsfladen, fordi hackere hele tiden får flere og nye sårbare mål, de kan angribe, og fordi muligheden for at skabe store botnet opretholdes eller ligefrem øges. Når antallet af sårbare enheder stiger, vil det samtidig øge mulighederne for de hackere, som ikke besidder avancerede hackerkompetencer.

Hvis der sikres et højt it-sikkerhedsniveau på de internetforbundne enheder og deres adgang til internettet, vil det blive sværere for hackerne at drage fordel af udviklingen.

Anbefalinger

CFCS anbefaler, at alle myndigheder og virksomheder inddrager truslen fra de ondartede scanninger i deres risikovurdering.

Da internetvendte tjenester i sagens natur er tilgængelige på internettet, er de mulige at finde via scanninger. Myndigheder og virksomheder bør derfor fokusere på at:

- Have overblik over, hvilke tjenester og porte der er tilgængelige
- Sikre, at kun de nødvendige og tiltænkte tjenester og porte er tilgængelige
- Holde software opdateret, og anvende sikre logins
- Minimere deling af software- og versionsinformation
- Have solide processer på plads, der sikrer det ovenstående

Hav overblik over tilgængelige tjenester og porte
Myndigheder og virksomheder bør sikre sig, at de har et klart overblik over de internetvendte tjenester, de er ansvarlige for. Det gælder, uanset om de driftes internt eller hos tredje-part. Opdateret dokumentation af disse er essentielt for at kunne sikre rettidige sikkerhedsopdateringer, undgå misforståelser på tværs af driftsfunktioner, og for at reducere risikoen for fejlkonfiguration.

Hav kun nødvendige og tiltænkte tjenester og porte tilgængelige
Da alle tjenester kan indeholde sårbarheder, er det vigtigt kun at gøre de nødvendige og tiltænkte tjenester tilgængelige fra internettet. Al trafik til porte, der ikke er nødvendige for tjenestens funktionalitet, bør blokeres i netværks- og hostfirewalls. Unødvendige tjenester bør ligeledes afinstalleres eller stoppes for at reducere angrebsfladen. Begræns også udgående kommunikation fra serverne til det nødvendige.

Hvor hjemmesider og mailgateways oftest skal være tilgængelige for alle på internettet, kan andre tjenester beskyttes bag eksempelvis en fler-faktor autentificeret VPN-forbindelse. Adgang til nogle tjenester kan også begrænses til kendte IP-adresser, som tilhører de samarbejdspartnere, der har behov for at kunne tilgå tjenesten. Tjenester til fjernadministration af en organisations it-infrastruktur bør aldrig være direkte tilgængelige på internettet. Ligeledes bør de heller ikke være tilgængelige for almindelige VPN-brugere.

For at sikre, at de tilgængelige tjenester afspejler det forventede, bør myndigheder og virksomheder regelmæssigt og automatiseret scanne deres egen infrastruktur udefra. Det kan hjælpe med hurtigt at identificere eventuelle fejlkonfigurationer, der utilsigtet synliggør unødvendige tjenester. Disse scanninger bør ikke stå alene, men suppleres med egentlige penetrationstests udført af it-sikkerhedsfirmaer med erfaring på området.

Hold software opdateret, og anvend sikre logins
Ondartede scanninger foretages ofte med det formål at identificere sårbare tjenester, der ikke har de seneste software opdateringer, eller anvender kendte standard passwords. Når tjenester stilles til rådighed på internettet, er det derfor essentielt, at den grundlæggende sikkerhed er på plads, herunder at de holdes rettidigt opdateret, og at der ikke anvendes konti med standard eller simple passwords. Login til internetvendte tjenester bør desuden suppleres med fler-faktor autentifikation.

Minimér deling af software- og versionsinformation
Mange scanningsværktøjer indsamler al information om de tjenester, der er tilgængelige på internettet. Det kan inkludere information om, hvilket produkt og version der anvendes. Hvis den anvendte version indeholder en kendt sårbarhed, vil denne information flage tjenesten som potentielt kompromitérbar og i nogle tilfælde automatisk blive forsøgt udnyttet. Myndigheder og virksomheder bør derfor rådføre sig med producenternes dokumentation for at se, om udstillingen af denne information kan begrænses eller blokeres. Det kan i nogle tilfælde gøres i selve produktet, og i andre tilfælde i eventuelle gateways eller reverse-proxy løsninger.

Hav solide processer på plads for håndtering af internetvendte tjenester
For at understøtte sikker drift af internetvendte tjenester er det vigtigt at følge etablerede processer for eksempelvis:

- Registrering og dokumentation af aktiver, anvendt software og komponenter
- Udrulning af sikkerhedsopdateringer
- Ændringshåndtering, herunder lancering af nye tjenester, regelændringer i firewalls, DNS ændringer, serverkonfiguration, netværksændringer osv.
- Sikring af servere og software, inden der åbnes op for adgang til dem

Derudover er det vigtigt at holde sig opdateret på viden om nye sårbarheder i software og komponenter i anvendelse, og om udgivelse af nye sikkerhedsopdateringer fra producenter.

Myndigheder og virksomheder med aktiv monitorering af deres internettrafik kan overveje at anvende løsninger til automatisk identifikation af kendte godartede scannere for at reducere falske positiver i deres monitoreringsløsninger.

I tillæg til ovenstående anbefalinger er det essentielt, at myndigheder og virksomheder har styr på deres grundlæggende it-sikkerhed. Det vil reducere risikoen for, at ondartede scanninger kan lede til udnyttelse af eventuelle sårbare tjenester, der er identificeret. På CFCS hjemmeside findes en række vejledninger, der kan være relevante i dette arbejde. Se eksempelvis:

- Cyberforsvar der virker
- Passwordvejledning
- Sikker håndtering af domæner

Undersøgelsesrapporten ”Anatomien af målrettede ransomware-angreb” indeholder også en række anbefalinger til sikring af fjernadgangstjenester, der ofte angribes med henblik på at opnå adgang til en organisations netværk.

Trusselsniveauerne

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynligheder i analyser