Door het oog van de naald

Analyse van het beveiligingsincident in Lochem

Datum: 3 september 2019

Status: DEFINITIEF

TLP: WHITE

Zaaknummer: 20190045

Over dit document

Dit document beschrijft de gebeurtenissen rondom de hack op de gemeente Lochem die op 6 juni 2019 aan het licht kwam. Het bevat zoveel mogelijk informatie van de vertrouwelijke onderzoeken om lering te kunnen trekken uit het incident.

Openbaarheid

In de informatiebeveiliging wordt gewerkt met het Traffic Light Protocol (TLP). Dit zijn internationale afspraken over de vertrouwelijkheid van documenten. *White* (wit) staat voor openbare informatie, *amber* (oranje) mag binnen de organisatie worden verspreid voor hen die het nodig hebben (*need to know*) en *red* (rood) is zeer vertrouwelijk (*for your eyes only*).

De status van dit rapport is TLP WHITE.

Er is een aanvullend gedeelte dat is geclassificeerd als TLP AMBER voor de stakeholders op een ‘need to know’-basis. De inhoud is gevoelig, omdat deze in verkeerde handen schadelijk kan zijn voor lopende onderzoeken.

Het beveiligingsincident

Verloop van het incident

Op donderdagmiddag 6 juni 2019 ontving de gemeente Lochem een melding dat er internetverkeer gaande was op een wijze die niet gebruikelijk is. De melder wist dat het om Lochem ging als verzender van het ongebruikelijke internetverkeer, omdat het desbetreffende IP-adres via open bronnen naar die gemeente was terug te voeren.

De gemeente Lochem heeft vervolgens over de betreffende melding contact gehad met de Informatiebeveiligingsdienst voor gemeenten (IBD). Het Nationaal Cyber Security Centrum (NCSC) heeft de IBD vervolgens op verzoek ondersteund in de uitvoering van haar taken. Gedurende de avond en nacht werd duidelijk dat er daadwerkelijk onbevoegde toegang tot de gemeentelijke systemen was geweest.

In de loop van de nacht verrichtten de Nationale Politie en het NCSC hun werkzaamheden en vertrokken daarna van de locatie.

Naar aanleiding van de melding en het bezoek van de Nationale Politie en het NCSC, heeft de gemeente Lochem besloten om IT-beveiligingsbedrijf NFIR B.V. te vragen voorbereidingen te treffen om op vrijdag 7 juni 2019 het incident te onderzoeken.

Op 7 juni 2019 is een crisisteam opgezet, waarbij is besloten tot het houden van een breed forensisch onderzoek, proactief te communiceren over het incident naar de samenleving en proactief om te gaan met de situatie. Het doel hierbij was om zoveel mogelijk en zo breed mogelijk lering te trekken uit het incident.

Het pinksterweekend is besteed door dag en nacht van alle relevante systemen een forensische kopie te maken. Tegelijkertijd werd op de veiliggestelde informatie onderzoek gedaan, om mogelijk meer relevante systemen te vinden en deze veilig te kunnen stellen. Dit is door de grote omgeving die gemeentelijke systemen zijn een zeer arbeidsintensieve taak. Uiteindelijk zijn deze werkzaamheden op 18 juni 2019 afgerond. Ondertussen is direct besloten om actief het interne netwerk en de internetverbinding intensief te monitoren om verdere aanvallen te detecteren en in zo’n geval onrechtmatige toegang, wijzigingen, of verwijdering te detecteren. Dit heeft geen meldingen opgeleverd.

Op 12 juni ontstond het vermoeden dat de aanvallers een kopie hadden gemaakt van een database met gegevens van medewerkers van de gemeente Lochem, waarbij informatie als e-mailadressen en gebruikersnamen zijn gekopieerd. Uit het forensisch onderzoek bleek niet uitgesloten te kunnen worden dat de aanvallers gebruikmaakten van een zogenoemde ‘golden ticket’ en hiermee beheerdersrechten zouden kunnen krijgen.

Hierop is door het crisisteam en de burgemeester besloten om de internetverbinding met de buitenwereld tijdelijk te onderbreken en het gehele toegangssysteem stil te leggen en opnieuw in te richten. Als de aanvaller daadwerkelijk beheerdersrechten zou hebben, konden deze niet meer worden ingezet. Deze actie had de hoogste prioriteit. Het gevolg van deze stap was merkbaar voor de gemeente: alle systemen werden daardoor ontoegankelijk. Om die reden is besloten de gemeentelijke dienstverlening die afhankelijk is van ICT op 13 juni 2019 te staken.

De operatie is in de avond van de 12de juni gestart en is ‘s nachts doorgegaan.

Met het inrichten van een nieuwe authenticatieserver, de computer die de aanmeldingen regelt, zijn ook alle overige IT-systemen beoordeeld om te bepalen of deze geschikt zijn om weer operationeel te laten worden. Hierbij is voorrang gegeven aan de systemen die de primaire processen van de gemeente ondersteunen richting de burger.

Hierdoor werd het op 14 juni alweer mogelijk de inwoners en ondernemers te bedienen. Binnen de organisatie waren toen nog niet alle systemen operationeel. Stap voor stap zijn ook deze systemen weer beschikbaar gekomen. Door deze aanpak werd de externe en interne dienstverlening van de gemeente Lochem weer beheerst beschikbaar.

De aanval

De beheerders kunnen niet verklaren waarom het RDP-protocol aanstaat en vermoeden dat dit niet door hen is aangezet. Maar uit bewijs blijkt ook niet dat deze dienst is geïnstalleerd door de aanvallers.

Gedurende de eerder genoemde periode hebben de aanvallers telkens geprobeerd iets verder te komen. Bij deze pogingen is uiteindelijk toegang verkregen tot de inlogdiensten. Op meerdere plaatsen zijn door de forensisch onderzoekers berichten van de aanvaller(s) aangetroffen, waarin geld wordt geëist. Daarnaast zijn meerdere soorten malware op systemen gezet. Er zijn diverse pogingen gedaan deze malware te activeren, maar deze waren niet succesvol. Op het moment dat de aanvallers dit deden, hadden ze niet voldoende rechten. In andere gevallen heeft de antivirussoftware de malware direct gestopt toen deze actief werd.

Het doel van de aanvallers is hiermee duidelijk geworden: het gijzelen van gegevens in ruil voor geld, ook wel bekend als ransomware[1]. Er zijn losgeldberichten achtergelaten. Er zijn enkele bestanden versleuteld, maar dat betreft geen persoonsgegevens. De versleutelde bestanden blijken niets operationeels te betreffen en verder komen ze niet.

Door het oog van de naald

Het is belangrijk om te beseffen dat de aanval net niet ver genoeg is gekomen om tot daadwerkelijk het gijzeling van relevante data te komen. Was dat wel gelukt, dan waren alle administratieve systemen of een groot deel daarvan niet meer toegankelijk geweest voor de gemeente Lochem. Het geduldig en doelgericht te werk gaan, is zeer alarmerend. Normaliter worden dit soort aanvallen snel uitgevoerd als een soort ‘*hit and run’*. Juist het feit dat zij rustig hun doel probeerden te bereiken, maakt duidelijk dat de aanvallers van plan waren een grotere slag te slaan. Er zijn andere gevallen bekend waar ook informatie op de back-ups niet meer bruikbaar is. In sommige zaken worden dan tonnen losgeld betaald. Recentelijk heeft het Amerikaanse Riviera Beach in de Staat Florida een bedrag van 600.000 dollar (bijna 537.000 euro) betaald. Dit bedrag was een onderhandelingsresultaat bereikt door de verzekeraar. Belangrijk is te beseffen dat deze stad ongeveer evenveel inwoners heeft als Lochem. Het Amerikaanse Lake City betaalde 460.000 dollar, terwijl Jackson County 400.000 dollar betaalde om bestanden terug te krijgen. De gemeente Lochem is duidelijk door het oog van de naald gekropen.

1 https://nl.wikipedia.org/wiki/Ransomware

Daarnaast is het belangrijk te beseffen dat de gemeente opereert in een keten met andere organisaties. In het geval dat de aanval specifieker en doelgerichter was geweest, zou een gemeente als springplank naar andere organisaties kunnen fungeren.

Samenwerking

Bij het incident is zeer constructief samengewerkt. De communicatie blijft gedurende de weken erna onderling intensief, gedetailleerd en open. Hierdoor is er coördinatie geweest. Dat heeft veel onnodig werk bespaard en geholpen om sneller de vinger achter problematieken te krijgen. Het is niet ongebruikelijk dat men in reactie op een incident binnen een organisatie met man en macht probeert te voorkomen dat iemand de ‘schuld in de schoenen geschoven’ krijgt. Al voor aankomst van de Nationale Politie, NCSC en IBD is met de burgemeester besloten niet te richten op schuld, maar op het vinden van fouten en die op te lossen. Alle inspanning is gericht op proactief handelen en op zoveel mogelijk leerpunten en verbeterpunten. De houding is er een geweest van berusting in het feitencomplex en een drang de problemen efficiënt op te lossen.

Binnen het crisisteam hebben geen competentieconflicten gespeeld. De goede en proactieve communicatie onderling heeft ervoor gezorgd dat sommige werkzaamheden – zoals regie en communicatie – op afstand plaats konden vinden. Dat heeft tijd en kosten bespaard.

Vooral de IT-afdeling verdient lof voor de enorme inzet die zij heeft getoond in het verhelpen van het probleem. Dit heeft bijgedragen aan een vlot herstel naar een operationele situatie en het doorvoeren van tientallen verbeteringen. Ook de communicatieafdeling heeft een enorme inzet getoond. De inzet van alle mensen (nadrukkelijk ook de forensisch onderzoekers) was zo groot dat het meerdere malen noodzakelijk was om mensen te gebieden verplicht te gaan slapen.

De burgemeester heeft direct besloten zo open mogelijk te communiceren en Lochem te gebruiken als een les voor iedereen. Op sociale media werd deze houding gewaardeerd. De prettige samenwerking werd publiekelijk vanuit de Nationaal Coördinator Terrorismebestrijding en Veiligheid geroemd.

Onderzoeken

Forensisch onderzoek

Het uitvoeren van forensisch onderzoek is belangrijk om de feitelijke waarheid boven tafel te krijgen, de vraag te kunnen beantwoorden hoe de aanval mogelijk tot stand kwam en vooral welke lering we hieruit kunnen trekken.

Het mag duidelijk zijn dat een aanval als deze niet op zichzelf staat. Door in te breken, te wachten en weer een stap verder te gaan, is duidelijk dat we te maken hebben met een actor die dit mogelijk vaker doet.

De politie is niet onbekend met het verschijnsel. Een grondig onderzoek, zoals nu in Lochem is uitgevoerd, voegt veel nieuwe informatie over de handelswijze van de dader(s) toe. Die informatie is niet alleen in het eigen onderzoek belangrijk, maar kan ook meerwaarde bieden in andere lopende onderzoeken. De pakkans van de dader(s) wordt daarmee vergroot. De Nationale Politie en het Openbaar Ministerie hebben in de richting van de burgemeester gemeld dat de investering van grote waarde is en dat het onderzoek veel waarde toevoegt.

Tijdens het forensisch onderzoek is duidelijk geworden dat er op een aantal punten in Lochem aanvullende beveiliging nodig is.

Het gevaar van het niet kennen van alle IT-componenten is dat updates op software en hardware niet tijdig geïnstalleerd worden en dat de IT-componenten daarmee een springplank kunnen vormen voor aanvallers (patchmanagement). Een ander probleem van het niet kennen van alle componenten is dat er onbedoeld meer functionaliteit beschikbaar is of aangeboden wordt aan gebruikers van de systemen (hardening). Door uit te zetten wat niet nodig is (RDP), kunnen aanvallers het ook niet misbruiken (hardening). En als het aanstaat, kan een goed updatebeleid ervoor zorgen dat zwakheden worden wegnomen door nieuwe updates (patchmanagement). Dit zijn veelvoorkomende fouten bij veel organisaties. Om deze reden is de IBD momenteel een landelijk traject gestart om bij alle gemeenten het inzicht in computersystemen (configuratiemanagement) zo accuraat en hoog mogelijk te krijgen. Dit ter verhoging van de digitale weerbaarheid.

Verder is een inventarisatie gemaakt van de hele technische omgeving in een uitgebreide penetratietest en netwerkscan. Tijdens het incident heeft NFIR diverse technische beveiligingsadviezen gegeven, welke zoveel als mogelijk direct door de IT-beheerders zijn opgevolgd. Tijdens de opschoonactie zijn de nodige verbeteringen doorgevoerd.

Penetratietest

Op verzoek van de burgemeester is aan beveiligingsbedrijf NFIR gevraagd een uitgebreide penetratietest uit te voeren. Bij een dergelijk onderzoek wordt gekeken naar de weerbaarheid van de digitale infrastructuur en worden zwakheden in systemen en technische beveiligingsproblemen in kaart gebracht. Een dergelijke actie is van groot belang om proactief te voorkomen dat nieuwe zwakheden opnieuw tot een hack kunnen leiden. Door deze te onderzoeken wordt de kans op een herhaling van een dergelijke aanval kleiner.

Uit de test zijn diverse bevindingen gekomen, welke inmiddels deels zijn opgelost. Voor een deel vragen bevindingen meer tijd, omdat sommige verbetervoorstellen meer tijd nodig hebben om gerealiseerd te kunnen worden. Zowel de burgemeester als de IT-afdeling hebben aangegeven alle aanbevelingen die gaan over de gemeente te willen realiseren.

Er zijn echter ook bevindingen welke niet door de gemeente kunnen worden opgelost, omdat er afhankelijkheden bij leveranciers zijn. Zo blijken er standaardwachtwoorden in producten te zitten, die niet zomaar zijn aan te passen. Deze en andere punten vragen bereidwilligheid van de leveranciers. Dit laatste is opmerkelijk, omdat dit betekent dat veel meer klanten zwakheden hebben die universeel zijn. Er is reeds overleg met diverse leveranciers om deze problemen te verhelpen.

Eigen observaties en gesprekken

In het kader van het incident hebben tientallen gesprekken plaatsgevonden met betrokkenen over operationele zaken en de status quo. Uit deze gesprekken worden een aantal organisatorische zaken helder. De gemeente Lochem heeft op het moment van schrijven zo’n 34.000 inwoners met bijbehorend budget. Daarvoor moet een volwaardige gemeentelijke ICT-omgeving worden geboden. Daardoor rusten er op de schouders van een beperkt aantal ICT’ers veel taken.

Deze druk is waarneembaar in de organisatie. De coördinator ICT is tevens de Chief Information Security Officer (CISO). Daardoor ontstaat een conflict tussen operationele taken en

beveiligingstaken. Waar gescheiden functies medewerkers de verschillende belangen tegenover elkaar kunnen zetten en erover debatteren, is dat hier niet mogelijk. Daarnaast wordt van de CISO verwacht dat hij ook de leiding neemt in het doen van een melding bij de Autoriteit Persoonsgegevens.

Hoge werkdruk op de ICT-afdeling is een constante factor, waardoor de ICT'ers onvoldoende tijd hebben zich te blijven ontwikkelen en verdiepen in hun vak. Precies deze spanning van het overleven is een factor in het maken van fouten of het missen van nieuwe inzichten met betrekking tot beveiliging.

Het beveiligingsincident trekt een enorme wissel op de gemeente Lochem. Want al is de gemeente klein in aantal inwoners, de financiële impact van een inbraak als deze is niet kleiner dan wanneer dit bij een middelgrote of grote gemeente was gebeurd. Er is hierdoor een onvoorzien gat in de begroting geslagen. Terecht heeft de burgemeester dan ook de vraag opgeworpen of – net als bij niet-digitale rampen – hier ondersteuning op zijn plaats is. Komt dergelijke ondersteuning er niet, dan is het niet onwaarschijnlijk dat een vergelijkbaar incident in een andere gemeente niet goed wordt uitgezocht. Juist het goed uitzoeken leidt tot aanbevelingen om herhaling te voorkomen.

Lessen uit Lochem

Er vallen uit het incident in Lochem de nodige lessen te trekken. Leren van incidenten helpt bij de weerbaarheid en verkleint de kans op herhaling.

Voor andere organisaties

1. Lochem is weliswaar een kleine gemeente, maar interessant voor een gerichte aanval als de kans zich aandient. Bij succes hadden de aanvallers de volledige dienstverlening kunnen platleggen. Uit de Amerikaanse voorbeelden wordt duidelijk dat met het gijzelen van overheidsinformatie tonnen aan losgeld binnen te halen zijn. Riviera Beach in Florida is qua aantal inwoners vergelijkbaar met Lochem. De bedragen waar dit soort aanvallen over gaan, lonen om gedurende langere tijd, geld en energie in te steken. Als je maar bij genoeg organisaties probeert aan te vallen, raak je vanzelf de jackpot. Denk daarom niet dat het jouw organisatie niet zal overkomen, want veel organisaties hebben waardevolle data om te gijzelen.
2. Bij gerichte aanvallen van dit kaliber zullen aanvallers er niet voor terugdeinzen om de back-up van een organisatie te vernietigen. Daarmee wordt de druk om te betalen groter. Maar zelfs als de back-ups er wel zijn, dan is het voor sommige organisaties toch aantrekkelijk om te betalen, omdat het herstel van systemen dan fors sneller is. Die simpele wetenschap noopt tot het kritisch kijken naar hoe herstel vanaf de eigen back-upsystemen werkt en of dat voldoet aan de wensen. Zorg voor goede, off-site back-ups.
3. In Lochem is veel complexiteit bij het incident uitgebannen, omdat tijdens het incident een goede cultuur heerst: geen geheimzinnigheid, geen verwijten, maar accepteren dat het incident nu de realiteit is. Hierdoor zijn onderzoek en systeemherstel eenvoudiger. Een 'alles boven tafel'-cultuur helpt bij het zoeken naar onderliggende problemen.

4. Probeer waar mogelijk meerfactorauthenticatie in te voeren. Bij een dergelijke authenticatie worden naast gebruikersnaam en wachtwoord ook een andere vorm van inloggen op hetzelfde systeem gebruikt. Denk daarbij bijvoorbeeld aan een SMS-code, een pasje of andere vorm van aanmelden. Dit type aanval had niet op deze manier uitgevoerd kunnen worden als de gemeente gebruikgemaakt had van meerfactorauthenticatie voor alle accounts.
5. Breng zoveel mogelijk alle systemen en software in kaart. Hou dit goed bij. Specifiek voor gemeenten: maak gebruik van de mogelijkheid van IBD om systemen te laten inventariseren.
6. Werk systemen goed bij. Zorg voor hardening (het configureren voor veilige systemen). De aanvallers waren niet op deze manier verder gekomen als dat overal was gebeurd.
7. Zorg dat er een stappenplan of crisisplan is dat bij incidenten beschikbaar is. Bedenk dat dit altijd toegankelijk is, ook als bestanden versleuteld zijn. Besef verder dat reguliere infrastructuur, zoals e-mail, door een incident wel eens niet beschikbaar kan zijn. Bij het bestrijden van de crisis is het belangrijk om alle stappen goed te documenteren: observaties, stappen die gezet zijn, gegeven adviezen en opdrachten. Het reconstrueren van vooral de eerste uren van het incident is door een gebrek aan documentatie tijdrovend gebleken.

Voor leveranciers van ICT-oplossingen

Stop met het gebruik van standaardwachtwoorden, communiceer helder met de klanten waar beveiliging van geleverde diensten en producten uit bestaat en zorg ervoor dat systemen met standaardwachtwoorden kunnen worden aangepast. Probeer deze situatie zo snel mogelijk te beëindigen.

Voor Lochem

1. Een belangrijke oorzaak van het maken van fouten is de werkdruk en het gebrek aan reflectie op de eigen omgeving. Er zal niet direct budget voor meer formatieplaatsen zijn. Het is wel realistisch na te denken over betere ondersteuning van de ICT-medewerkers door bijvoorbeeld de volgende stappen te nemen:
    1. Geef meer ruimte voor opleiding en verdieping. Zo blijven medewerkers up-to-date en kunnen ze effectiever werken. Dat kan onder meer door tijdens een training ondersteuning te regelen bij andere gemeenten of de tijdelijke inhuur van personeel.
    2. Beleg de CISO-rol anders, waardoor deze niet zo conflicteert met IT-coördinatie. Dat zou bijvoorbeeld kunnen door een externe CISO aan te trekken voor een afgesproken aantal uur of een CISO met een of meerdere andere gemeenten te delen. Een andere optie is om de huidige CISO te ondersteunen met een sparringpartner. Op dit moment ontbreekt positief kritische tegenspraak. Een andere mogelijkheid is om een kring van gemeentelijke CISO’s op te zetten om ervaringen uit te wisselen of geplande besluiten te spiegelen en uitgewerkte producten en aanpakken te delen. Zo maak je de medewerkers effectiever en hoeft niet steeds het wiel opnieuw uitgevonden te worden. Laat de CISO daarnaast gebruikmaken van de IBD. De IBD is onafhankelijk opgericht voor alle gemeenten en heeft geen verborgen agenda.

3. Reserveer een vast budget voor informatiebeveiliging als percentage van de ICT-uitgaven en breng de CISO in positie als eerste adviseur op het gebied van risicomanagement rondom de informatievoorziening. Zet informatiebeveiliging op de bestuurlijke agenda en maak risicomanagement een vast onderdeel van de bestuurstafel.
4. Het melden van een datalek wordt nu gezien als onderdeel van het technisch incident. De privacykant van een incident gaat nauwelijks over techniek. Veel belangrijker zijn de procesmatige kant die heeft geleid tot een incident en de wettelijke verplichtingen. De tijd van de CISO wordt al opgeslokt door de operationele zaken. De meldplicht en de aspecten die daarbij komen kijken, zouden logischerwijs dan beter door een andere persoon kunnen worden opgepakt.

2. Bij de penetratietest zijn 64 bevindingen aan het licht gekomen. De urgente bevindingen zijn inmiddels verholpen. Er zijn een aantal bevindingen die meer fundamentele aanpassingen vereisen. Het is heel belangrijk dat deze worden opgevolgd. Het is niet meteen duidelijk of daar financiële consequenties zijn.
3. De IBD treft de voorbereidingen om gemeenten technisch in kaart te brengen. Dat is de eerste stap naar een Security Operations Center, waardoor het mogelijk is om bij aanvallen sneller alarm te slaan en de juiste stappen te zetten. Het verdient aanbeveling dat de gemeente Lochem van deze en andere dienstverlening van de IBD maximaal gebruikmaakt. Zo voorkom je dat mensen zelf het wiel moeten uitvinden.
4. De lange periode waarbinnen het incident afspeelde had daarnaast nog verkort kunnen worden door een aantal andere maatregelen. Zoals al eerder beschreven aan de voorkant (preventie) zijn maatregelen niet goed geïmplementeerd en daaropvolgend had ook aan de detectiekant iets gedaan moeten worden. De goedkoopste maatregel is voorkomen dat het gebeurt. Daarop volgend is het waarnemen dat het gebeurt en de duurste maatregel is het oplossen als het is gebeurd. Nadat de inbraak succesvol uitgevoerd was, had een gemanagede (je moet er wel naar kijken) detectieoplossing er mogelijk voor kunnen zorgen dat de aanvallers eerder opgemerkt waren in plaats van pas na maanden in een extern onderzoek.
5. Beveiliging is nooit af. Maak een speerpunt van het voldoen aan de Baseline Informatiebeveiliging Overheid die dit jaar beschikbaar is gekomen en volgend jaar de norm is. Maak een concreet plan om stap voor stap hieraan te gaan voldoen.
6. De algemene opmerking over meerfactorauthenticatie geldt nadrukkelijk ook voor de gemeente Lochem: gebruik het waar het maar mogelijk is.

Voor de gemeenteraad

1. Zorg ervoor dat er een politiek klimaat is en blijft, waarin het loont om te investeren in informatiebeveiliging. Dit kan concreet door met het College van Burgemeester en Wethouders samen te kijken naar haalbare stappen om de beveiliging blijvend te verbeteren en daarop te controleren. Creëer politiek en financieel ruimte om dat mogelijk maken, bij voorkeur als vast budget van de ICT-uitgaven.

2. Koester de ‘alles boven tafel’-cultuur. Door niet te vervallen in verwijten, worden ook geen pogingen ondernomen het incident weg te moffelen.

Vragen over het incident

De hack roept een aantal begrijpelijke vragen op, die de afgelopen weken gesteld zijn binnen de gemeente, de gemeenteraad en externe partijen. Deze worden hier zo goed mogelijk beantwoord.

Zijn er persoonsgegevens van inwoners gelekt?

Uit het forensisch onderzoek blijkt niet dat er persoonsgegevens van inwoners zijn gelekt, ingezien, gewijzigd of vernietigd. Uit het logboek is voldoende vast te stellen dat dit niet met de aanval heeft gespeeld. De aanval is gestopt op het moment dat de aanvallers probeerden bestanden te gijzelen. Er zijn bestanden versleuteld, maar deze waren niet operationeel relevant en de schade was simpel te herstellen. Was de aanval wel gelukt, dan waren persoonsgegevens zeer waarschijnlijk wel geraakt.

Is dit een datalek?

Ja, dit is een datalek. De aanvallers hebben toegang gekregen tot de databank met gebruikersnamen, namen en e-mailadressen van medewerkers. Daarmee konden ze waarschijnlijk nog niet verder komen. Maar het simpele feit dat een inlognaam of een naam van een gemeentemedewerker toegankelijk is geweest, maakt dit een datalek. Dat lek is dan ook gemeld aan de Autoriteit Persoonsgegevens.

Hoe kwam de hack aan het licht?

De gemeente Lochem ontving een melding dat er internetverkeer gaande was op een wijze die niet gebruikelijk is. De melder wist dat het om Lochem ging als verzender van het ongebruikelijke internetverkeer, omdat het desbetreffende IP-adres via open bronnen naar die gemeente was terug te voeren. Hierop is direct alarm geslagen en een onderzoek gestart. Daarbij zijn de Nationale Politie, het Nationaal Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst voor Gemeenten (IBD) van VNG Realisatie, De Winter Information Solutions en NFIR betrokken.

Is dit een malware- of ransomware-uitbraak?

Nee, op de valreep is dat voorkomen. De aanval en de feiten uit het forensisch onderzoek wijzen erop dat het doel is om bestanden te versleutelen en losgeld te eisen. Er is malware aangetroffen en er zijn bestanden versleuteld. Maar de aanval is niet met succes gelanceerd op een manier dat gevoelige gegevens zijn gegijzeld. Was dat wel gelukt, dan blijkt uit andere internationale voorbeelden dat er soms tonnen losgeld worden geëist. Vaak is de situatie dan zo beroerd dat er betaald had moeten worden. Daarom is deze aanval daadwerkelijk een geval van ‘door het oog van de naald’.

Waarom de gemeente Lochem?

Uit niets blijkt dat Lochem als gemeente is geselecteerd ‘omdat het Lochem is’. Ook uit het losgeldbericht is niet gebleken dat er heel bewust op Lochem is gericht. Het lijkt er sterk op dat gebruik is gemaakt van een zwakheid in systemen. Eenmaal binnen is geprobeerd verder te gaan en is maatwerk geleverd.

Het feit dat Lochem een willekeurig slachtoffer is geworden, betekent niet dat er daarna niet doelgericht is gewerkt. Juist dit is een zorgelijk signaal, omdat een ogenschijnlijk weinig spannende gemeente opeens toch het onderwerp van een zeer gerichte aanval kan worden.

Waarom detecteerde Lochem de aanval niet eerder?

De aanval is uitgevoerd door in te breken via het extern bureaublad (RDP). Daarbij is gebruikgemaakt van een gebruikersnaam en wachtwoord die ongelukkig gekozen zijn. Als iemand deze achterhaalt en er vervolgens mee inlogt, dan lijkt voor computers alles normaal. Door heel geduldig te zijn en niet zeer agressief aan te vallen, zijn de sporen subtiel. De sporen in de virusscanner die aanvallen met malware hebben gestopt, zijn niet heel uitzonderlijk. Er wordt regelmatig malware gestopt door een virusscanner.

De subtiele signalen zijn lastig met elkaar in verband te brengen, wanneer iemand hierin niet gespecialiseerd is. Dat bij een organisatie met de omvang van Lochem dit niet onderkend is, is niet uitzonderlijk.

Er werd in juni gezegd dat er 32 Mb aan data is gestolen. Wat is dat?

De 32 Mb aan dataverkeer viel op in het onderzoek als netwerkverkeer. Dat is vervolgens gemeld in het interview met Omroep Gelderland. Wat er in het netwerk omgaat, wordt niet tot in detail vastgelegd. Dat zou erg veel opslag vragen. Veel verkeer gaat versleuteld over het netwerk, waardoor het niet mogelijk is te weten wat er in het verkeer zit zonder de versleuteling ongedaan te maken. In theorie zou het om verschillende zaken kunnen gaan zoals sessies van de aanvaller(s), het ophalen van de lijst van gebruikers of iets anders. Het is niet mogelijk nog te achterhalen waar dit om gaat.

Zijn er fouten gemaakt?

Fouten maken is menselijk en zeker in gemeentelijke omgevingen is de complexiteit van systemen groot. In de gemeente Lochem is dat niet anders. Er zijn meerdere verbeterpunten gevonden, die in dit rapport in algemene bewoordingen zijn benoemd. Opmerkelijk is hier wel dat de burgemeester zich betrokken toont bij informatiebeveiliging en zelf hamert op het belang. De gemeenteraad heeft duidelijk in het verleden het onderwerp informatiebeveiliging besproken. Er is politieke aandacht en dat helpt bij beveiliging.

Zoals bij ieder incident zijn er fouten gemaakt. Dat gaat bijvoorbeeld om fouten in complexe configuraties, een update die niet bleek te zijn uitgevoerd en het gebruik van standaardwachtwoorden. Sommige van die fouten zijn te herleiden naar leveranciers en sommige naar medewerkers. Soms is het echter niet te achterhalen waar de fout is ontstaan. Het is ook belangrijk de aanbeveling uit dit rapport te volgen om het aantal problemen te blijven te verminderen.

De aanval als geheel is niet naar een enkele fout te herleiden. Het is een ongelukkige samenloop van omstandigheden in combinatie met een aanvaller die met veel geduld en doorzettingsvermogen aan de slag ging om de aanval uit te voeren.

Laat dit een waarschuwing voor andere organisaties en overheidsinstellingen zijn om te beseffen dat deze situatie niet uniek is. Dat Lochem is getroffen, lijkt tot op zekere hoogte een toevalstreffer.

Maar de situatie in Lochem is niet afwijkend van andere gemeenten. Ik wijs in dit kader nadrukkelijk op diverse gemeenten waar de lokale rekenkamers zich kritisch hebben geuit.

Is de oorzaak een menselijke fout?

Er is zeker sprake van menselijk falen bij dit incident. Dat zit bijvoorbeeld in een te vrij digitaal toegangsbeleid. Aan de andere kant schort het op dit moment aan de juiste middelen om een aanval te kunnen detecteren. Dit is een klassiek geval waar de ongunstige factoren op de verkeerde manier bij elkaar komen en deze situatie mogelijk maken.

Bijkomend probleem is dat in een aantal systemen problematieken aanwezig zijn. Zo is bijvoorbeeld uit de penetratietest gebleken dat er leveranciers zijn die werken met standaardwachtwoorden. In sommige gevallen heeft de klant (in dit geval de gemeente Lochem) daar geen weet van. Zonder die kennis weet de gemeente niet dat zij kwetsbaar is. Dit belang overstijgt het belang van de gemeente en gaat over veel meer gemeenten. Daarom zal energie worden gestoken in het overtuigen van leveranciers om deze praktijken te verbeteren en beveiliging meer tot speerpunt te maken.

Is dit een ethische hack?

Er is absoluut geen sprake van een ethische hack. Er is geen misstand aangetoond, noch de kans geboden om verbeteringen door te voeren of aangestuurd op verbetering. Bij de aanval is energie gestoken in het verbergen van de aanval. Op systemen zijn losgeldberichten aangetroffen. Het motief lijkt economisch gemotiveerd te zijn. Van enige ethiek om de beveiliging te verbeteren is dan ook niets gebleken.

Is de problematiek in Lochem uniek?

Nee. De problematieken in Lochem zijn veelvoorkomend in de ICT-industrie, bij gemeenten, overheden en veel bedrijven. Dat maakt deze organisaties kwetsbaar voor ‘maatwerk’-aanvallen die met voldoende geduld worden uitgevoerd. Het loont daarom te investeren in beveiliging. De ervaring leert dat de kwaadwillende(n) dan uitwijken naar organisaties die een eenvoudiger doelwit zijn.

Hoe is de situatie in Lochem nu?

Er is veel verbeterd sinds het incident. Veel systemen zijn fors beter beveiligd. De kans op een nieuw incident is daarom kleiner. Wel heeft Lochem nog een lang traject te gaan om het ICT-niveau zover te krijgen dat informatiebeveiliging uitmuntend te noemen is. Dat vraagt niet alleen inzet van de kant van de gemeente. Ook leveranciers zullen aan de slag moeten om de kwaliteit van hun producten te verbeteren. Daarvan is de gemeente immers afhankelijk.

Momenteel zou eenzelfde aanval niet meer mogelijk zijn. Dat is echter geen situatie om in te berusten. Er zal energie moeten worden gestoken in het wegwerken van alle zwakheden die zijn gevonden en het maken van een kwalitatieve verbeterslag. Belangrijk is te beseffen dat na grondige onderzoeken er geen kritieke zwakheden bekend zijn die tot een nieuwe, vergelijkbare aanval kunnen leiden.

De opschoonactie zou bewijs hebben vernietigd. Klopt dat?

Nee, dat is pertinent onjuist. Op 13 juni 2019 heeft de gemeente Lochem – zoals beschreven – de dienstverlening aan de burgers op het gemeentehuis gestaakt. Na de communicatie hierover is door *Tubantia* geschreven:

De gemeente is een onderzoek begonnen naar de computeraanval en is meteen begonnen op gaan schonen om zo snel mogelijk weer aan het werk te kunnen. Volgens ethisch hacker Sijmen Ruwhof betekent dat wel dat niet meer te achterhalen is wie de hack heeft uitgevoerd. "Als je het systeem opschoont, zijn de vingerafdrukken ook weg."

Dit verhaal van *Tubantia* is niet in overeenstemming met de feitelijke gang van zaken. Toen de hack op 6 juni 2019 in de avond werd ontdekt, zijn de Nationale Politie, het Nationaal Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD) ter plaatse geweest om direct relevant bewijs veilig te stellen, de systeembeheerders te voorzien van informatie en de eerste stappen in deze crisis te zetten.

Om iedere partij de ruimte te bieden, is het digitaal forensisch onderzoeksbedrijf NFIR diezelfde avond benaderd. Bij hen is het voorlopige verzoek neergelegd voorbereidingen te treffen om de volgende dag een groot onderzoek te starten naar alle betrokken systemen. Op 7 juni 2019 is het formele verzoek gedaan en zijn de werkzaamheden gestart. Gedurende het hele pinksterweekend is letterlijk dag en nacht doorgewerkt aan het veiligstellen van al het bewijs op alle mogelijk relevante systemen.

Uit de analyses van de gemaakte digitale forensische kopieën werd op 12 juni 2019 definitief vastgesteld dat de aanvallers bij gegevens van medewerkers gekomen zijn. Daarom moesten voor alle systemen maatregelen worden genomen om zeker te stellen dat zij geen toegang tot de systemen meer zouden kunnen krijgen. De herstelactie op 13 juni 2019 heeft dan ook geen bewijs vernietigd.

In het kader van dit rapport is contact geweest met de heer Ruwhof, die in het artikel is aangehaald. Hij stelt dat hij in een langer gesprek met de betreffende journalist uitleg heeft gegeven over wat in soortgelijke situaties bij veel andere bedrijven vaak aan de hand is. Daarbij zou hij de journalist hebben verteld dat hij regelmatig observeert dat er bij grotere malware-uitbraken door grotere organisaties de keuze wordt gemaakt snel weer terug in bedrijf te zijn. Hij ziet dat deze houding als gevolg heeft dat er vaak belangrijk bewijsmateriaal verloren gaan. Hij benadrukt geen uitspraken over de gemeente Lochem te hebben gedaan, aangezien ten tijde van het gesprek geen technische details over de situatie bij de gemeente publiekelijk bekend waren.

Er is geen reden om aan te nemen dat enig bewijs is vernietigd bij herstelwerkzaamheden.

Waarom maakt de gemeente niet alle documenten openbaar?

In de rapportages van NFIR staan onderzoeksgegevens die voor nog lopende onderzoeken belangrijk zijn. Dit kan gaan om daderkennis, de stand van het strafrechtelijk onderzoek of bepaalde methodieken rond opsporing.

Daarnaast blijkt uit de onderzoeken de interne netwerkstructuur met de daarbij horende zwakheden. Sommige zijn verholpen, maar sommige onderdelen vergen meer tijd om te repareren. Door deze

actief naar buiten te brengen, wordt een complete handleiding gegeven aan kwaadwillenden. De verhoogde monitoring op het netwerk zal er niet voor zorgen dat actief misbruik direct voorkomen kan worden.

De monitoring zorgt er wel voor dat aanvallen mogelijk worden ontdekt en aan het strafrechtelijk onderzoek kunnen worden toegevoegd als daar aanleiding voor is.

Waarom duurt het verzamelen van bewijs zo lang?

Het verzamelen van digitaal bewijs is een arbeidsintensieve taak. Een gemeente heeft veel systemen waar mogelijk sporen te vinden zijn. Van alle systemen moet een digitale forensische kopie worden gemaakt. Dat moet op de juiste manier gebeuren om te voorkomen dat bewijs verloren gaat en ervoor te zorgen dat deze bij een strafzaak rechtsgeldig is. Hierbij is apparatuur gebruikt die in Nederland wordt erkend door het Nederlands Forensisch Instituut en in de Verenigde Staten door het Ministerie van Justitie. Voor het bedienen is gecertificeerd personeel ingezet. Omdat het hier om grote hoeveelheden data gaat en het veiligstellen nauwgezet moet gebeuren, is er nogal wat doorlooptijd. In totaal is grofweg 7 terabyte (ruim 7.000 gigabyte) aan gegevens veiliggesteld en minutieus onderzocht.

Verklarende woordenlijst

Autoriteit Persoonsgegevens: de Nederlandse toezichthouder voor de privacywetgeving Algemene Verordening Gegevensbescherming (AVG).

CISO: Chief Information Security Officer, de adviseur op het gebied van informatiebeveiliging.

Extern Bureaublad: zie Remote Desktop Protocol.

Golden ticket: benaming voor een certificaat waarmee gedurende een bepaalde tijd alle systemen in een Windows-domein volledig toegankelijk zijn. Deze functionaliteit is nodig om Windows bepaalde beheerstaken te laten uitvoeren. In handen van een aanvaller betekent dat deze letterlijk overal bij kan komen.

IBD: afkorting voor Informatiebeveiligingsdienst voor Gemeenten. Dat is een onderdeel van VNG Realisatie dat ondersteuning biedt op het gebied van informatiebeveiliging en privacybescherming.

ICT: Informatie en Communicatie Technologie.

NCSC: Nationaal Cyber Security Centrum. Overheidsinstelling die zich richt op informatiebeveiliging door expertise te leveren aan bepaalde partijen binnen de overheid en de vitale sectoren, partijen aan elkaar te koppelen en te proberen maatschappelijke schade te voorkomen.

RDP: afkorting voor Remote Desktop Protocol. Een protocol om op afstand computers over te nemen. In het Nederlands noemen we deze functionaliteit ook wel ‘extern bureaublad’. Dit protocol staat bekend om diverse beveiligingsproblemen in het verleden. Daarom is het niet gebruikelijk deze dienst aan te hebben staan.

TLP: Traffic Light Protocol (verkeerslichtprotocol). Dit zijn internationale afspraken over de vertrouwelijkheid van documenten. *White* (wit) staat voor openbare informatie, *amber* (oranje) mag binnen de organisatie worden verspreid voor hen die het nodig hebben (*need to know*) en *red* (rood) is zeer vertrouwelijk (*for your eyes only*).