VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

# Lessen uit de hack en datalek bij Gemeente Buren

## Lessons Learned

**Op vrijdagavond 1 april 2022 ontdekte een medewerker van systeembeheer bij de gemeente Buren vreemd gedrag op het ICT-netwerk. Bestanden waren niet langer toegankelijk. Een nadere blik leerde dat zo'n 12 systemen waren versleuteld, waaronder een aantal bedrijfskritische systemen. Criminelen hadden kans gezien ransomware te installeren; malafide software die bestanden gijzelt in combinatie met afpersing. Alleen na het betalen van losgeld worden de bestanden vrijgegeven.**

### Impact op de bedrijfsvoering

De gemeente Buren bewaart haar backups ook offline, los van het netwerk. Daardoor kon ze direct starten met het opruimen en herstellen van de versleutelde systemen. De gemeente wilde voorkomen dat inwoners en ondernemers hinder ondervonden van de aanval. Direct na het weekend kon de dienstverlening aan hen doorgaan. In de eigen bedrijfsvoering waren de gevolgen echter groot. E-mail en samenwerkingstools waren enkele weken in meer of mindere mate bruikbaar. De incidentrespons trok een zware wissel op de eigen medewerkers omdat ze naast het reguliere werk nu ook betrokken waren om de gevolgen van de hack voor de inwoners zo beperkt als mogelijk te houden.

### Impact op privacy: Datadiefstal en publicatie

De ransomwaregroepering in kwestie staat bekend om drievoudige afpersing (triple extortion). Slachtoffers worden afgeperst met 1) versleuteling van data, 2) DDoS-aanvallen (distributed-denial-of-service), pogingen om systemen niet of moeilijker bereikbaar te maken), en 3) verkoop/publicatie van data. Op 14 april bleek een monster van 130 gigabyte van de buitgemaakte data te zijn gepubliceerd op de publicrelations-pagina van de ransomwaregroepering. Na downloaden van dit sample kon worden vastgesteld dat het gegevens betrof van de gemeente Buren en om welke gegevens het precies ging. De criminelen claimden 5 terabyte te hebben gestolen en dat klopte

in de tijdlijn van het forensisch onderzoek. Hiermee werd het zwartste scenario werkelijkheid. Niet alleen werden de bedrijfsvoering en dienstverlening van de gemeente bedreigd, ook bleek de vertrouwelijkheid van data van de gemeente Buren en in ernstige mate geschonden. Omdat de gemeente Buren enkele taken voor de gemeente Neder-Betuwe uitvoert, bleek dat ook te gelden voor data van die gemeente.

## Hoe verliep de incidentrespons?

Hoogste prioriteit was dat inwoners en ondernemers zo min mogelijk hinder ondervonden van het incident. Systemen voor de dienstverlening werden daarom als eerste opgeschoond en hersteld. Vrijwel tegelijkertijd zette de gemeente de veilige wederopbouw van de eigen ICT-systemen in gang en nam zij beschermende maatregelen tegen de DDoS-aanvallen. De uitkomst van de risicoanalyse was dat de gemeente inwoners van haar gemeente zo volledig mogelijk moest informeren over de diefstal en publicatie van data. Om het risico op misbruik te minimaliseren (zie paragraaf 'Handelingsperspectief') bood te gemeente betrokkenen aan om kosteloos identiteitsbewijzen te vervangen. Van de hack is aangifte gedaan bij de politie en het datalek is gemeld aan de Autoriteit Persoonsgegevens.

Zoals bij alle grote incidenten is (crisis)communicatie een belangrijke component van de incidentrespons. Naast inwoners moet er ook oog zijn voor ondernemers, eigen medewerkers, leveranciers/ketenpartners en de gemeenteraad. Voor de laatste doelgroep organiseerde de gemeente twee informatiebijeenkomsten voorafgaand aan de raadsvergadering, waar externe experts uitleg gaven over voorval en aanpak.

## Risicoanalyse publicatie data

De gestolen data bevatte privacygevoelige gegevens van inwoners. Een dergelijke diefstal kan leiden tot verschillende soorten (strafbaar) misbruik. Betrokkenen kunnen schade ondervinden door mogelijke identiteitsfraude, pesten of intimidatie. Voor crimineel of strafbaar gedrag zijn middelen, gelegenheid, motief en intentie nodig. Een dataset met gegevens geeft criminelen een instrument om strafbare feiten te plegen, maar de IBD schatte de kans op feitelijk misbruik laag in. Dit heeft te maken met ervaringen bij grote datalekken bij andere gemeenten en de relatief moeilijke vindbaarheid van de dataset.

**Zoals bij alle grote incidenten is (crisis)communicatie een belangrijke component van de incidentrespons.**

Ook is kennis nodig van het Nederlandse openbaar bestuur en de Nederlandse taal om uit de dataset de 'nuttige' gegevens te halen. Men heeft in elk geval een zekere basiskennis nodig van zoeken op het dark-web. Voor de actoren die dat hebben, zijn daar heel wat aantrekkelijkere en meer gestructureerde datasets te vinden. De gemeente bezit in de regel weinig informatie die directe handelswaarde heeft onder criminelen, zoals gebruikersnamen en wachtwoorden van gebruikers en creditcard-gegevens.

## Handelingsperspectief datadiefstal

Tegen zaken als pesten en intimidatie kan pas iets worden gedaan wanneer ze zich voordoen. Hier past alertheid van de gemeente en van inwoners. Door inwoners te vragen om elk vermoeden van misbruik (pesten, intimidatie of fraude) te melden, kan de gemeente met behulp van een forensische kopie van de data ten tijde van de hack nagaan of daadwerkelijk sprake is van misbruik. In dat geval kan de inwoner aangifte doen bij de politie. Aanvullend heeft de gemeente afspraken gemaakt met politie en Openbaar Ministerie over de opvolging van dergelijke aangiftes.

Dan resteert het risico op identiteitsfraude, waarvoor naam, adres, aanvullende gegevens en een kopie van een identiteitsbewijs nodig zijn. De gemeente kan het risico op misbruik tot een minimum reduceren door de betrokkenen aan te bieden om kosteloos een nieuw document aan te vragen. Het oorspronkelijke document wordt geregistreerd als ongeldig, waarmee de mogelijkheid voor criminelen vervalt om met de kopie zaken te doen met overheidsinstanties en banken.

## Externe ondersteuning

Gemeente Buren meldde het incident op 2 april bij de Informatiebeveiligingsdienst (IBD) van VNG en bij de cyberverzekeraar. Ook schakelde de gemeente digitaal onderzoeksbureau en securityadviseur Hunt & Hackett in. Op 22 april riep de gemeente de versterking in van het bedrijf Hoffmann voor crisismanagement en onderzoek naar de buitgemaakte data. Ten slotte huurde de gemeente ook het bedrijf Parcival in om te ondersteunen bij de crisiscommunicatie rondom het incident. De IBD bleef als adviseur in het crisisteam betrokken tot de voorlopige afsluiting van de crisissituatie.

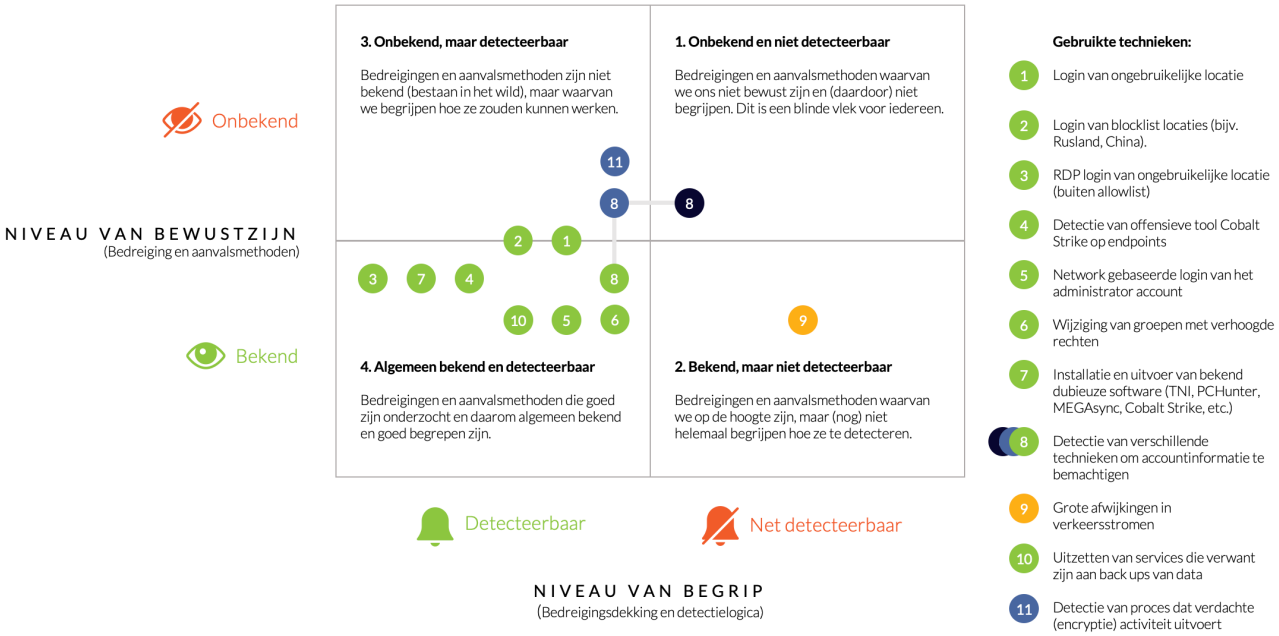
## Management en uitvoering

De eerste fase van de crisisbeheersing was gericht op het veilig herstellen van de ICT-systemen en het implementeren van technische maatregelen (o.a. anti-DDoS, meerfactorauthenticatie (MFA) waar dat ontbrak, monitoring en detectie). In die fase van het werk waren keuzes door management en bestuur prominent. In latere fasen nam het werk af van de uitvoerende functies (bijvoorbeeld de CISO, PO, ICT-Beheerder) en nam die van het lijnmanagement, de directie en het bestuur toe. Doordat ook veel externe partijen aan het werk waren, waanden operationele medewerkers zich soms minder betrokken. Om dit te voorkomen is interne communicatie tijdens een incident van groot belang. Daarom informeerde de gemeente Buren de eigen medewerkers vaak over de voortgang.

## Voorkomen is beter dan genezen

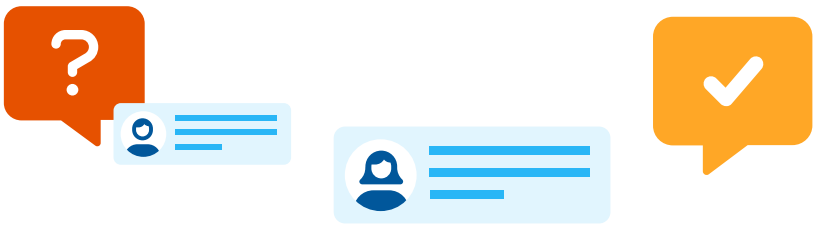
Uit het digitaal forensisch onderzoek bleek dat met name meerfactorauthenticatie (op twee systemen waar dat nog ontbrak), en detectie cruciaal zouden zijn geweest om de aanvallers in een vroeg stadium te kunnen stoppen. Hiermee hadden de datadiefstel en de versleuteling van data hoogstwaarschijnlijk voorkomen kunnen worden.

Met behulp van goede backups in combinatie met een goed proces om data te bewaren en te herstellen, kon de gemeente binnen enkele dagen herstellen van de versleuteling van data. De offline (niet met het netwerk verbonden) backups van de gemeente waren niet te vernietigen of te versleutelen door de criminelen. Ook het backup-proces bleek niet te stoppen, ondanks het feit dat de criminelen voor langere tijd met beheerrechten in de systemen van de gemeente zaten. De offline backups hebben daarmee ernstige gevolgen voor de bedrijfsvoering weten te voorkomen.




Detectiematrix waarin de aanval is geplot op het MITRE ATT&CK framework

# Wat waren de dilemma's?



## Losgeld

De lijn van de Nederlandse overheid is dat in gevallen van ransomware geen losgeld wordt betaald. Toch moet een organisatie alle opties afwegen. Het betalen van losgeld is in sommige situaties de enige optie: het kopen van de sleutel geeft de beschikking over de versleutelde data.

De gemeente Buren had een werkend backup-systeem waardoor geen belangrijke data voor de organisatie verloren zijn gegaan. Betaling was daarom niet noodzakelijk. Dan blijft de optie om met betalen de doorverkoop of publicatie van gestolen data wellicht te voorkomen. Argumenten tegen betaling zijn in stand houden van een crimineel verdienmodel, geen garanties, uitlokken nieuwe aanvallen op de Nederlandse overheid. Argumenten voor betaling zijn vernietiging van de resterende data en een einde aan verkoop en/of publicatie. De betrokken externe specialisten, waaronder de IBD, namen alles in overweging en adviseerden de gemeente dat de argumenten tegen betaling zwaarder wogen dan argumenten voor betaling. De gemeente heeft geen losgeld betaald.

## Bestuurlijke grip op digitale veiligheid

Na de eerste fase van de incidentrespons was er tijd voor reflectie: hoe had dit kunnen gebeuren? Uit gesprekken met de gemeente bleek dat zowel bestuur als management relatief veel aandacht hadden voor het thema digitale veiligheid. De gemeente had een programmatische aanpak, de jaarlijkse ENSIA-rapportage gaf geen aanleiding tot zorg, men had recent nog penetratietesten uitgevoerd.

Uit het digitaal forensisch onderzoek bleek wel dege-lijk dat het incident voorkomen had kunnen worden (2-factorauthenticatie) of eerder herkend (monitoring, detectie en respons). Bestuurlijk en politiek gezien zijn dit operationele details voor de bedrijfsvoering. Het is de vraag hoe politici en bestuurders hier grip op kunnen hebben en houden.

## Omgang met data in het algemeen

De gestolen data waren 5 terabyte aan ongestructureerde gegevens, grotendeels onder beheer van afdelingen en medewerkers. Het is belangrijk dat een gemeente, naast beveiliging, ook grip heeft op de informatie: weten wat er is, wat de kroonjuwelen zijn en vervolgens gefundeerde keuzes maken over welke beschermende maatregelen daarbij horen.

## Informeren betrokkenen met beperkt handelingsperspectief

Het uitgangspunt van de crisiscommunicatie is inwoners en ondernemers zo transparant mogelijk informeren over het incident, de mogelijke gevolgen en het handelingsperspectief. Het handelingsperspectief voor betrokken inwoners en ondernemers is beperkt: men kan hoogstens alert zijn. In gevallen waar de gemeente een kopie van het identiteitsbewijs opslaat, kan de betrokkene een nieuw document aanvragen.

Direct nadat duidelijk was dat data van de gemeente gestolen waren, liet de gemeente huis-aan-huis een brief bezorgen aan alle inwoners. Hierin stond wat er was gebeurd, wat de gemeente ging doen en wat inwoners zelf konden doen: zij moesten alert zijn op signalen van (identiteits)fraude.

In de eindfase van de incidentrespons leidde dit tot een dilemma waarbij de vraag was of een nieuwe brief van de gemeente aan de inwoners zinnig zou zijn of slechts zou leiden tot onzekerheid en angst. Uiteindelijk is toch voor de volle transparantie gekozen voor een herhaling van de boodschap: "wij zijn gehackt, wij zijn alert en u dient dat ook te zijn." Lokale partij PCG Buren nam aanvullend haar verantwoordelijkheid door een document ter beschikking te stellen met tips en adviezen rondom identiteitsfraude, dit document is gedeeld op de gemeentewebsite.

Het internationale karakter van ransomware maakt dat de Nederlandse Politie en Openbaar Ministerie vooralsnog weinig instrumenten hebben om deze criminaliteit tegen te gaan of de gevolgen voor inwoners te kunnen beperken.

# Lessen voor gemeenten

## 1. Tref basismaatregelen en controleer deze regelmatig

In oktober 2021 stuurde VNG-voorzitter Jan van Zanen een brief aan alle burgemeesters met een dringende oproep om basismaatregelen te treffen voor informatiebeveiliging. De adviezen in deze brief zijn onverkort van kracht:

- Houd hard- en software up-to date;
- Gebruik meerfactorauthenticatie (2FA/MFA);
- Hanteer een strikte netwerksegmentatie;
- Zorg voor robuuste backups;
- Test en oefen uw ICT-crisisplannen.

## 2. Richt, ondanks de kosten, zo snel mogelijk monitoring en detectie in

Monitoring, detectie en een adequate respons op meldingen zijn onmisbaar anno 2022. Het is voor gemeenten van belang dat bekend is wat er op het netwerk en in de (cloud-)systemen gebeurt zodat kan worden geacteerd als hierin afwijkingen van de norm optreden. Voor de meeste gemeenten is het aan te raden om dit als een dienst af te nemen in de vorm van een MDR-oplossing (Managed Detection & Response).

**Meer weten?**
Bekijk de IBD visie op monitoring response en de richtlijnen & aandachtspunten voor de inkoop en implementatie van een M&R-oplossing.

## 3. Controleer afspraken met leveranciers en ketenpartners en herzie deze waar nodig

Gemeenten zijn voor veel processen afhankelijk van leveranciers en ketenpartners. De gemeente kan nog zo veilig zijn, maar de keten is zo sterk als de zwakste schakel. Het is daarom van belang dat gemeenten niet alleen afspraken maken, maar ook toezien op de naleving ervan. Als gemaakte afspraken niet toereikend blijken te zijn, moeten deze worden herzien.

## 4. Communiceer snel, vaak en transparant na een hack

Een informatiebeveiligingsincident heeft grote impact. Anders dan bij een fysiek incident is er geen zichtbare component. De brand, zwaailichten en afzetlinten ontbreken immers. Het onderwerp is bovendien abstract, technisch en complex. Door snel, veel en transparant te communiceren straalde de gemeente Buren daadkracht en betrokkenheid uit. Communicatie moet niet alleen gericht zijn op inwoners, maar ook op ondernemers, eigen medewerkers, leveranciers/ketenpartners en de gemeenteraad.

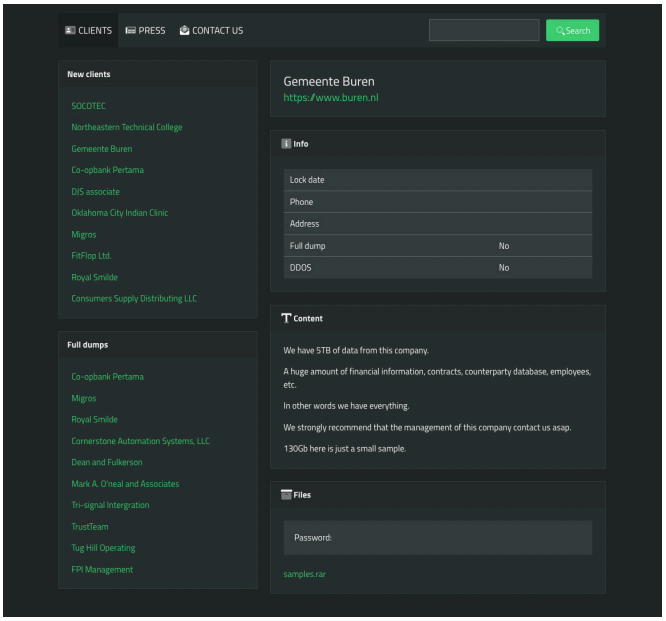
## 5. Wat je niet (online) opslaat, kun je ook niet lekken

De gemeente Buren moest midden in een crisis nagaan wat er precies op de systemen stond en wat dus mogelijk gelekt kon zijn. Veel aandacht ging naar het opsporen van kopieën van identiteitsbewijzen. Identificatie van inwoners wordt in de praktijk vaak gedaan door een kopie van het identiteitsbewijs op te vragen. Het is echter niet nodig om de kopieën online te bewaren.

De IBD adviseert om in brede zin periodiek na te gaan of en welke data precies noodzakelijk zijn om te bewaren op het netwerk. Het register van verwerkingen kan hierbij een belangrijke rol spelen. De overige data (waaronder kopieën van identiteitsbewijzen) kunnen worden gearchiveerd of zelfs vernietigd. Het bewaren van data moet een duidelijk proces zijn dat bekend is bij alle medewerkers en afdelingen.

**Bonustip: meld ieder incident bij de IBD**
De IBD helpt gemeenten bij de incidentrespons. De vaste contactpersonen weten de IBD-CERT (het Computer Emergency Response Team) goed te vinden. De IBD kan ook de gemeentesecretaris en burgemeester van advies voorzien. Vertrouwelijkheid is hierbij geborgd.

Juist in de eerste fase kan de IBD gemeenten bijstaan in moeilijke keuzes: welk onderzoek laat u door wie uitvoeren? Wat moet eerst en wat kan later? Wat en hoe communiceren we met medewerkers, de gemeenteraad, inwoners en ondernemers? Ook helpt de IBD bij het informeren van andere gemeenten, de ministeries en gemeentelijke leveranciers. De IBD sluit graag (virtueel) aan bij het interne crisisteam, zodat de gemeente focus houdt op de eigen organisatie en de juiste afwegingen maakt.




1 https://nl.wikipedia.org/wiki/Distributed_denial_of_service
2 https://www.huntandhackett.com/redmudnester
3 https://openpub.buren.nl/wp-content/uploads/2022/06/Identiteitsfraude-Tips-en-adviezen.pdf
4 https://www.buren.nl/nieuws/datadiefstal-gemeente-buren/7399/
5 https://vng.nl/sites/default/files/2021-10/20211028_ledenbrief_oproep-aan-alle-burgemeesters-cyberalert.pdf

## Informatie & Downloads

Kijk op **informatiebeveiligingsdienst.nl** voor meer informatie.

vng.nl