Managementsamenvatting Security Incident Lochem

Inleiding

Op 6 juni 2019 waren indicaties dat een aanval plaatsvond bij de gemeente Lochem. Vervolgens is uitvoering gegeven aan Incident Response. Naar aanleiding hiervan heeft gemeente Lochem (hierna: opdrachtgever) aan NFIR B.V. (hierna NFIR) verzocht digitaal forensisch onderzoek te verrichten naar de ICT-infrastructuur van opdrachtgever.

Het doel van dit onderzoek is om te achterhalen in hoeverre sprake is van een datalek en welke gegevens dit zijn. Daarnaast is NFIR gevraagd om te achterhalen wat de volledige omvang is van het incident. Op basis van de initiële intake en de doelstelling zijn in overleg met de gemeente de volgende onderzoeksvragen opgesteld:

- Op welke wijze is ongeautoriseerd toegang verkregen tot het geautomatiseerd en/of (net)-werk?
- Tot welke systemen is ongeautoriseerd toegang verkregen?
- Welke handelingen zijn uitgevoerd in het tijdsbestek waarin ongeautoriseerd toegang is verkregen?
- Welke gegevens zijn door ongeautoriseerde personen ingezien, gekopieerd of geëxtraheerd?

Als onderdeel van het onderzoek zijn gegevens op forensische wijze veiliggesteld en is ondersteuning geboden bij (het uitvoeren van aanvullende) mitigerende maatregelen.

Conclusie

Op welke wijze is ongeautoriseerd toegang verkregen tot het geautomatiseerde (net)werk?

Op basis van onderzoek aan de thuiswerkserver (inclusief de daarbij behorende back-ups), Firewall en authenticatieservers is bevonden dat er in totaal tientallen inlogsessies hebben plaatsgevonden, waarbij toegang is verkregen tot de thuiswerkserver middels een RDP-verbinding. RDP staat voor Remote Desktop Protocol, in het Nederlands vaak "Extern bureaublad" genoemd. Dit protocol wordt gebruikt bij het overnemen van een pc van op afstand.

Deze sessies hebben plaatsgevonden middels twee gebruiker accounts gedurende een periode van een half jaar. De RDP-poort is op 14 december 2018 opengezet, waarna de aanvallen hebben plaatsgevonden. De omstandigheden rondom het openzetten van deze poort kan niet meer worden onderzocht door het inmiddels ontbreken van logbestanden.

NFIR heeft verder vastgesteld dat miljoenen verbindingen afkomstig van duizenden unieke IP-adressen zijn vastgelegd door de firewall, waarbij poort 3389 op de thuiswerkserver is benaderd. Deze poort is de standaard toegangspoort van RDP.

Door loginformatie te correleren heeft NFIR meerdere unieke IP-adressen gevonden welke te koppelen zijn aan bepaalde inlogacties. Diverse IP-adressen zijn op het internet bekend om het uitvoeren van brute-force aanvallen. Bij een brute-force aanval worden vaak in korte tijd meerdere gebruikersnamen en wachtwoordcombinaties geprobeerd om ongeautoriseerd toegang te (kunnen) verkrijgen.

Tot welke systemen is ongeautoriseerd toegang verkregen?

Naar aanleiding van onderzoek aan de Firewall, authenticatieservers en de systemen zelf is vastgesteld dat extern toegang tot een systeem voor thuiswerken en tot een testcomputer zijn verkregen. De toegang heeft meermaals plaatsgevonden over een periode van een half jaar. Op basis van de gebruikte accounts en IP-adressen zijn geen legitieme verklaringen gevonden voor de inlogacties door de gemeente en worden derhalve gezien als ongeautoriseerd.

Welke handelingen zijn uitgevoerd in het tijdsbestek waarin ongeautoriseerd toegang is verkregen?

Over de gehele periode zijn applicaties gebruikt die voornamelijk gericht zijn op het verkrijgen van informatie over het netwerk en de gebruikers. Daarnaast zijn twee programma's gestart die kenmerken hebben van Ransomware. Tevens is een derde applicatie op het systeem geplaatst, die zeer waarschijnlijk ook Ransomware betreft. Ransomware is malware die een computer en/of gegevens die erop staan blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden' middels een tegen betaling verstrekte code.

Een van de applicaties heeft daadwerkelijk een aantal bestanden versleuteld en op meerdere plaatsen een zogenoemde 'ransomnote' opgeslagen. Dit is een brief waarin gevraagd wordt om een transactie uit te voeren met de belofte dat na de transactie toegang tot de gegevens weer mogelijk zal zijn.

Tot slot is ook laterale beweging waargenomen van het thuiswerksysteem naar de testcomputer. Binnen deze sessie geen sporen aangetroffen dat de aanvaller actief handelingen heeft uitgevoerd.

Welke gegevens zijn door ongeautoriseerden ingezien, gekopieerd of geëxtraheerd?

Op basis van de onderzochte sporen, kan niet met volledige zekerheid worden gezegd welke gegevens zijn ingezien, gekopieerd of geëxtraheerd.

Waarschijnlijk is de inhoud van de "Active Directory" gekopieerd en is deze kopie geëxtraheerd. Wel kan met redelijke zekerheid worden gezegd dat deze kopie gegevens over het netwerk, waaronder gebruikersnamen en emailadressen van medewerkers van de gemeente Lochem, bevatten. Daarnaast zijn er tevens hashwaardes van wachtwoorden opgenomen in deze kopie. Een 'hashwaarde' is een berekening over gegevens en wordt onder andere gebruikt om wachtwoorden geanonimiseerd op te slaan.

Er zijn geen aanwijzingen waargenomen dat andere bestanden met persoonsgegevens zijn benaderd.