NORTHWAVE
Intelligent Security Operations

Memo security incident Hoppenbrouwers Techniek

Pim Takkenberg
Director Cybersecurity
6 juli 2021

Management summary

Op vrijdag 2 juli 2021 ontdekte Hoppenbrouwers Techniek ongebruikelijke activiteit binnen hun bedrijfsnetwerk. De verschillende verdedigingslinies binnen de IT-omgeving van Hoppenbrouwers Techniek sloegen alarm en begonnen automatisch verdachte activiteiten te blokkeren. Nadere inspectie door het IT-team wees uit dat een indringer toegang had gekregen tot het interne netwerk via de Kaseya supply chain-aanval, waardoor alle machines met de Kaseya-agent geïnstalleerd, werden versleuteld.

Tijdens het eerste onderzoek volgde Hoppenbrouwers Techniek vooraf gedefinieerde procedures, waaronder:

1. De verbinding met internet verbreken en al het inkomende en uitgaande verkeer te blokkeren
2. Het vooraf gedefinieerde beleid uitvoeren om alle systemen af te sluiten

Deze acties hebben de aanval effectief gestopt en verdere impact op de omgeving voorkomen.

Direct nadat deze situatie onder controle was, heeft Hoppenbrouwers Techniek een Computer Emergency Response Team (van Northwave) ingeschakeld om te helpen op een veilige en adequate manier van het incident te herstellen. Tijdens het onderzoek van Northwave werd duidelijk dat Hoppenbrouwers Techniek inderdaad het slachtoffer was van de aanval op de toeleveringsketen van Kaseya. Al het bewijs dat op de systemen of binnen het netwerk is geïdentificeerd, komt overeen met de Kaseya-aanval. Bovendien werden alleen hosts met de geïnstalleerde Kaseya-agent getroffen door de aanval.

Gelukkig beschikte Hoppenbrouwers Techniek over een goede back-up oplossing voor hun servers, waardoor de omgeving snel kon worden hersteld. Northwave onderzocht alle servers voordat ze werden goedgekeurd om weer in productie te gaan. Verder heeft Hoppenbrouwers Techniek de getroffen laptops en computers opnieuw geïnstalleerd om een schone werkplek te garanderen en een nieuw wachtwoord voor alle gebruikers gemaakt. Daarnaast houdt het Security Operations Center (SOC) van Northwave nu de complete omgeving van Hoppenbrouwers Techniek 24*7 nauwlettend in de gaten. Bovendien beschikte Hoppenbrouwers Techniek al over Multi-Factor Authenticatie (MFA) voor alle externe verbindingen. Tot slot heeft Hoppenbrouwers Techniek alle Kaseya software van hun systemen verwijderd en zal deze oplossing niet meer gebruiken in de toekomst.

Als onderdeel van de herstelprocedures heeft Hoppenbrouwers Techniek alle noodzakelijke en aanvullende ondersteunende maatregelen genomen om de IT-infrastructuur en de gegevens daarop te beveiligen. Met deze maatregelen beschouwt Northwave de omgeving van Hoppenbrouwers Techniek als veilig, waarbij alle kwaadwillende activiteiten gerelateerd aan de aanval verwijderd zijn. Bovendien is het, gezien de aard van de geautomatiseerde aanval, hoogst onwaarschijnlijk dat de dreigingsactor toegang heeft gekregen tot het netwerk van Hoppenbrouwers Techniek.

In dit geval was de aanval gericht op endpoints waarop Kaseya was geïnstalleerd, waarvan Hoppenbrouwers Techniek gebruik maakte. De aanval heeft dan ook niet het vermogen om zich te verspreiden naar klanten, leveranciers of andere partners van Hoppenbrouwers Techniek.

Hoppenbrouwers Techniek heeft de Autoriteit Persoonsgegevens formeel op de hoogte gesteld van het probleem. Bovendien communiceren de juridische en privacy teams van Hoppenbrouwers Techniek voortdurend om ervoor te zorgen dat aan alle wettelijke rapportagevereisten wordt voldaan.

Northwave concludeert dat er op basis van de huidige bevindingen van het onderzoek geen data uit de omgeving van Hoppenbrouwers Techniek is geëxfiltreerd.