Te goed van vertrouwen?
Duidingsrapportage ransomware-aanval Hof van Twente

Brenno de Winter, De Winter Information Solutions

8 maart 2021

Inhoudsopgave

Samenvatting

Op 1 december 2020 ontdekt de Gemeente Hof van Twente het slachtoffer te zijn van een ransomware-aanval. Veel bestanden blijken versleuteld en een groot aantal servers is weggegooid. Een losgeldbericht staat op computers en ligt her en der op de printer. Het signaal is helder: als geen losgeld wordt betaald, komen de bestanden niet meer terug. Maar voor een gemeente is betalen geen optie, omdat het overheidsbeleid is dit niet te doen.

De organisatie is net als het college van burgemeester en wethouders verrast. Zij wisten niet beter dan dat de zaakjes al jaren prima op orde waren. Onderzoeken van de laatste jaren gaven geen zorgwekkende beeld. Voor het beheer zijn afspraken gemaakt met een dienstverlener, waarmee prima wordt samengewerkt. Kortom alles lijkt prima in orde. Het incident trekt veel media-aandacht. Niet eerder is zo publiekelijk zichtbaar dat bij een overheid grote delen van de administratie ontoegankelijk zijn. Dat is voelbaar in de relatie met de burger. In andere gevallen wordt de versleuteling ongedaan gemaakt; hier lukt dat niet. Sterker nog: de backups blijken niet toegankelijk. Dit is geen probleem dat eenvoudig te verhelpen is en nog altijd werkt de gemeente aan herstel.

In de eerste fase wordt onderzoek gedaan door een beveiligingsbedrijf. Het zusterbedrijf daarvan, de dienstverlener van de gemeente, had het hiervoor gevraagd. Er worden wat losse aanknopingspunten gevonden, maar dit maakt niet de volle omvang van de aanval duidelijk. Daarnaast telt dit onderzoek niet als een forensisch onderzoek, omdat deze organisatie niet beschikt over een opsporingsvergunning. Voor het college is juist de vertrouwdheid van de leverancier geruststellend. Er is een langlopende en vooral goede relatie. Na het wijzen op het belang van onafhankelijk onderzoek door een marktpartij met de juiste vergunning worden meerdere bedrijven benaderd. NFIR voert het digitaal forensisch onderzoek uit.

Er lekt informatie naar de Volkskrant. Hierdoor kan een journalist contact opnemen met de criminelen. Daarmee ontstaat een ingewikkelde situatie, waarbij contact met de criminelen via de media verloopt. De informatie die normaliter uit dit soort contacten vloeit is nu opeens niet voor het strafrechtelijk onderzoek beschikbaar en de timing verstoort de gekozen aanpak. Via de krant geven de gijzelnemers aan hoeveel geld zij willen hebben om de data vrij te geven. Als bewijs wordt een wachtwoord geleverd dat inderdaad blijkt te werken op de aangegeven machine, waardoor er sprake is van daderkennis. Het bedrag van zo'n 750.000 euro is beduidend hoger dan in andere gevallen werd gevraagd. Dat roept de vraag op of het fungeren als boodschapper of

juist het geven van informatie via vragen een invloed op de prijs heeft gehad.

Voor een organisatie die zo enorm is getroffen, is de vraag onvermijdelijk of er geen signalen waren dat dit risico bestond. Bij een incident van deze omvang is helder dat de beveiliging onvoldoende is gebleken. Het blijft risicobeheersing, maar duidelijk is dat als er een incident optreedt dit sneller opgemerkt had moeten worden en dat de impact minder had moeten zijn.

Er is gezocht naar signalen aan het college van burgemeester en wethouders, die mogelijk gemist zijn en hadden moeten leiden tot actie. Die zijn niet aangetroffen. De leverancier van de systeembeheerdiensten heeft voor zover bekend geen signalen afgegeven om te waarschuwen voor tekort schietende beveiliging. Deze zijn niet in de rapporten aangetroffen. Binnen de ambtelijke en bestuurlijke organisatie zijn deze ook niet aangetroffen. Voor zover nu te overzien is, ontbrak het aan signalen om op te acteren voor de burgemeester.

Uit een audit en een pentest komen geen signalen naar voren dat deze risico's werden gelopen. Vooral bij de pentest is dat opmerkelijk. Het rapport beschrijft namelijk een onderzoek naar onder andere de computer waarop de aanvaller is ingebroken. Op basis van het forensisch onderzoek was er sprake van een zwakheid, die logischerwijs gevonden had moeten worden door de pentesters. Uit open bronnen blijkt namelijk dat de open staande poort in de periode van het onderzoek ook open heeft gestaan. Deze cruciale informatie heeft de burgemeester niet bereikt.

De audits qua beveiliging (ENSIA) zien op het voldoen aan de vereisten van aansluiting op DigiD en Suwinet. Hier wordt gekeken naar informatiebeveiliging met betrekking tot de aansluiting. Als stuurinformatie voor het college is dit onvoldoende geschikt. Pas wanneer de tekortkomingen zo ernstig zijn dat aansluiting wordt geweigerd, zou het bruikbaar zijn. Dan is echter sprake van een zeer extreem falen van informatiebeveiliging.

Een jaar eerder, in juni 2019, werd een aanval ontdekt bij de gemeente Lochem. De gemeente Hof van Twente heeft de lessen tijdens dit incident ter harte genomen. De burgemeester besluit zo transparant mogelijk te zijn over de hack. Doordat over het dan nog vertrouwelijke onderzoek is gelekt en de Volkskrant bemiddelt tussen criminelen en gemeente, is het lastig transparant te zijn zonder de opsporing verder te schaden.

Daarnaast roept Hof van Twente breed de hulp van andere gemeenten in. Die komt onder andere vanuit Enschede en Rotterdam. Daarnaast helpt de Informatiebeveiligingsdienst voor Gemeenten met het incident.

Uit het forensisch onderzoek wordt duidelijk dat een beheerder van de gemeente een aanpassing in de firewall heeft gemaakt. Hierdoor kon overal vandaan een zogenaamde FTP-server (server om bestanden uit te wisselen) worden bereikt. Op deze server draaide het Remote Desktop Protocol om op in te loggen. Toen daarna het wachtwoord werd veranderd in een eenvoudig te raden wachtwoord, duurde het niet lang voor de aanvaller op dit systeem inlogde. Er was geen meerfactorauthenticatie (een extra beveiligingslaag) ingesteld. Daarnaast bleek ook nog eens dat vanaf deze server bijna alle systemen van de gemeente zonder obstakel te bereiken waren. Waarschuwingen in logboeken werden tijdens de aanval niet ontdekt, waardoor de aanvaller dagenlang de tijd had. De fout triggerde de aanval, maar de infrastructurele fouten maakten de aanval voor de criminelen effectief.
Verder valt op dat Hof van Twente kijkt voor de ICT gebruik te maken van de expertise van grotere buurgemeente. Deze keuze is zeer begrijpelijk, omdat uit deze crisis en die bij andere gemeenten telkens blijkt dat kleinere bestuursorganen moeite hebben hun ICT op orde te krijgen en te houden. Ze moeten als kleine organisatie namelijk een breed palet aan ICT-diensten ondersteunen. Dat maakt de keuze niet minder moedig.

Dit rapport draagt als titel 'Te goed van vertrouwen?'. Dit kenschetst het beeld dat in de eerste week van het incident duidelijk werd. De gemeente geeft veel vertrouwen aan leveranciers. Daarbij ligt al vlot bloot dat de informatie waar de bestuurders en de gemeente op acteerden anders was dan de realiteit die uit het incident is gebleken. De stuurinformatie gaf geen aanleiding om aan de knoppen te draaien, toch zat het niet goed. Is het bestuur te goed van vertrouwen? Of is dit breder in de industrie een probleem en zijn we allemaal te goed van vertrouwen?

Het is niet bekend of er sprake is van een enkele aanvaller of een groep. Voor de leesbaarheid wordt gesproken van een aanvaller.

Hoofdstuk 1

Over Ransomware

Het incident bij de gemeente Hof van Twente is een digitale aanval met ransomware, zogenaamde gijzelsoftware. Dit betekent concreet dat computerbestanden voor de gemeente ontoegankelijk zijn, totdat er losgeld is betaald. Voor een goede duiding staan we eerst stil bij het verschijnsel ransomware.

1.1 Algemene beschrijving

De methode van het gijzelen van computersystemen is op zich niet nieuw. Het is eigenlijk afpersing met een digitale component. Sommige zaken zijn reuze-eenvoudig. Zo zijn er incidentele voorbeelden bekend van bijvoorbeeld beheerders, die met wachtwoorden computers of netwerkapparatuur gijzelen. Daarnaast zijn er gevallen bekend waar leveranciers software die toegang geeft tot data of de data zelf gijzelen. De afhankelijkheid van een derde maakt een organisatie kwetsbaar.

Criminelen op afstand doen dit digitaal door bestanden op de computers te versleutelen en losgeld te eisen. Om zekerheid te geven dat de aanvaller authentiek is, wordt vaak bij contact als bewijs de sleutel voor een machine afgegeven. Besluit het slachtoffer te betalen, dan ontvangt deze de sleutels voor de overige machines. Soms levert de aanvaller maatwerksoftware voor het ontsleutelen.

Om de gijzelactie succesvoller te laten zijn, is een veelvoorkomend patroon dat de aanvaller langdurig in de systemen aanwezig is. De belangrijkste reden is om uit te zoeken waar de back-up wordt gemaakt en deze te beschadigen. Zonder recente reservekopieën is de schade groter. Er is dan meer druk om te betalen en de waarde van de data stijgt.

Precies om dezelfde redenen kopiëren de gijzelnemers data. Daarmee dreigen ze dan publiek te gaan als betaling uitblijft. In combinatie met het verlies van de data is dat een ideaal drukmiddel om slachtoffers over de streep te trekken toch te betalen.

1.2 Betalen of juist niet?

De vraag of er al dan niet betaald moet worden, is ingewikkeld. Het Nederlandse overheidsstandpunt is dat er niet betaald wordt. Voor een overheid is dat logisch, omdat belastinggeld aan criminelen geven een bizarre situatie zou creëren. Daarnaast zou betalen het zakelijke model van de criminelen stutten.

Alleen buiten de overheid ligt dit debat complexer. Waar een decentrale overheid in een extreem geval voor geld bij het Rijk terecht kan, geldt dat voor bedrijven niet. Een ransomware-aanval kan daarmee leiden tot een faillissement. De keuze is dan opeens 'einde bedrijf' of 'betalen en overleven'.

Daarnaast is er het argument dat betalen kan leiden tot het niet-publiceren van persoonsgegevens van medewerkers, klanten of burgers. Dat maakt het debat ingewikkeld voor organisaties. Want niemand wil een crimineel businessmodel voeden, maar evenmin wil je een faillissement of je relaties beschadigen door gelekte data.

Hoofdstuk 2

Het incident in Hof van Twente

2.1 Ontdekking van het incident

Op 1 december 2020 treedt er een verstoring op in de systemen van Hof van Twente. De ernst hiervan is duidelijk om 08:45 en ongeveer een kwartier later treedt het bedrijfscontinuïteitsplan in werking. De servicedesk van de ingehuurde dienstverlener voor systeembeheer ontdekt een bericht op de backup server:

> Hello, need data back? contact us fast:
> <emailadres1>
> <emailadres2>
> Best Regards

De e-mailadressen zijn onderdeel van het strafrechtelijk onderzoek en zijn daarom niet gedeeld.

Het losgeldbericht verschijnt op meerdere systemen en ligt op diverse printers.

2.2 Eerste dagen incident

Het bericht maakt duidelijk dat er iets met de gegevens van de gemeente is gebeurd. Wat een storing leek te zijn, is mogelijk een beveiligingsincident. De beheerderspartij schakelt een zusterbedrijf in met ervaring op het gebied van informatiebeveiliging. Er blijken meerdere systemen niet meer toegankelijk te zijn. Het beveiligingsbedrijf komt ter plaatse en bekijkt de situatie. Uit de rapportage wordt duidelijk dat er een achterdeur open staat. Een server voor bestandsuitwisseling, een FTP-server, staat naar de buitenwereld open en laat vanaf het hele internet verbindingen toe.

Het blijkt dat er geen goede backup beschikbaar is voor snel herstel van de gegevens. Het is daarmee waarschijnlijk dat er informatie blijvend verloren is gegaan. De gemeente huurt voor het herstellen van de data een gespecialiseerd bedrijf in. Dat probeert de wachtwoorden te kraken om de data te kunnen ontcijferen. Daarnaast wordt binnen de overheid hiervoor rekenkracht beschikbaar gesteld.

De gemeente zoekt contact met de Politie Oost-Nederland. Die start een onderzoek. Daarnaast ondersteunt deze politie-eenheid de gemeente met adviezen. Haar handelen is erop gericht om erger te voorkomen. Tot slot komt er ondersteuning vanuit de Veiligheidsregio, Informatiebeveiligingsdienst voor Gemeenten en enkele gemeenten. In de eerste fase valt op dat Hof van Twente zoekt naar het opzetten van een structuur.

Bestuurders zijn getraind op een fysiek incident, maar digitaal zijn structuren moeilijker zichtbaar voor ze. Dat betekent niet dat er geen fysieke uitwerking is. Alle administratieve systemen en processen zijn niet beschikbaar. Het contact binnen het team verloopt via de mobiele telefoon en persoonlijke e-mailaccounts. De gemeente ligt letterlijk plat, wat de sturing lastig maakt.

De eigen systemen zijn niet toegankelijk, maar er is cloud dienstverlening. Deze wordt versneld ingezet om te kunnen werken. Er worden meerdere maatregelen genomen:

1. Opbouwen van een nieuwe, veilige netwerkomgeving. Door deze stap te zetten, wordt direct gewerkt met de laatste stand van de techniek en best practices. Belangrijke verbetering daarbij is een betere scheiding van de netwerkonderdelen, zodat bij een nieuwe aanval niet de hele of een groot deel van de organisatie wordt getroffen.

2. Nieuwe wachtwoorden. Om uit te sluiten dat oude wachtwoorden gelekt zijn en om zeker te zijn dat nieuwe wachtwoorden lastig te kraken zijn, hebben alle gebruikers nieuwe wachtwoorden moeten instellen.

3. Niet wachtwoorden alleen. Voor de clouddienst is functionaliteit aangezet, waardoor er niet alleen met een wachtwoord in te loggen is. Een andere factor (sms, unieke eenmalige code of iets anders) moet worden ingegeven. Hierdoor betekent het verlies van een wachtwoord niet automatisch dat een aanvaller toegang tot systemen krijgt.

4. Extra beveiligingssoftware op laptops. Op alle laptops van de gemeente is aanvullende beveiligingssoftware geïnstalleerd om aanvallen sneller in de kiem te smoren.

5. Nieuwe versleutelde verbindingen. Op alle laptops is nieuwe software geladen, die beveiligde verbindingen opzet met de gemeentesystemen.

6. Nieuwe beheerssoftware laptops. Er is nieuwe software op laptops geïnstalleerd om te waarborgen dat systeembeheer goed verloopt. De software waarborgt dat niet zomaar verouderde software gebruikt kan worden, onbevoegde software niet op de machines wordt geplaatst en beveiligingsstandaarden worden nageleefd.

Er worden meerdere bedrijven aangezocht om digitaal forensisch onderzoek en incident response (het verhelpen van de technische problemen) te verrichten. De gemeente vraagt NFIR deze taak op zich te nemen. Die partij neemt vanaf dat punt de regie over.

2.3 Losgeld betalen

Er is vanaf het eerste moment een duidelijke lijn: de gemeente Hof van Twente gaat niet betalen aan de gijzelnemers. Losgeld betalen is door staand landelijk beleid en voor het lokaal bestuur geen optie. Dat is in het begin de houding en wordt later een daadwerkelijk collegebesluit.

Het dilemma of er een onderhandeling moet worden gestart is ingewikkeld. Aan de ene kant is dit politiek gevoelig, omdat de beleidslijn is om niet met gijzelnemers te onderhandelen. Aan de andere kant is het onderhandelen belangrijk in de opsporing, omdat hier informatie uit kan komen. Daarnaast kan er zekerheid komen of de aanvaller daadwerkelijk over data beschikt. Dit tactisch goed uitspelen is secuur werk. Wie te veel informatie prijsgeeft, kan daarmee de kostprijs verhogen of duidelijk maken welke gekopieerde informatie de vaak buitenlandse criminelen daadwerkelijk in handen hebben. Er wordt besloten niet direct contact op te nemen, maar dit te doen als de informatiepositie rond het incident iets sterker is.

2.4 Berichtgeving de Volkskrant

Deze onderzoeksaanpak wordt echter doorkruist door een actie van de Volkskrant. Een journalist van die krant krijgt de mailadressen van de gijzelnemers in bezit. Hij besluit contact met de criminelen op te nemen. Deze verstrekken een code ('12345') aan de verslaggever. Deze code blijkt daadwerkelijk op de door de criminelen aangegeven systemen te werken. De bestanden op vier servers worden ontcijferd. Daarmee is duidelijk dat de journalist nu daadwerkelijk beschikt over een stuk dat daarvoor daderkennis was: de juiste code behorend bij de systeemnamen.

De Volkskrant verstrekt de communicatie met de criminelen niet, waardoor er een aantal complicaties in het strafrechtelijke onderzoek optreedt. Bij

ransomware-zaken is het contact met de gijzelnemers een mogelijkheid informatie te vergaren en inzicht in de werkwijze of de kennispositie van de daders te krijgen. Die mogelijkheid is er niet en de berichtenuitwisseling wordt niet verstrekt. Uit gesprekken met politiemedewerkers wordt duidelijk dat deze situatie het strafrechtelijk onderzoek in ieder geval niet heeft ondersteund.

De journalist in kwestie geeft aan dat de aanvaller niet weet dat een gemeente is gegijzeld. De burgemeester staat de journalist te woord. Een dag na het gesprek meldt de Volkskrant dat er een bedrag van 50 Bitcoins (op dat moment zo'n 750.000 euro in waarde) wordt geëist. Verder stelt de krant dat de criminelen 40 terabyte zouden hebben gestolen. Langs meerdere wegen blijkt dat later in tegenspraak met het feitenrelaas uit het digitaal forensisch onderzoek. Daaruit blijkt niet dat er data uit systemen is gestolen.

Wat opvalt is dat dit bedrag hoger is dan in andere, vergelijkbare zaken in die periode is geëist. Zo is de eis lager bij de veel grotere Universiteit van Maastricht, grote productiebedrijven en administratieve organisaties. Dit roept de vraag op of het simpele feit dat de media een doorgeefluik voor criminelen worden de prijs van het losgeld opdrijft. Het gegeven dat criminelen via de mail of het krantenartikel weten dat deze zaak te linken is aan een overheid kan invloed hebben. Het kan de prijs opdrijven en anderzijds kan het - als er inderdaad data is gekopieerd - leiden tot effectief misbruik van de data.

Hoofdstuk 3

Onderzoeken

3.1 Eerste onderzoek

Wanneer het duidelijk is dat er sprake is van een incident, wordt een beveiligingsbedrijf door de leverancier van ICT-diensten ingeschakeld voor een onderzoek. Beide bedrijven blijken volgens het Handelsregister van de Kamer van Koophandel te behoren tot dezelfde groep van ICT-bedrijven.

Het beveiligingsbedrijf geeft op de website aan dienstverlening te bieden op het gebied van privacy, ethisch hacken en security monitoring. Uit het dienstenportfolio blijkt niet dat incident response (het reageren op een digitale inbraak), digitaal recherchewerk of onderzoek tot de hoofdbedrijfsactiviteiten behoren. Evenmin valt dat uit de beschrijving van de Kamer van Koophandel op te maken. Het bedrijf staat niet vermeld op de lijst van POB-vergunninghouders en vermeldt op de eigen website ook niet dat het beschikt over een dergelijke vergunning. De rapportage van het bedrijf wordt daarom niet als forensisch accuraat gewogen, maar als een expert rapportage. Het verslag geeft geen onderzoeksvraag aan.

Het beveiligingsbedrijf ontdekt dat de firewall verkeer van internet doorlaat naar een FTP-server (een server bestemd om bestanden uit te wisselen). Zij huren een antivirusexpert in om logboeken te analyseren. Daarnaast is er een backup gemaakt van de aanmeldservers in het netwerk van de gemeente en de FTP-server. De rapportage toont diverse afbeeldingen gelabeld als bewijs. In alle gevallen (zowel bij het veiligstellen van data als het vergaren van bewijs) vertelt het rapport niet hoe dat is gedaan, met welke hulpmiddelen, of dat forensisch accuraat is gebeurd en wie dat heeft vastgesteld.

Op basis van open bronnen onderzoek stelt het beveiligingsbedrijf vast dat er veel poorten op de FTP-server open stonden. Dat betekent dat er veel verschillende soorten software een verbinding konden maken met de betref-

fende server.

3.2 Forensisch onderzoek

Zoals beschreven is NFIR een forensisch onderzoek gestart. Dat is een feitelijk onderzoek op basis van wetenschappelijke methodes om feiten te achterhalen. Voor een dergelijk onderzoek worden gesprekken gehouden, worden digitale sporen verzameld en wordt het bewijs geanalyseerd. Belangrijk bij een dergelijk onderzoek is dat het navolgbaar is, zodat het ook bij juridische (strafrechtelijke) procedures kan worden gebruikt. In het geval van Hof van Twente is het doel van het onderzoek als volgt bepaald:

> Het doel van het forensisch onderzoek is om vast te kunnen stellen op welke wijze ongeautoriseerde toegang is verkregen tot het geautomatiseerde netwerk. Dit omvat eveneens de momenten waarop de toegang heeft plaatsgevonden en de uitgevoerde malafide handelingen. Daarnaast heeft het onderzoek tot doel om vast te stellen in hoeverre gegevens door ongeautoriseerde personen zijn ingezien, gekopieerd, dan wel geëxtraheerd. Tot slot is door de opdrachtgever gevraagd te onderzoeken waarom en hoe het incident plaats heeft kunnen vinden.

Uit het forensisch onderzoek komt een aantal interessante bevindingen naar voren:

1. Twee fouten geven toegang. Op 15 oktober 2020 wordt het wachtwoord van een beheerdersaccount aangepast naar Welkom2020. Dit is makkelijk te raden. Op 29 oktober 2019 wordt een regel in de firewall aangepast. Vanaf dat moment mag iedereen op internet verbinding zoeken met een server voor bestandsuitwisseling (FTP-server). Op deze machine draait een kwetsbare versie van het Remote Desktop Protocol (RDP). Van af het moment dat dat is gedaan, worden er iedere dag tussen de 50.000 en 100.000 inlogpogingen gedaan. De eerste succesvolle poging blijkt op 9 november 2020 te zijn.

2. Aanval. Op 16 november 2020 worden er meerdere malafide tools geïnstalleerd. In de dagen erna volgen tools voor de malware Cobalt Strike, geschikt voor het uitvoeren van ransomware. Deze software begint contact te zoeken met de moederserver (de Command & Control Server). De signalen zijn te vinden, maar zijn voor zover bekend niet door de verantwoordelijk beheerders gedetecteerd.

3. Versleutelen servers. Waar vaak specifieke malware wordt gebruikt om systemen te versleutelen, is dat hier niet het geval. Er is software ingezet die legitiem gebruikt wordt om harde schijven te versleutelen.

Alleen in dit geval heeft de aanvaller het wachtwoord. Na het opstarten moet het wachtwoord worden ingegeven voor het ontcijferen van de data. Bij het tonen van het scherm voor het wachtwoord kan ook een boodschap worden gegeven. Hier wordt de eerder genoemde losgeldtekst gebruikt.

4. Beheerder. Voor herhaalde toegang heeft de aanvaller zichzelf voorzien van een inlog met de rechten van een systeembeheerder.

5. Onderzoek. De aanvaller heeft software gebruikt om onderzoek te doen welke systemen het slachtoffer heeft. Het is verder duidelijk dat er handelingen zijn verricht om de omgeving beter te leren kennen.

6. Malware. De malware (Cobalt Strike) bevat software om contact op te nemen met een moedersysteem van de aanvaller, een zogenaamde Command & Control Server.

7. Werkomgeving afschermen. In de periode van de aanval gebruikt de aanvaller software om werkbladen, die hij heeft overgenomen, te kunnen afsluiten. Een rechtmatig beheerder kon er - gedurende de tijd van de aanval - dan ook niet bij.

8. Meer dan ransomware. Bij de aanval is eerst software geïnstalleerd en gebruikt om spammail te versturen. Dit is echter door de firewall tegengehouden.

9. Weggooien. Naast het versleutelen van data zijn door de aanvaller 90 virtuele servers weggegooid. Een virtuele server is een computer met alle functionaliteit die draait op een andere machine tezamen met andere virtuele servers om zo capaciteit te sparen. Het weggooien van dergelijke servers is aanvullend op het versleutelen van machines.

10. Signalen. De gemeente Hof van Twente beschikt ten tijde van de aanval over meerdere softwareoplossingen om kwaadaardige software te herkennen. Deze heeft gefunctioneerd en herhaaldelijk bestanden verwijderd en in de logboeken melding gemaakt van kwaadaardige software. In een aantal gevallen heeft de software de malware niet kunnen verwijderen of niet verwijderd, maar wel herkend.

11. Voorkomen. NFIR concludeert dat de fouten van de beheerders hebben geleid tot toegang. De inrichting van de infrastructuur heeft de verdere aanval mogelijk gemaakt. Zo hadden vrijwel alle systemen toegang tot elkaar. De monitoring heeft niet zo gefunctioneerd dat de signalen die er waren zijn opgepikt en hebben geleid tot actie. De aanvaller is in staat gebleken om commando's uit te voeren, waardoor backups buiten het netwerk van de gemeente zijn vernietigd en de lokale backups zijn versleuteld.

De aanleiding voor de digitale inbraak is een tweetal fouten door de beheerders: het kiezen van een makkelijk te raden wachtwoord om in te loggen als beheerder en daarnaast het open zetten van de firewall voor al het verkeer van internet creëerde de mogelijkheid tot inbreken.

Het ontbreken van meerlaagse beveiliging maakt de inbraak ook succesvol. Juist de aanwezigheid van meerdere lagen is gebruikelijk om daarmee eventueel falen nog te kunnen opvangen en te waarborgen dat de impact van een aanval minder wordt. Een enkele fout zou geen catastrofale gevolgen mogen hebben.

In dit geval ontbrak het aan meerfactorauthenticatie (een beveiligingsmiddel naast een wachtwoord), waardoor het raden van het wachtwoord ook daadwerkelijke toegang betekende. Het ontbrak aan afscherming met een speciale beveiligde verbinding (vpn), waardoor daadwerkelijk iedereen naar het netwerk van de gemeente kon gaan. Eenmaal binnen waren alle systemen te bereiken. Tot overmaat van ramp bleek het mogelijk om de backups te vernietigen.

3.3 ENSIA-verklaring

Voor het incident zijn er eerdere onderzoeken geweest. Een van de stuursignalen voor het bestuur zijn de ENSIA-verklaringen voor Suwinet en DigiD. Dat wordt door de VNG uitgelegd als:

> ENSIA structureert verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid.

Het beeld dat is samengesteld over 2019 leidt niet tot het begin van vermoeden dat een grote aanval, zoals heeft plaatsgevonden, tot de mogelijkheden behoort. Het lijkt eerder dat de organisatie voldoende in controle is over de maatregelen. Een verklaring van een auditor, die aangeeft dat het bestuur de situatie scherp op het netvlies heeft, bevestigt dit beeld.

Het incident illustreert dat de beheersmaatregelen onvoldoende op orde waren. Het blijkt mogelijk in te loggen zonder iets naast het wachtwoord, accounts te voorzien van zeer slechte wachtwoorden en nagenoeg het hele interne netwerk te raken vanaf een bestandsuitwisselserver. Daarnaast blijkt er een leverancier te zijn gecontracteerd voor het beheer, terwijl bij de gemeente medewerkers ook beheerstaken uitvoeren. Kort samengevat: ENSIA

in deze vorm blijkt niet voldoende geschikt als stuurmiddel voor het college en de raad. Er moet echt breder worden gekeken.

Deze vaststelling diskwalificeert ENSIA op geen enkele wijze. Het maakt wel helder dat duidelijker voor het openbaar bestuur moet worden wat de waarde van dit hulpmiddel is: wat mag je hier wel en wat mag je hier niet van verwachten?

3.4 Penetratietest

Voor de aanval op het netwerk van Hof van Twente blijkt er een zogenaamde penetratietest uitgevoerd. Daarbij kijken beveiligingsonderzoekers naar zwakheden in de systemen. In het onderzoek wordt de server onderzocht, waarop later door de aanvaller zal worden ingebroken. Het doel van de rapportage is een onderzoek naar de externe infrastructuur. De pentest wordt op 25 mei 2020 gestart en op 16 juni 2020 wordt de rapportage definitief vastgesteld.

Uit de rapportage valt niet op te maken dat er problemen spelen met de FTP-server. Het hele beeld van de pentest geeft geen hoge bevindingen (ernstige risico's), maar wel verbeterpunten. Het betreft 11 bevindingen, waarvan 1 een middelgroot risico is, 5 de inschatting laag risico krijgen en 5 als informatief worden aangemerkt.

De opstellers geven in de rapportage aan het onderzoek handmatig te hebben uitgevoerd conform een eigen ontwikkelde methodiek. Wat de methodiek behelst is niet duidelijk. Daarom is het ook niet mogelijk vast te stellen of deze methodiek zich kan verhouden tot bestaande internationale standaarden voor pentesten. Een aantal zaken in de pentest is opvallend:

1. Bij iedere bevinding ontbreekt de methodiek hoe men tot een bevinding is gekomen. Daarmee kan het lastig zijn een bevinding te controleren of reproduceren.

2. Er wordt expliciet gemeld dat er wordt gekeken naar toegang tot achter de infrastructuur liggende systemen. Toch leidt dat niet tot de bevinding dat nagenoeg alle systemen bereikbaar zijn vanaf nagenoeg iedere machine. Er wordt niet gewezen op de best practice om een netwerk te segmenteren (in stukken te verdelen) om daarmee bij een aanval minder toegankelijk te maken. Expliciet benoemt de pentest daarnaast nog:

   (a) Via het domein toegang krijgen tot andere onderdelen binnen het domein (bijvoorbeeld de beheeromgeving, of de gegevens of omgeving van andere organisaties of gebruikers die binnen hetzelfde

domein opereren) en aldaar gegevens inzien, wijzigen of verwijderen;

(b) Via het domein toegang krijgen tot andere systemen en aldaar gegevens inzien, wijzigen of verwijderen.

3. Op de server waar uiteindelijk op zal worden ingebroken worden geen bevindingen gedaan. Uit open bronnen (vanaf het internet) valt echter op te maken dat in mei en juni 2020 de RDP-poort (Remote Desktop Protocol) open staat. Bij een scan zou dat de vraag moeten oproepen, waarom dat het geval is. Veel inbraken beginnen met open staande RDP-poorten. Bij onder meer de hack op de gemeente Lochem was dit ook het geval. Als het noodzakelijk is deze dienst te gebruiken, dan zijn er een aantal best practices, die in mei, juni en ten tijde van de hack niet waren ingevoerd:

   (a) Gebruik van een virtual private netwerk, waardoor er altijd met een beveiligde en geverifieerde verbinding wordt gewerkt.

   (b) Het alleen beschikbaar maken van deze dienst voor de internetadressen van mensen die er echt bij moeten.

   (c) Het beperken van de mogelijkheden na het inloggen op het systeem.

4. Er staat een tweetal testomgevingen open naar het internet. Voor risico's wordt gewerkt met een zogenaamde CVSS-score dat de ernst van de bevindingen duidt op een schaal tot 10. Deze score krijgt de waarde 0.0. De bevinding maakt niet duidelijk waar deze omgevingen op zijn aangesloten en of een inbraak op die systemen invloed op de rest van het netwerk zou kunnen hebben. Daarmee wordt niet het signaal afgegeven dat hier nader naar gekeken zou moeten worden. Er staat immers een score van 0.0 en dat wekt de indruk dat het een verwaarloosbaar risico betreft.

5. De rapportage beschrijft alleen wat de onderzoekers is opgevallen. Het beschrijft niet wat er daadwerkelijk is onderzocht en hoe aansluiting wordt gezocht bij internationale standaarden. Hierdoor is vaag wat er is onderzocht, alleen dat er een aantal bevindingen is gedaan. Zo is bijvoorbeeld onduidelijk of er alleen met technische hulpmiddelen is gekeken of is gekeken naar netwerkarchitectuur en deze technisch is geverifieerd.

De pentest wekt de indruk dat er geen dreigende problemen waren bij Hof van Twente en dat de beveiliging redelijk op orde was. Een bestuurder kan

hieruit niet destilleren welke problemen door de onderzoekers niet in beeld zijn gebracht.

De pentest kan helpen om een beeld te krijgen van de actuele situatie en daarmee dienen als stuurmiddel. Daarvoor is het wel noodzakelijk dat glashelder is wat een onderzoek exact heeft onderzocht en bevonden. In deze specifieke casus geeft het onderzoek een bestuurder niet het beeld dat er kwetsbaarheden zijn, die kunnen leiden tot een hack van het kaliber Hof van Twente. Dat hoeft op zichzelf geen probleem te zijn, maar veel bestuurders lezen in een dergelijk onderzoek een signaal hoe goed de beveiliging is. Die helderheid verschaft dit onderzoek niet.

3.5 Losse bevindingen

Naarmate duidelijker werd dat een fout van een medewerker van de gemeente heeft geleid tot het incident, kwam de vraag op wie nu waarvoor verantwoordelijkheid draagt. Een complete analyse voert te ver voor een duidingsrapportage. Wel is duidelijk dat de rollen in de praktijk minder strak belegd bleken te zijn dan op papier werd verondersteld.

Voor het beheer was een externe leverancier aangetrokken. Echter bleken interne medewerkers soms ook beheerstaken uit te voeren. Dat was historisch zo gegroeid, omdat de vorige dienstverlener veelal op kantoor kwam en de dienstverlener ten tijde van de aanval op afstand werkte. Het is onduidelijk of tussen leverancier en gemeente voldoende is gecommuniceerd over technische wijzigingen.

Gedurende de eerste dagen van het incident werd duidelijk dat er door de gemeente flink werd geleund op de vaste leveranciers. Een zusterbedrijf van de vaste dienstverlener werd door diezelfde dienstverlener gevraagd onderzoek te verrichten. Dat hoeft op zichzelf geen probleem te zijn. Het risico is dat dit op een later moment leidt tot een discussie of het beveiligingsbedrijf de dienstverlener bij eventueel gebleken tekortkomingen de handen boven het hoofd houdt.

Het vertrouwen in vaste leveranciers was dermate groot dat signalen van andere betrokkenen niet meteen op volle waarde werden geschat. Dat bleek uit het niet direct willen grijpen naar een onafhankelijk digitaal forensisch onderzoek. Daarbij speelde het vertrouwen een rol dat mogelijk nog veel te herstellen was. Dat er mogelijk een compleet nieuw netwerk moest worden gebouwd, was de eerste dag moeilijk voorstelbaar. Daarbij werd in de week erna heel duidelijk dat de gemeente stuurt op duurzame relaties gebaseerd op wederzijds respect en vertrouwen. Iedere verandering daarin is juist tijdens

een crisis ingewikkeld.

Hoofdstuk 4

Conclusies en aanbevelingen

4.1 Conclusies

De aanval op de gemeente kwam voor het college als een donderslag bij heldere hemel. De informatie waarvoor college en de gemeenteraad beschikten, gaven geen signalen af dat er iets fundamenteel niet in orde was. De onderzoeken bleken onvoldoende geschikt om rond informatiebeveiliging de juiste stappen te zetten. Hierdoor ontstond er een kloof tussen het openbaar bestuur en de technische realiteit. Terwijl alle signalen waren dat de gemeente de zaakjes best goed op orde had, bleek er toch van alles mis te zijn. De stuurinformatie, waarop de gemeente acteerde, was onvoldoende om als niettechneut te kunnen doorgronden dat er mogelijk iets mis was. Het probleem daarbij is dat het nog ontbreekt aan eenduidige informatie en veel eisen nog relatief nieuw zijn. Dat betekent dat bestuur niet kan weten wat de werkelijke waarde van een onderzoek of rapportage is.

Directe aanleiding voor het incident zijn de handelingen geweest om de firewall aan te passen en een wel erg eenvoudig te raden wachtwoord. Omdat het ontbrak aan meerlaagse beveiliging, gaf het raden van het wachtwoord meteen toegang. Een extra factor om zelfs met een goed wachtwoord niet naar binnen te kunnen, bleek niet aanwezig. Eenmaal binnen bleek dat er rechten waren om als beheerder te werken. De computer gaf direct toegang tot veel andere systemen van de gemeente en daarmee vielen de systemen als dominostenen om. De afwezigheid van een effectieve detectie gaf vervolgens de aanvaller de ruimte om rustig de aanval uit te voeren. Snelle detectie had het gijzelen van de data mogelijk voorkomen. Het niet goed genoeg hebben ingericht van de backups maakte de aanval zeer schadelijk voor de gemeente.

Hof van Twente geeft goede openheid van zaken over het incident zonder daarbij het strafrechtelijk onderzoek in gevaar te brengen. Hierdoor is het mogelijk lessen te trekken en daadwerkelijk beter te worden. Soms gaan inci-

denten rond informatiebeveiliging gepaard met de nodige geheimzinnigheid. Juist een open cultuur helpt een sfeer te creëren, waarbij het mogelijk is om te waarschuwen voor dreigingen.

Voor een organisatie die zo is getroffen door ransomware bleek de organisatie verrassend veerkrachtig te zijn. De burger heeft in de dienstverlening kunnen merken dat er problemen waren. Deze problemen werden niet groter dan noodzakelijk door de beschikbaarheid van alternatieve processen.

Tijdens het incident wordt meerdere malen duidelijk dat wachtwoorden voor systemen door de beheerspartij niet direct worden verstrekt en dat hierover discussie ontstaat. Mij is niet duidelijk wat de aanleiding hiervoor is. Belangrijk is dit gegeven te benoemen en te voorzien van een aanbeveling.

4.2 Aanbevelingen

Er valt een aantal aanbevelingen te doen op basis van dit incident. Voor een deel ligt dat bij de organisaties die betrokken zijn bij het incident. Maar voor een deel is dat iets wat industriebreed een leerpunt zou kunnen zijn:

1. Stuurinformatie. Verzorg betere stuurinformatie door bredere beveiligingsonderzoeken te laten uitvoeren, waarbij duidelijk is wat er tijdens het onderzoek wordt uitgevoerd. Laat een penetratietest niet alleen vertellen wat er niet goed is, maar ook hoe zo'n bevinding tot stand is gekomen. Daarnaast moet duidelijk zijn welke onderzoeken er zijn gedaan met welk resultaat om het beeld beter compleet te krijgen. Gebruik de Baseline Informatiebeveiliging Overheid (BIO) als kans om beter inzicht in de informatiebeveiliging te krijgen. Organiseer tegenspraak op de rapportages, waardoor een kritische blik duidelijk maakt wat er wel en wat er niet uit een rapport mag worden afgeleid.

2. Verantwoordelijkheden. Borg dat de verantwoordelijkheden op papier en in de praktijk worden nageleefd. Het is logisch dat een partij die op papier verantwoordelijk is dat in de praktijk ook is en die rol ook neemt. Laat daar periodiek (bijvoorbeeld jaarlijks) op controleren. Blijkt de uitwerking in de praktijk te weerbarstig, dan moeten óf de procedures worden aangepast óf de verantwoordelijkheden anders belegd.

3. Bevraag op beveiliging. Een groot gedeelte van het proces van een gemeente loopt via digitale systemen. Dat maakt ons afhankelijk. De politiek kan een rol spelen door het bestuur te bevragen over de beveiliging om daarmee dit onderwerp levend te houden. Daarbij is belangrijk te beseffen dat er altijd incidenten zijn. De vraag is hoe weerbaar de organisatie is om incidenten snel te detecteren, ze niet onnodig groot te laten worden en snel weer naar een normale situatie terug te kunnen.

4. Blijf hulp zoeken. Van gemeenten wordt veel gevraagd, waarbij (bijna) bij iedere taak ook ICT-ondersteuning noodzakelijk is. De omvang van Hof van Twente maakt het lastig dit met eigen mensen goed in te regelen. Bij het incident is hulp ingeroepen van andere gemeenten. Blijf dat doen in de toekomst voor die zaken die net een maat te groot zijn, waardoor de taak behapbaar blijft.

5. Oefen. Een digitaal incident is niet hetzelfde als een fysiek incident en vraagt om andere kennis. Ondertussen kan een digitaal incident - zo blijkt hier ook weer - uitwerking in de fysieke wereld hebben. Oefen op de regie van incidenten, noodplannen en herstel.

6. BIO. Grijp het voldoen aan de Baseline Informatiebeveiliging Overheid aan als een kans om een groeiplan op beveiligingsgebied te realiseren.

7. Incidentenmanagement. Maak een plan voor een volgend incident. Denk na wie welke rol in het incident krijgt. Als er een juridisch onderdeel in de casus zit (bijvoorbeeld strafrechtelijk handelen), is het aan te raden meteen te grijpen naar een forensisch onderzoek door een bureau met een opsporingsvergunning. Maak heldere afspraken met leveranciers wanneer ze zich melden met een probleem en hoe daarmee wordt omgesprongen.

8. Toegang tot systemen en informatie. Zorg ervoor dat goed is geborgd dat de gemeente op ieder moment moet kunnen beschikken over de data (en de systemen). De gegevens horen het eigendom te blijven van het openbaar bestuur en die moet altijd kunnen handelen op basis van die data. Bedenk dat een incident niet alleen bij de gemeente zelf hoeft te spelen, maar door externe factoren kan worden getriggerd, bijvoorbeeld door een beslaglegging op systemen, faillissement van een onderneming, hack in een andere omgeving, een aanwijzing van de landelijke overheid of het verbod op het gebruik van een dienst door bijvoorbeeld een rechterlijke uitspraak.

9. Inkoop management. Maak informatiebeveiliging en privacybescherming bij het inkopen van diensten en producten een standaard onderdeel van de overeenkomst. Maak heldere afspraken dat een leverancier tenminste aan vergelijkbare eisen voldoet als de gemeente.

10. Bestuurskamer. Een gemeente is zo afhankelijk van ICT. Laat u bijstaan in de bestuurskamer door expertise op dit vlak net zoals dat bijvoorbeeld gebruikelijk is voor financiële keuzes.

11. Neem de technische aanbevelingen van NFIR ter harte:

    (a) 3-2-1-principe voor back-ups. NFIR adviseert het toepassen van een 3-2-1 back-up principe. Dat staat voor 3 kopieën van de

data, waarbij 2 kopieën op verschillende datadragers staan en 1 kopie op een andere locatie wordt bewaard. Wanneer dit principe goed geïmplementeerd is, kan men bij een ransomware-aanval altijd eenvoudig terugschakelen naar de oude situatie met een beperkt verlies van data. Hierbij dienen de juiste authenticatie en autorisaties te zijn ingericht.

(b) Toegangsbeleid. Een strak toegangsbeleid zorgt ervoor dat bepaalde rechten niet zomaar aan diverse accounts worden toegekend. Wanneer multi-factor authenticatie wordt gebruikt, zijn gelekte of geraden wachtwoorden geen probleem omdat de aanvaller niet over de multi-factor beschikt. Tevens wordt aangeraden om een wachtwoordbeleid af te dwingen dat gebruik van eenvoudig te raden wachtwoorden weet te voorkomen.

(c) IT-security beleid. Een duidelijk IT-security beleid zorgt ervoor dat er weloverwogen keuzes worden gemaakt bij de inrichting van het netwerk en het gebruik van het netwerk. Wanneer hier duidelijk over wordt gecommuniceerd met medewerkers, zal dit voor een algeheel verhoogd veiligheidsniveau zorgen.

(d) Segmentatie. Het is belangrijk om een netwerk gesegmenteerd in te richten zodat niet alle servers en alle data in één keer getroffen worden bij een aanval. Segmentatie moet zorg dragen dat bij een aanval slechts één of enkele servers worden getroffen en niet de gehele infrastructuur.

(e) Security awareness traingen. Training kan ervoor zorgen dat het algehele security niveau van de organisatie omhoog gaat en medewerkers beter beschermd zijn tegen phishing en getraind worden in het gebruik van goede wachtwoorden.

(f) Security-audits. NFIR adviseert om periodiek security audits uit te voeren. Door middel van security audits kunnen dreigingsrisico's vroegtijdig aan het licht komen en worden aangepakt. Het periodiek uitvoeren van security audits is van belang vanwege het dreigingslandschap dat continu verandert.