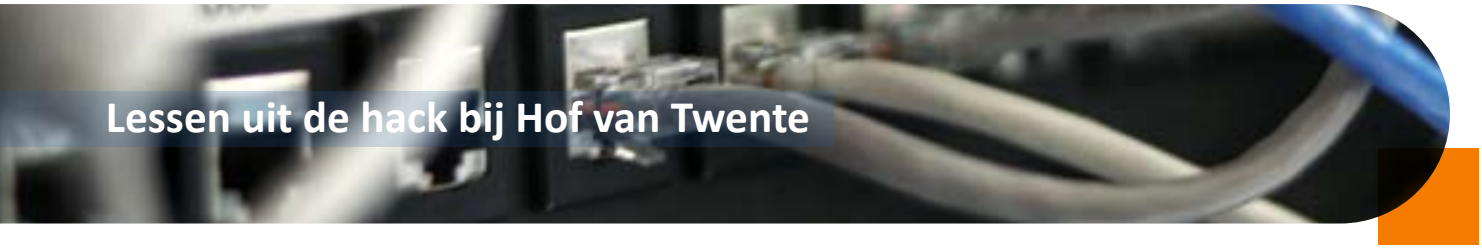

# Lessen uit de hack bij Hof van Twente

**Op 1 december 2020 bleek dat medewerkers van de gemeente Hof van Twente niet konden inloggen op de thuiswerkomgeving.[1] Een beheerder ontdekte dat er een onbekend beheerdersaccount was aangemaakt op systemen van de externe dienstverlener die de kantoorautomatisering voor de gemeente verzorgt. Criminelen zijn op of rond 9 november de systemen binnengekomen via een openstaande RDP-poort die kan worden gebruikt voor beheer op afstand. Door middel van een brute-force aanval ofwel het proberen van grote hoeveelheden gebruikersnaam/wachtwoord-combinaties, kregen de aanvallers toegang tot een van de servers met een testbeheerdersaccount.[2] Tussen 9 en 30 november wisten de aanvallers zo ver te komen in het netwerk dat ze de backups konden versleutelen en data konden vernietigen op tientallen servers.**

## Wat waren de gevolgen?

Na ontdekking van het incident is de bestaande ICT-omgeving afgekoppeld van het internet en geïsoleerd voor onderzoek. Het gevolg was dat vanaf 1 december nagenoeg alle gemeentelijke dienstverlenings- en bedrijfsvoeringsprocessen stil lagen.[3] Zo lag de complete kantoorautomatisering plat en konden inwoners niet terecht voor aanvragen, uittreksels en overige gemeentelijke producten en diensten. Er is een installatiestraat ingericht om een nieuwe tijdelijke ICT-omgeving op te bouwen. Op 4 december 2020 zijn de uitkeringen uitbetaald en vanaf 11 december konden de eerste medewerkers in een nieuwe werkomgeving weer beperkt werken en kon de eerste dienstverlening weer worden opgestart. De daaropvolgende dagen is deze dienstverlening steeds verder uitgebreid.[4] Op 21 december konden medewerkers weer gebruik maken van e-mail.[5]

## Waar liep de gemeente tegen aan?

Het bleek in de eerste fase moeilijk om de exacte situatie te overzien. De leverancier van de kantoorautomatisering zocht met een externe partij naar mogelijkheden om de situatie te herstellen. De politie deed onderzoek. De gemeente had op veel vlakken behoefte aan ondersteuning maar kon nog niet exact bepalen wat nodig was. De zakelijke e-mail van de gemeente was onbruikbaar met als gevolg dat veel communicatie per telefoon en alternatieve mailadressen verliep. De hectiek trok een zware wissel op de bij de crisisbestrijding betrokken eigen medewerkers. De IBD en de gemeente wisten elkaar in de beginfase moeilijk te vinden. Om de wederzijdse verwachtingen af te stemmen en de relaties te leggen is de IBD een aantal keren ter plaatse geweest. Op 4 december startte het forensisch onderzoek in opdracht van de gemeente. De forensisch onderzoekers namen het stokje over van de politie en assisteerden ook bij de crisisrespons. Na het incident werd de gemeente geconfronteerd met een dilemma rond het betalen van losgeld, dit dilemma werd versterkt doordat een journalist van een landelijk dagblad contact heeft gezocht met de daders. Hoe de journalist aan de contactgegevens en informatie over de situatie kwam is vooralsnog onduidelijk.

## Hoe was de crisisorganisatie ingericht?

Vanaf 1 december werkte de gemeente met een crisisorganisatie. Deze organisatie bewoog continue mee met de actuele stand van zaken en kende vanaf het eerste begin drie tafels: ICT, communicatie en kritische bedrijfsprocessen. Ook is er direct opgeschaald en is samenwerking gezocht met externe partijen: collega-gemeenten, Veiligheidsregio Twente (VRT) en diverse externe deskundigen. Tot medio januari is gewerkt in een structuur die volledig is gebaseerd op de crisisorganisatie van de VRT onder GRIP-3.[6] Formeel was er geen sprake van een GRIP-3 situatie, maar op deze structuur kon wel de crisisorganisatie worden gebaseerd. Een senior adviseur crisiscommunicatie draaide vanaf 2 december vol mee in het crisisteam. De gemeente kon een beroep doen op de crisisondersteuning vanuit de veiligheidsregio en ook op de kennis en expertise van andere gemeenten uit de regio en vanuit andere gemeenten in het kader van het gemeentelijk responsnetwerk. Met name de gemeente Rotterdam heeft een grote bijdrage geleverd.

## Wat had de gemeente voorbereid?

De verschillende plannen zoals het bedrijfscontinuïteitsplan (BCM-plan) en het incident-responseplan maakten dat de gemeente snel kon starten met de interne opschaling naar een crisisorganisatie. Het BCM-plan bevatte een prioritering van de belangrijkste processen en producten waarmee de gemeente gefundeerd keuzes kon maken ten aanzien van de volgorde van opstarten van processen. Tegelijkertijd lieten de plannen, vanwege de onvoorstelbare impact van het incident, nog veel vragen onbeantwoord.

## Van crisisorganisatie naar projectorganisatie

Na de eerste crisisfase konden veel essentiële processen weer worden opgestart, dat gebeurde met noodvoorzieningen en tijdelijke constructies. Om de stap te maken van de noodvoorzieningen naar een toekomstbestendige invulling is in de loop van januari 2021 een projectorganisatie ingericht. Het is de verwachting dat compleet herstel minimaal een jaar zal duren. In de

eerste maanden loopt de gemeente nog dagelijks tegen problemen en uitdagingen aan als gevolg van verlies en onbruikbaarheid van data. In de projectorganisatie maakt de gemeente richtinggevende keuzes ten aanzien van de inrichting van de IV-voorziening voor de komende jaren.

## Lessen voor andere gemeenten

### Les 1: Ontbreken van basismaatregelen leidt tot rampscenario en voor een deel onherstelbare schade

De gemeente Hof van Twente werd slachtoffer van een ransomwareaanval door een combinatie van configuratiefouten: een open RDP-poort, een zwakke gebruikersnaam/wachtwoordcombinatie op een tijdelijk beheerdersaccount, onvoldoende netwerksegmentatie en onvoldoende monitoring. Elk van de configuratiefouten zou op zichzelf niet ernstig hoeven te zijn en zou kunnen worden opgevangen door andere beveiligingsmaatregelen. De gevolgen van de combinatie van fouten zijn desastreus te noemen, de dienstverlening en de bedrijfsvoering lagen lange tijd plat en de herstelkosten zijn onvoorstelbaar hoog.

### Les 2: Het is complex om inzicht te krijgen en te houden van beveiliging bij leveranciers en ketenpartners

Goed opdrachtgeverschap houdt in dat u als organisatie stevige afspraken maakt over beveiliging van leveranciers. De leverancier dient ten slotte de beveiliging van de gemeentelijke systemen en gegevens te faciliteren. Na het maken van die afspraken dient de opdrachtgever ook toe te zien op naleving. Bij Hof van Twente was de ICT-voorziening voor een groot deel uitbesteed. Er waren afspraken gemaakt over de beveiliging en de gemeente hield toezicht. Vlak voor het incident is zelfs nog een penetratietest uitgevoerd. Toch kon het incident gebeuren. Het is van belang om de balans te houden tussen streng toezicht en werkbaarheid.[7]

### Les 3: Crisismanagement bij informatiebeveiligingsincidenten staat in de kinderschoenen

De gemeente gaf aan behoefte te hebben aan een duidelijk handelingskader voor een digitaal incident, vergelijkbaar met een ‘kaartje aan de gasmeter’. Voor een externe fysieke crisis bestaan vele procedures en processen. De rol van politie, brandweer, geneeskundige diensten en de burgemeester is helder. Datzelfde geldt voor interne fysieke crises: brand, overstroming, stroomuitval, ontruimingen, die zijn allemaal voorzien en worden regelmatig geoefend. Dat is anders bij informatiebeveiligingsincidenten. Voor dit onderwerp is specifiek aandacht in de Agenda Digitale Veiligheid 2020 - 2024 (ADV).[8] Bij crisismanagement rond digitale incidenten is crisiscommunicatie een belangrijke component die, anders dan bij veel andere interne crises, vanaf het begin een plek moet hebben aan de crisistafel.

### Les 4: De rol van management en bestuur bij incidenten groeit naarmate de impact toeneemt

De CISO is vaak het eerste aanspreekpunt bij incidenten. De CISO kent immers de risico’s, is de eerste adviseur op het thema informatiebeveiliging en weet bij de meeste incidenten ook goed wat nodig is om de situatie te herstellen. Naarmate de impact groeit, krijgen managers en bestuurders een rol, zowel in de communicatie als in de overwegingen rond de oplossing van het incident (zie ook les 3). Zo ook bij een grote ransomwareaanval: Wat zijn onze prioriteiten? Zetten we de systemen uit? Welke stappen zetten we als eerst? Welke processen starten we als eerste op? Hoe informeren we de inwoners? Hoe gaan we om met aansprakelijkheid? Allemaal vragen waarbij de CISO niet leidend is, maar een belangrijk adviseur.

### Les 5: Een gemeente redt het niet alleen bij een groot incident

Als een gemeente geconfronteerd wordt met langdurige uitval van processen en systemen, dan wordt de reguliere organisatie per definitie overvraagd. Het werk gaat door, maar wordt ernstig bemoeilijkt en daar bovenop moet de crisis worden overwonnen. Het is niet vooraf te bepalen aan welke competenties een behoefte ontstaat maar het is van groot belang dat gemeenten elkaar bijstaan in geval van een incident.

## Aanbevelingen

De overheid is gehouden aan de normen in de Baseline Informatiebeveiliging Overheid. De implementatie van deze baseline is geen eenmalige actie maar een doorlopend proces van plannen, uitvoeren, controleren en bijstellen. In deze cyclus adviseert de IBD op basis van het incident in Hof van Twente de volgende prioriteiten voor gemeenten:

1. Dwing op de kortst mogelijke termijn 2FA/MFA af op beheeraccounts (intern- en extern), e-mail, kantoorautomatisering en cloudapplicaties.[9]
2. Breng de basis op orde (Zie voor meer informatie de website van de IBD: programma Verhogen Digitale Weerbaarheid (VDW) module 1)[10]
3. Maak een overzicht van uw cruciale processen en prioriteer deze
4. Actualiseer het bedrijfscontinuïteitsplan, het backup- en restorebeleid en het incidentmanagementproces voor een grootschalige en langdurige uitval van cruciale processen
5. Oefen regelmatig een informatiebeveiligingsincident (U kunt hiervoor o.a. gebruik maken van het oefenpakket van de VNG)[11]
6. Maak gebruik van de 3-2-1 methode[12] bij backups: 3 verschillende kopieën, 2 verschillende media en 1 kopie offline / off site. Test ook regelmatig de mogelijkheid van het herstellen van een kopie.

### Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatiebeveiligingsdienst.nl. De helpdesk van de IBD is te bereiken tijdens kantooruren van 9:00 tot 17:00 uur op het nummer 070 204 55 11 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 204 55 11 (instructies voor het piketnummer op de voicemail).

## Verwijzingen en bronnen


1 Melding aan de IBD dd. 1 december 2020
2 https://www.hofvantwente.nl/actueel/veelgestelde-vragen-cyberaanvalhack-gemeentehuis.html
3 https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2020/12/artikel/update-dienstverlening-gemeente-hof-van-twente-1780.html
4 https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2020/12/artikel/aanvragen-paspoorten-en-identiteitskaarten-weer-mogelijk-1787.html
5 https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2020/12/artikel/medewerkers-weer-bereikbaar-via-e-mail-1794.html
6 https://nl.wikipedia.org/wiki/Geco%C3%B6rdineerde_Regionale_Incidentbestrijdings_Procedure
7 https://www.informatiebeveiligingsdienst.nl/product/inkoopvoorwaarden-en-informatiebeveiligingseisen/
8 https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024
9 https://www.informatiebeveiligingsdienst.nl/nieuws/dringend-advies-dwing-zsm-2-factorauthenticatie-af/
10 https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/
11 https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/
12 https://duckduckgo.com/?q=3-2-1+backup+rule