KROMANN REUMERT

SOLARWINDS OG HAFNIUM - HVAD VI KAN LÆRE AF DE TO STØRSTE CYBERANGREB I 2020/2021

Christel Teglers, advokat og partner i Kromann Reumert, 6. april 2021

Oveni i en global pandemi med coronavirus er der kommet en global pandemi med computervirus: De omfattende SolarWinds- og Hafnium/Exchange-angreb i 2020/2021 viser alvoren i kædehack - og den er skræmmende. Listen af ramte virksomheder vokser, og oprydningsarbejdet bliver enormt i Danmark og globalt.

SolarWinds og Hafnium/Exchange er i deres essens klassiske cyberangreb - men samtidig en påmindelse om, at cyberspionage ikke er for the faint hearted, og hvor hurtigt det går, når virus spreder sig.

Men hvad er der egentlig sket, og hvad dækker Solarwinds og Hafnium/Exchange over, og hvad kan vi lære af dem? Hvis du ikke har fulgt med i SolarWinds- og Hafnium/Exchange-hackene, har jeg samlet et overblik her.

1. STATSSTØTTEDE, SOFISTIKEREDE HACK MED SPIONAGE SOM HOVEDFORMÅL

Fællestrækkene for SolarWinds- og Hafnium/Exchange-angrebene er, at ***1)*** begge angreb tyder på at være statsstøttede (SolarWinds russisk, Hafnium kinesisk), ***2)*** begge angreb er højst avancerede, og kræver stor kapacitet at udføre, og ***3)*** begge angrebs primære mål var spionage. Herudover er angrebene ganske forskellige, og de gennemgås hver for sig nedenfor.

2. SOLARWINDS-ANGREBET

Supply chain-angreb: SolarWinds er et såkaldt *supply chain*-angreb (forsyningskædeangreb), hvor en hacker gemmer malware i en softwareopdatering, som det inficerede firma utilsigtet distribuerer til sine godtroende kunder. Supply chain-angreb er effektive, da angriberen kun behøver lykkes ét sted for at inficere potentielt tusindvis af netværk og systemer hos kunder, samarbejdspartnere osv. Det var således også et supply chain-angreb, der i 2017 lagde Mærsk-koncernen og andre internationale virksomheder ned, da et russisk cyberangreb målrettet ukrainske organisationer kom ud af kontrol, og inficerede flere globale og mindre virksomheder med et samlet tab på over 10 mia. USD til følge.

Russisk ATP-gruppe: SolarWinds-kampagnen startede formentlig i foråret 2020, men blev først opdaget i slutningen af 2020. Bagmændene er med al sandsynlighed statsstøttede russiske hackere (sporene peger på en russisk APT-gruppe, (Advanced Persistent Threat), en form for elitecyberenhed, der bl.a. kaldes Cozy Bear, UNC2452, Dark Halo, ATP29, SolarStorm og StellarParticle ("kært" barn har mange navne). Målet i angrebet har været spionage og indsamling af efterretninger, herunder hackerværktøjer der bl.a. bruges til kritiske redteam-test (avancerede cybersikkerhedstest). Det anslås, at over 1.000 professionelle hackere har arbejdet på angrebet, hvilket siger noget om dets usædvanligt store kapacitet og kompleksitet.

SolarWinds' sikkerhedshul: Det amerikanske it-sikkerhedsfirma, SolarWinds, spiller en ufrivillig hovedrolle i angrebet. Et af Solarwinds' bedst sælgende produkter er programmet Orion, der bruges til netværksovervågning. Hackerne lykkedes med at indsætte en bagdør (trojansk hest) i en sikkerhedsopdatering til Orion, som Solarwinds sendte ud til alle kunder, der bruger Orion-platformen. Hackerne gjorde det ved at udnytte et banalt sikkerhedshul hos SolarWinds: Kodeordet til SolarWinds server med opdateringer var "solarwinds123", hvilket hverken er svært at gætte eller bryde. Kodeordet var angiveligt fastsat af en tidligere praktikant, og havde formodentlig været uændret siden 2018 (måske længere)

Sunspot, Sunburst, Teardrop og Raindrop (malware): Ved brug af bagdøren kunne hackerne installere malware, der har givet adgang til interne systemer hos de organisationer, der bruger SolarWinds' Orion-platform (og installerede opdateringerne). Man har indtil videre identificeret mindst fire malware-typer, der er blevet brugt i angrebet: Sunspot, Sunburst (Solorigate), Teardrop og Raindrop. Hackerne plantede angiveligt først Sunspot-malwaren i SolarWinds' systemer, der blev anvendt til at plante Sunburst-malwaren, der blev distribueret til omkring 18.000 kunder. Hackerne udvalgte herefter nogle få mål ud af de 18.000, der havde fået installeret bagdøren, til at installere Teardrop-malwaren, der blev anvendt som såkaldt loader for Cobalt Strike-beacon (Cobalt Strike er en type malware der kan forblive skjult i operativsystemet og inficere netværk uden at vise synlige symptomer). I alle fire tilfælde anvendtes også Raindrop-malwaren.

Højst avanceret angreb: Sunburst-malwaren er indrettet sådan, at den ikke giver sig til at virke lige med det samme, men først efter omkring 14 dage, hvilket gør den endnu sværere at opdage. Efter en dvale-periode på ca. to uger begynder programmet at hente og udføre kommandoer (*jobs*), bl.a. filoverførsel, fileksekvering, systemprofilering, system genstart og deaktivering af systemservices. Malwaren har skjult sig i netværkstrafikken og gemt resultaterne af sin rekognoscering i legitime plugin konfigurationsfiler, hvilket har gjort det muligt for den at blande sig med legitim SolarWinds-aktivitet og undgå at blive opdaget af antivirusværktøjer.

Umuligt at forsvare sig imod: En række andre omstændigheder gør SolarWinds-hacket ydermere alvorligt, og viser, at det er umuligt at beskytte sig 100% imod et it-angreb: ***1)*** Malwaren kom ind via opdateringer til en anerkendt software (fra SolarWinds), der netop har til formål at beskytte mod ondsindet trafik. ***2)*** Angrebet har ramt organisationer, der netop har fulgt best practice med at holde deres systemer opdateret (dvs. ved at installere sikkerhedsopdateringen fra SolarWinds). ***3)*** Malwaren er fundet hos kunder, der slet ikke bruger SolarWinds-løsninger. ***4)*** Kun én ud af 18.000 organisationer opdagede bagdøren, - og det endda efter flere måneder -, hvilket nok primært skyldes, at det professionelle sikkerhedsfirma, FireEye, der opdagede bagdøren, har ressourcerne til at lede efter hack i deres systemer 24/7 og gennemteste al software (hvilket de færreste organisationer trods alt har)

Vanskelig forensic-opgave: Selvom op mod 18.000 kunder har fået installeret den bagdør, som Sunburst-malwaren skabte, er det usikkert i hvor mange tilfælde, hackerne konkret har udnyttet disse bagdøre, og hvor meget skade de har gjort. Usikkerheden skyldes bl.a., at angrebet stod på over 6-9 måneder, og at de fleste organisationer kun gemmer netværksovervågning og datalogning i 3-6 måneder. Dvs. uden komplet data er det særdeles svært at spore, hvad der er sket, og sandsynliggøre, at bagdøren ikke er blevet brugt. På verdensplan er identificeret mindst 200 organisationer og agenturer, der er hacket ved hjælp af bagdøren, herunder flere amerikanske statsorganer og firmaer (der umiddelbart var det primære mål).

Ramte i Danmark: I Danmark er omfanget af inficerede organisationer ikke (offentlig) kendt. SolarWinds-angrebet har dog øjensynligt ramt bredt, og mindst 30 myndigheder og virksomheder vides at have fået bagdøren installeret, heriblandt Vestforbrændingen, Bankernes EDB Central (BEC), Cowi, Statens IT, flere danske kommuner, SAS og to unavngivne danske energiselskaber. Tallet er angiveligt højere i praksis, og vi skal være glade for, at Danmark ikke var det direkte mål i lyset af, at bagdøren bl.a. blev etableret hos leverandører af kritisk infrastruktur i Danmark, der kunne have givet mulighed for at lukke for strøm- og varmeforsyning m.v.

Efterspil: SolarWinds udsendte i december 2020 nye softwareopdateringer til Orion-platformen, der fjernede bagdøren. Organisationer, der anvender SolarWinds Orion-platform, må forventes at have opdateret til denne version nu. Et overblik over hackets fulde konsekvenser har dog formentlig lange udsigter. Herhjemme har Center for Cybersikkerhed ikke be- eller afkræftet, om bagdøren hos de berørte danske myndigheder og virksomheder har været udnyttet til at stjæle data eller til at installere andre hackerværktøjer på det ramte netværk. Angrebet betragtes dog som så alvorligt, at det forlyder, at de

danske myndigheder specifikt har supply chain-angreb på agendaen, når de skal lægge den nye cybersikkerhedsstrategi for Danmark i 2021. Dette er i øvrigt i tråd med det lovforslag, der blev fremsat den 10. marts 2021 (L190), som skal sikre, at der kun anvendes pålidelige leverandører til 5G-nettet i Danmark, herunder for at imødegå risikoen for supply chain-angreb og spionage i den kritiske teleinfrastruktur.

3. HAFNIUM/EXCHANGE-ANGREBET

Nul-dags angreb (zero-day): Hafnium/Exchange er en type angreb, hvor en hacker udnytter en såkaldt "nul-dags sårbarhed" (zero-day vulnerability) til at inficere systemer og netværk med malware. En nul-dags sårbarhed er en sikkerhedsfejl, der endnu ikke er kendt af udvikleren/producenten, og som udnyttes af hackere, før en opdatering (patch) er udstedt. Sådanne angreb kaldes nul-dags angreb (zero-day attack/exploit), fordi udvikleren/producenten har 0 dage til at lukke (patche) sårbarheden. Informationer om nul-dags sårbarheder er særdeles værdifulde for it-kriminelle, virksomheder og efterretningstjenester, der gerne betaler mange penge ('bug bounties') for at få fat i dem - enten for at udnytte dem eller for at lukke sikkerhedshullet. Der er et stort, globalt marked for at købe og sælge 0-dags sårbarheder på det sorte og grå marked.

China Chopper og Exchange-sårbarheder: Hafnium-angrebet blev opdaget i januar 2021 af det danske sikkerhedsfirma, Dubex, der fik nogle alarmer fra en kunde, og kunne se, at kundens Exchange-server, der bl.a. indeholder alle Outlook-mailkonti, var inficeret af et kendt webshell kaldet China Chopper. Et webshell er et ondsindet fjernstyringsværktøjet (en bagdør), som giver hackeren mulighed for at fjernstyre serveren. Da Dubex undersøgte, hvor bagdøren kom fra, endte sporene ved Microsoft. Det viste sig, at Dubex havde opdaget en af i alt fire hidtil ukendte sårbarheder i Microsoft Exchange Server, der tilsammen kunne udnyttes til at få adgang til en Microsoft Exchange Server og installere en bagdør (her et webshell) uden at være logget ind eller have adgang til et internt netværk. Sårbarhederne og bagdøren har dermed givet adgang til at kopiere data, herunder mailindbakker, ud fra tusindvis af virksomheders computersystemer.

On-premise og hybridløsninger af Microsoft Exchange Server: De ramte systemer i Hafnium/Exchange-angrebet er ***1)*** kunder med on-premise installationer af Microsoft Exchange, og ***2)*** kunder, der benytter Office 365 og Exchange Online, og har en on-premise Exchange Server (dvs. en hybridløsning) - og som har installeret de inficerede opdateringsfiler til Exchange Server. Brugere til cloud-tjenesten Office 365 er ikke berørt.

Et af de største og mest sofistikerede angreb: Ifølge Microsoft har en gruppe formodede kinesiske statshackere, som Microsoft har døbt Hafnium (det latinske navn for København), målrettet udnyttet sårbarhederne i Exchange-serverne til at placere bagdøre (webshells) og ad den vej kunne overtage kontrollen af de interne systemer hos de Exchange-kunder, der har installeret de inficerede opdateringsfiler fra Microsoft. Man mener herudover, at mindst 9 andre APT-grupper, heriblandt LuckyMouse, Tick, Websiic, Winnti Group og Calypso, har stået eller står i kø for at udnytte de kritiske Exchange Server-sårbarheder, der endnu ikke er patchede (dvs. lukkede og opdaterede). Der spekuleres i, at oplysningerne om Exchange-sårbarhederne enten er blevet lækket i hackermiljøet eller fundet af en tredjepart, der leverer sårbarhedsoplysninger til cyberspioner. Det betragtes under alle omstændigheder for sandsynligt, at sårbarhederne har været kendt i hackermiljøet i længere tid

Over 250.000 organisationer ramt globalt: Ingen kender Hafnium/Exchange-angrebets præcise omfang, men det anslås indtil videre, at over 250.000 organisationer globalt er ramt, herunder 30.000 i USA, Den Europæiske Banktilsynsmyndighed (EBA), det norske Storting og godt 1.800 servere i Danmark. Der kan altså være mange store og små virksomheder samt offentlige myndigheder, der allerede er angrebet med succes og har fået - eller kan have - fået kopieret/stjålet data, herunder e-mails med forretningshemmeligheder, fortrolig, sensitiv eller anden personlig data. Ifølge Microsoft er de berørte

bl.a. forskere i smitsomme sygdomme, advokatfirmaer, universiteter, politiske tænketanke og NGO'er. Microsofts præsident har beskrevet angrebet som det største og mest sofistikerede angreb, verden hidtil har set. I starten tydede det på, at angrebet gik mod udvalgte organisationer, men det er nu så udbredt, at det næppe længere er tilfældet.

Nød-patches lukker sikkerhedshullet - men reparerer ikke, hvis skaden er sket: Microsoft udsendte i starten af marts 2021 såkaldte nød-patches (ekstraordinære sikkerhedsopdateringer udenfor Microsofts månedlige opdateringscyklus), som lukkede sårbarhederne. I dag må stort set alle virksomheder, der kunne være berørt af Hafnium-angrebet, forventes at have opdateret (patchet) deres systemer. Problemet er imidlertid, at selv hvis sikkerhedshullet er blevet lukket nu, kan skaden allerede være sket, hvis hackere forinden har fået adgang til systemer. Det kan i den forbindelse være særdeles vanskeligt at vurdere, hvilke systemer hackerne er i, hvor dybe de er, hvilken adgang de har, og hvilke værktøjer de har efterladt, f.eks. til at installere kryptominers og ransomware (se nedenfor).

Udløbere med DearCry og Black Kingdom ransomware: Det blev hurtigt kendt i marts 2021, at andre hackere har udnyttet Hafniums offentlige webshells til kompromitterede mailservere, og har været i gang med at installere ransomware på serverne (ransomware er ondsindet software, der inficerer et system, og kræver et pengebeløb for at låse det op igen). Det kræver ikke andet end URL'en til et af de offentlige webshells for at få kontrol over den kompromitterede server. Alene i marts 2021 har været mindst to ransomware operationer i kølvandet på Exchange-sårbarhederne: Én med en ny type ransomware kaldet DearCry og én med en kendt type ransomware kaldet Black KingDom. Det anslås, at kompromitterede myndigheder og virksomheder for disse ransomware-angreb bl.a. findes i USA, Canada, Australien, Tyskland, Frankrig, UK og Israel.

Efterspil: Udover nød-patches har Microsoft udsendt vejledninger til at installere programrettelser og en række indikatorer, som kan anvendes til at undersøge, hvorvidt en Exchange Server-installation er kompromitteret. Disse vejledninger og øvrige anbefalinger til håndtere de kritiske sårbarheder i Microsoft Exchange Server, er samlet på Center for Cybersikkerheds hjemmeside (Varsel om Exchange-sårbarheder (cfcs.dk)). Sagen er imidlertid også, at hackere allerede har brugt Exchange-sårbarhederne til at forberede deres egne ransomware-angreb på de inficerede systemer, og vi har derfor desværre næppe set de sidste angreb i kølvandet på Exchange-sårbarhederne.

4. LÆRINGSPUNKTER

Vi må acceptere, at statslig digital krigsførelse - cyberkrig - er virkelighed, og at den kæmpes på ryggen af private virksomheder, der typisk bliver ofre for målrettede, sofistikerede kampagner af militær præcision. Der findes ikke nogen nemme løsninger. Uanset hvor meget man gør, for at beskytte sig, kan man stadig risikere at blive ramt. Enten målrettet eller tilfældigt.

Hændelserne understreger, at cybersikkerhed og cyberrobusthed er en tværorganisatorisk risikostyringsopgave, der starter hos topledelsen, og adresserer alt lige fra risikovurderinger til implementering af foranstaltninger og beredskab til dels at *forebygge* sikkerhedsbrud, dels at *reagere* effektivt på hændelser, og hurtigt *komme tilbage* igen. Dette fokus afspejles også i EU-Kommissionens udkast til et nyt NIS-direktiv (NIS2), hvor der lægges op til at styrke cyberrobustheden gennem bedre overblik, beredskab, videndeling og operativt samarbejde.

SolarWinds- og Hafnium/Exchange-angrebene vil formentlig få flere organisationer til at revurdere deres risikobillede. Nogle faktorer, der må forventes at spille ind, omfatter:

- Overblik: Om organisationen har et retvisende og opdateret overblik over sin infrastruktur (systemer, netværk, applikationer, leverandørlandskab mv.). Uden dette er det svært at vurdere både risici (præventivt) og om man kan være i risikogruppen ved en it-sikkerhedshændelse (reaktivt).

- Patching: Om organisationen (eller dens leverandører) følger best practices med altid at holde it-software og kritiske systemer opdateret.

- Logning: Om organisationen (eller dens leverandører) foretager tilstrækkelig logning for at have det nødvendige datagrundlag til at afdække eventuelle it-sikkerhedshændelser, herunder om der logges længe og omfangsrigt nok, og om man logger de rigtige enheder / kritiske systemer.

- Sensorer: Om organisationen (eller dens leverandører) anvender tilstrækkelige digitale sensorer, der skal identificere usædvanlige hændelser og opdage angreb i netværket så tidligt som muligt.

- Zero-trust tilgang: Om organisationen ift. alle eller udvalgte kritiske leverandører skal have en sikkerheds-indstilling, hvor man tager udgangspunkt i "assume breach", herunder ved at antage, at systemer og services kan være kompromitterede, og derfor kun skal have absolut færrest mulige rettigheder (ud fra "least privilege"-princippet).