Dagboek van een ransomware-aanval: aanval, wederopbouw, best practices

Ransomware kan snel en hard toeslaan. Het is zaak om daar goed op voorbereid te zijn. Een Nederlandse multinational ondervond dit toen het slachtoffer werd van de Conti-ransomware.

We horen en lezen vrijwel dagelijks over de gevaren van ransomware. Die berichten komen dan vrijwel altijd van leveranciers van security-oplossingen. Een open gesprek met een slachtoffer van een dergelijke aanval is echter zeer zeldzaam. Dat is op zich niet zo gek natuurlijk. Organisaties praten nu eenmaal niet graag over hoe ze hun cybersecurity ingericht hebben met de pers. Dat zou hen alleen maar kwetsbaarder maken, is het idee. De aanvallers kunnen ook meelezen.

Of spreken over je cybersecuritystrategie je ook daadwerkelijk kwetsbaarder maakt, betwijfelen we. We snappen echter wel dat dit niet bepaald hoog op de lijst van prioriteiten staat voor organisaties. Je kunt er minder goede sier mee maken in de media dan met alles rondom 'digitale transformatie'. Daarnaast nemen veel organisaties grote beslissingen op het gebied van cybersecurity vaak pas nadat er iets ernstigs heeft plaatsgevonden. Dat is natuurlijk ook niet bepaald de boodschap die je de wereld in wilt brengen over je organisatie.

Daarom zou het juist goed zijn om dit soort verhalen vaker te brengen. We waren dan ook erg blij dat wij als SentinelOne een klant bereid vonden om uitgebreid te praten over hoe hij eind 2021 slachtoffer werd van een ransomware-aanval. De enige voorwaarde was dat we de naam van zowel het bedrijf als de woordvoerder uit het verhaal zouden laten. Het doet verder niets af aan de impact van het verhaal overigens. De lessen die eruit te trekken zijn, veranderen niet.

Multinational met een divers landschap

Het bedrijf waar we het in dit artikel over hebben is een multinational die bestaat uit vijftien ondernemingen. De woordvoerder waar wij mee spreken is verantwoordelijk voor security. De multinational heeft in totaal zo'n 2000 endpoints in beheer en enkele honderden servers. Dit geeft een goede indicatie van het formaat van het bedrijf.

Als het gaat om cybersecurity binnen de multinational, heeft de woordvoerder te maken met een tamelijk divers landschap. Dat wil zeggen, de ondernemingen liggen niet alleen in verschillende landen, maar hebben ook niet allemaal dezelfde infrastructuur. Ook het securityniveau verschilt tussen ondernemingen. Het bedrijf is weliswaar continu bezig om het niveau te verhogen, maar sommige ondernemingen komen van verder en doen er langer over om op het gewenste niveau te komen. De intentie is overigens wel om nieuwe oplossingen en tooling zo breed mogelijk uit te zetten bij alle ondernemingen, maar soms is dat vanuit technisch oogpunt lastig of onmogelijk.

Dag 1: Zwakste schakel is het doelwit, maar besef is er niet meteen

Bovenstaande situatie had als resultaat dat niet iedere onderneming van de multinational bij de tijd was, zoals de woordvoerder het noemt. Het uiteindelijke doelwit van de ransomware-aanval viel daar ook onder. Deze onderneming had geen MFA, deed geen awareness training en er waren zoals vrijwel altijd het geval is enkele kwetsbare servers. Er was wel een goede back-up bij die onderneming.

Het eerste signaal dat er iets niet in de haak was, kwam op een vrijdagavond. Een monitoringtool gaf een melding dat servers niet bereikbaar waren. Op dat moment gingen er echter nog geen alarmbellen af, omdat er in de periode ervoor een aantal stroomstoringen waren geweest in verband met onderhoud aan het stroomnet in die regio. Die stroomstoringen werden in eerste instantie gezien als de veroorzaker. “We zouden dit probleem de volgende dag wel oplossen”, geeft de woordvoerder de gemoedstoestand op dat moment aan.

Bovenstaande reactie klinkt wellicht niet bijster slim, maar is wel een heel natuurlijke reactie, zeker in combinatie met de stroomstoringen. Dit soort dingen maakt een IT-afdeling regelmatig mee. Zonder de juiste tools (die op dat moment dus niet aanwezig waren bij dit bedrijf) heb je simpelweg niet in de gaten dat er iets mis is. Je kunt dit natuurlijk proberen op te vangen door alle incidenten in eerste instantie als een securityincident te bestempelen, maar dat is in de praktijk waarschijnlijk ook geen prettige manier van werken.

Dag 2: Omvang wordt duidelijk, snel reageren gewenst

Was het op vrijdagavond nog niet meteen duidelijk dat er dingen niet in de haak waren, op de tweede dag (de zaterdag dus) was dat wel het geval. De woordvoerder kreeg die dag een melding dat het foute boel was bij die ene onderneming. Alle servers waren door de ransomware ge-encrypt, waarmee ook alle bedrijfskritische applicaties niet meer bruikbaar waren. Met andere woorden, alles stond stil, de core business van de onderneming was onmogelijk geworden. De situatie werd de eerste uren daarna ook alleen maar erger. Het ene na het andere systeem bleek onbereikbaar. Het werd steeds duidelijker dat de onderneming in zijn geheel hard getroffen was.

Op het moment dat duidelijk is dat het om een ransomware-aanval gaat, is de eerste reactie erg belangrijk, geeft de woordvoerder aan. Voor dit bedrijf was het de eerste keer dat ze het meemaakten, dus niemand had er ervaring mee. Toch reageerde men snel en krachtig. Uiteraard ging meteen de firewall volledig dicht. Daarnaast zette de onderneming een crisisteam op. Het is heel belangrijk om dit zo snel mogelijk te doen, volgens de woordvoerder. Zorg ook dat je weet wie er in dat crisisteam moet. Met andere woorden, leg dit op voorhand vast, op een moment waarop het geen crisis is. De profielen in zo’n team en dan met name de ervaring met het nemen van beslissingen zijn verder cruciaal, geeft hij aan.

Hulp inroepen, soms tevergeefs

Na het organiseren van het crisisteam, moeten er daadwerkelijke stappen gezet worden om de ransomware te lijf te gaan. De getroffen onderneming had echter een probleem. Het nam nog geen managed diensten af bij securitypartijen die het in kon zetten als het getroffen werd. Dat is volgens de woordvoerder wel echt heel belangrijk. De meeste organisaties zijn niet in staat om de specialisten die hiervoor nodig zijn, zelf aan te nemen.

De multinational was al in gesprek met een aantal endpointsecurity leveranciers, waaronder de huidige leverancier, om managed services af te gaan nemen. Het was al snel duidelijk dat de huidige endpoint security leverancier geen capaciteit had om te helpen. Formeel was er nog geen sprake van een getekende overeenkomst, dus op zich stond die partij in zijn recht.

Er is vervolgens door het crisisteam besloten om contact te leggen met één van de andere endpoint security leveranciers waarmee men al in overleg mee was; SentinelOne. De andere leverancier waarmee gesprekken liepen was CrowdStrike, de andere *usual suspect* op het gebied van geavanceerde EDR/XDR.

De keuze om voor SentinelOne te gaan was enerzijds financieel gedreven, maar er was ook al een POC mee gedaan. Daarnaast heeft de multinational de neiging om voor best-of-breed oplossingen te kiezen, niet voor best-of-suite. Bij SentinelOne is dat meer het geval dan bij CrowdStrike, geeft de woordvoerder aan.

Nog geen anderhalf uur na contactopname had SentinelOne een Vigilance team (Digital Forensics and Incident Response Team) opgezet speciaal voor de getroffen onderneming. Ze hoefden niet eerst allerlei zaken te tekenen, omdat men bij SentinelOne heel goed begreep dat er eerst een crisis bestreden moest worden. Het Vigilance-team van SentinelOne was duidelijk zeer ervaren met het bestrijden van dit soort aanvallen en ging meteen van start. Het is volgens de woordvoerder cruciaal geweest dat het een perfecte samenwerking betrof en het eigenlijk een prettige ervaring was midden in een crisis. “Het Vigilance team van SentinelOne stelde de juiste vragen, deed de juiste voorstellen, waardoor we uiteindelijk een soort *lifeguard* gevoel kregen en elke stap daadwerkelijk een stap voorwaarts betrof”, vat de woordvoerder het samen. Het feit dat er een goede (immutable) backup beschikbaar was heeft dit proces vereenvoudigd.

Dag 3: De wederopbouw

Intussen was er samen met SentinelOne een stappenplan gemaakt om de onderneming stukje bij beetje weer in de lucht te krijgen. Dat was een behoorlijke klus, want in principe moest alles opnieuw opgebouwd worden. Dat wil zeggen, alle servers draaiden en draaien in VMware en ook de hosts waren niet meer beschikbaar. Dat betekent dat VMware zelf in principe ook weg was. Ze moesten alle hosts volledig vanaf de grond opnieuw opbouwen.

De wederopbouw begon met het restoren van de servers die randvoorwaardelijk zijn voor de omgeving van het getroffen bedrijf, zoals de VMware hosts en vervolgens de domain controllers (VMs). Als een VMware host eenmaal weer in de lucht is, kan de restore van een VM gedaan worden vanuit een back-up.

Vervolgens werd op de server de SentinelOne-agent gezet. De SentinelOne agent op de server werd dan in een modus opgestart waarmee alleen communicatie met de SentinelOne cloud gemaakt kon worden. Vanuit SentinelOne kon men dan (op afstand) controleren of de server gezond was. Zeker bij de eerste servers die op deze manier weer tot leven werden gewekt, trof men nog sporen van ransomware aan. Om ervoor te zorgen dat dit geen verdere problemen oplevert, heeft men op aangeven van het Vigilance team bepaalde poorten en hosts op de firewall direct geblokkeerd. Via die poorten communiceert de ransomware met de buitenwereld. Zodra een server uiteindelijk groen licht kreeg, nam SentinelOne deze op in de reguliere 24/7 managed dienst.

Vanuit SentinelOne ging men overigens niet alleen reactief te werk. Men vroeg ook pro-actief om zoveel mogelijk informatie te delen. Dit om te kunnen bepalen welk type ransomware het was. Denk hierbij aan de logfiles van de firewalls die de onderneming heeft staan. Uit die bestanden identificeerde SentinelOne al vrij snel de zogeheten *beacons* voor de aanval. Daarnaast wilde SentinelOne ook graag een image of in ieder geval toegang tot een van de versleutelde servers van de onderneming. Dat had op dag twee vanzelfsprekend niet de aandacht, maar kon de onderneming tegen het einde van dag drie, op zondagavond dus, al wel leveren. Op basis van al deze informatie stelde SentinelOne vast dat het om de Conti-ransomware ging.

Dag 4 en verder: Stap voor stap herstarten
Op zondagavond, toen de onderneming het image richting SentinelOne stuurde, was het al behoorlijk ver met de herstart. Zaken zoals domain-, mail- en fileservers waren alweer in de lucht bijvoorbeeld. Zondagavond/maandagochtend ziet de woordvoerder dan ook als omslagpunt. Toen kregen ze ook de eerste kritische applicaties online. Daarna kwamen één voor één de belangrijkste applicaties weer online.

Let wel, de onderneming was toen nog altijd niet operationeel. Daarvoor moest het geduld hebben tot in de loop van de dinsdag. Toen kwamen de systemen weer in de lucht waarmee het bedrijf orders aanneemt. Dat is onderdeel van de kern van de activiteiten van de multinational en dus ook van deze onderneming. Een voordeel van deze specifieke onderneming is dat deze in de weekenden eigenlijk niet zoveel zakendoet. Dit betekent dat het onderaan de streep maar 1,5 dag echt last gehad heeft van de ransomware-aanval. Dat is een geluk bij een ongeluk. Het volledig herstellen van de aanval duurde nog wel een paar weken extra trouwens. Dat is de tijd die het duurde om alle servers weer in de lucht te krijgen op een veilige manier.

Het is voor vrijwel iedere organisatie van belang om zo snel mogelijk te herstellen van een ransomware-aanval. Voor de onderneming waar we het nu over hebben stond het voortbestaan ervan echt op het spel. In het segment waarin deze actief is kun je maximaal een week stilliggen. Daarna wordt het heel lastig om het marktaandeel te behouden. Vandaar ook dat de beslissers binnen de multinational de lijnen richting de Conti-groep open hebben gehouden. De optie tot betalen heeft ook altijd op tafel gelegen. Het is makkelijk zeggen dat je niet moet betalen, maar als het voortbestaan van een bedrijf ervan afhangt, ligt dat toch net even anders.

Belangrijke lessen geleerd
Al met al was de multinational dus na een paar dagen weer operationeel. De aanval is afgeslagen en het voortbestaan van het bedrijf is verzekerd. Na een dergelijke aanval is het echter ook belangrijk om duidelijk te krijgen welke lessen eruit getrokken kunnen worden. Die lessen, die ook relevant zijn voor andere organisaties, zetten we in het restant van dit artikel onder elkaar. Je zou dit kunnen zien als een uitgebreide conclusie.

Les 1: Krijg en hou de juiste mindset
Als we de woordvoerder van de multinational aan het einde van het gesprek vragen wat hij en de organisatie als geheel ervan geleerd hebben, komt als eerste de term ‘mindset’ bovendrijven. Die is fundamenteel veranderd binnen de hele organisatie. Cybersecurity initiatieven zijn nu in een stroomversnelling gekomen.

Nu is het zaak om deze staat van paraatheid vast te houden. Het ebt namelijk nu ook al wel weer een beetje weg, constateert de woordvoerder ook. Vandaar ook dat er stevig is ingezet op security awareness trainingen. Daar heeft niet iedereen zin in, maar de gebeurtenissen van eind 2021 zijn een les geweest voor het bedrijf. Dus iedereen zal er toch aan moeten geloven, linksom of rechtsom.

Les 2: Zet een ervaren crisisteam op
Een tweede belangrijke les is dat de samenstelling van het crisisteam van cruciaal belang is. Als ze niet zo’n ervaren team hadden gehad, was het anders afgelopen, is de stellige overtuiging van de woordvoerder. Wat dat betreft ziet de woordvoerder het Vigilance team als onderdeel van het crisisteam. “Zonder SentinelOne hadden we zo tegen een tweede aanval aangelopen”, is hij stellig van

mening. Met het team dat er nu stond, was iedere stap er eentje vooruit. Iedereen had continu het gevoel dat het de goede kant op ging.

De belangrijkste eigenschap die in ieder geval meerdere leden van een dergelijk team moeten bezitten, is dat ze ervaring hebben met het managen van crises en goed kunnen samenwerken met de specialisten van een extern team, in dit geval het SentinelOne Vigilance team. Praktijkervaring dus, niet alleen gebaseerd op trainingen. Trainingen zijn ook altijd beter dan geen trainingen, maar in de praktijk is het toch fundamenteel anders.

Les 3: Basishygiëne helpt al heel veel om aanvallen te voorkomen

SentinelOne is een van de meest geavanceerde cybersecurityspelers in de wereld op dit moment. Het bedrijf heeft de aangevallen onderneming ook zeker heel goed geholpen. Toch begint goede security ergens anders, bij de basis. Dat betekent MFA overal doorvoeren, servers en systemen updaten en patchen en security awareness trainingen door het personeel laten doen. Daarbij spreken ze ook mensen aan die er niet aan meedoen. De vrijblijvendheid is weg op dat vlak. Daarnaast moeten back-ups over de hele organisatie 'ransomwareproof' zijn. Tot slot is het goed om sterk te sturen op SSO en password management.

Het is kortom geen rocket science, om de woorden van de woordvoerder te gebruiken. Zo werken de meeste organisaties al Active Directory of Azure Active Directory. Maak dan ook gebruik van de mogelijkheden op het gebied van MFA, geeft de woordvoerder als voorbeeld.

Les 4: SentinelOne is echt next-gen

Een laatste les die de woordvoerder en de multinational als geheel uit de ervaringen rondom de ransomware-aanval hebben getrokken, is dat SentinelOne niet alleen op papier next-gen is. In de praktijk is dat ook echt zo, geeft de woordvoerder aan. In eerste instantie hadden ze natuurlijk niet zoveel keuze, maar inmiddels is SentinelOne bij alle ondernemingen binnen de multinational uitgerold. Dat ging volledig foutloos en zonder issues in enkele weken tijd. De SentinelOne-agent heeft geen enkele negatieve invloed op het functioneren van applicaties bijvoorbeeld.

Daar komt ook nog eens bij dat het beheer dankzij de SaaS-omgeving van SentinelOne kinderlijk eenvoudig is. Niet alleen omdat hij nu geen on-prem server meer nodig heeft, maar ook omdat hij nu in wezen zelf het beheer voor de hele groep aan ondernemingen zou kunnen doen. Zo eenvoudig is het SentinelOne-platform in de praktijk te gebruiken. Gevraagd naar negatieve punten van SentinelOne moet de woordvoerder dan ook het antwoord schuldig blijven. Hij durft zelfs de stelling wel aan dat ze ondanks de gedateerde omgeving van de getroffen onderneming, de ransomware geen vat zou hebben gekregen op hun omgeving als ze toen al SentinelOne hadden gebruikt.

SentinelOne heeft de multinational niet alleen geholpen bij het herstellen van de aanval. Bovenop bovenstaande voordelen zorgt het gebruik ervan ook voor het drastisch verkleinen van het aanvalsoppervlak voor een volgende aanval. De multinational kon namelijk ook snel met SentinelOne Ranger aan de slag. Die tool scant alles wat er gebeurt op het netwerk en meldt vervolgens welke onbeveiligde endpoints hij ziet. Deze tool gebruikten ze tijdens de crisis regelmatig.

Tot slot is het nog goed om te vermelden dat SentinelOne na het afslaan van de aanval ook nog een uitgebreid rapport opleverde. Dat rapport was bedoeld om zoveel mogelijk inzicht te geven zodat de onderneming er zoveel mogelijk van kon leren. In zo'n rapport staan volgens de woordvoerder adviezen

waar je ook daadwerkelijk iets mee kunt, inclusief een volledig Attack Diagram. Deze after-sales gekoppeld aan de next-gen capaciteiten van het platform en de uitstekende pre-sales (helpen nog voor er een handtekening op papier stond) zijn zonder meer een uitstekend visitekaartje voor SentinelOne. Belangrijker nog is dat de multinational er in de breedste zin van het woord een stuk veiliger op geworden is. En daar gaat het uiteindelijk toch om.