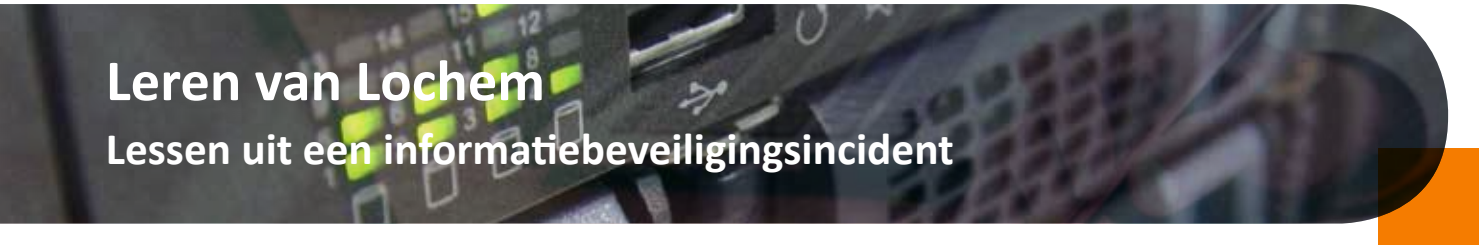

# Leren van Lochem

## Lessen uit een informatiebeveiligingsincident

**Op 6 juni 2019 kwam een IP-adres van de gemeente Lochem in beeld bij een melding van een beveiligingsincident. In de loop van de avond werd duidelijk dat er daadwerkelijk sprake was van een inbreuk op de beveiliging. Hierop verrichtten de politie, de Informatiebeveiligingsdienst voor gemeenten (IBD) en het NCSC onderzoekende en corrigerende werkzaamheden. Gemeente Lochem heeft uitgebreid onderzoek laten doen naar de oorzaak en de gevolgen van de inbreuk op de beveiliging en stelt de belangrijkste resultaten beschikbaar zodat gemeenten en andere (overheids)organisaties kunnen leren van de ervaringen.[1]**

## Oorzaak

Door onbekende reden bleek op een van de systemen van de gemeente onbedoeld het Remote Desktop Protocol (RDP) open benaderbaar via het externe IP-adres. Door een (te) eenvoudige combinatie van gebruikersnaam en wachtwoord konden de aanvallers vervolgens inbreken op het systeem middels een brute force aanval, ofwel het proberen van naam/wachtwoord-combinaties. De situatie laat zich samenvatten als onrechtmatige toegang door een configuratiefout.

## Onderzoeksresultaten

In de fase na ontdekking is direct uitvoerig forensisch onderzoek gedaan. In de periode van ruim vijf maanden is enkele tientallen malen onrechtmatig ingelogd door de aanvallers. Na de inbraak probeerden de aanvallers verder te komen in het systeem en meer rechten te verkrijgen. Hierbij is in elk geval een overzicht buitgemaakt van (interne) gebruikersaccounts van de gemeente.

Analyse van de gedragingen toont dat het de aanvallers te doen was om ransomware te installeren ofwel bestanden te versleutelen in ruil voor losgeld. Er zijn in de genoemde periode diverse soorten malware geïnstalleerd, maar door verschillende redenen, zoals rechtenbeheer en antivirus, konden deze niet worden geactiveerd. Uiteindelijk zijn de aanvallers niet geslaagd in hun doel.

## Herstel

In de fase na het onderzoek nam de gemeente maatregelen om de onrechtmatige toegang definitief te kunnen beëindigen. De wachtwoorden van alle gebruikers- en beheerdersaccounts zijn gereset. De gemeentelijke dienstverlening was hierdoor een dag uit de lucht. Een penetratietest bracht nog enkele tientallen kwetsbaarheden aan het licht die op basis van een risicoinschatting zijn verholpen of ingepland voor oplossing. Het onderzoek, de herstelacties, gemiste werkuren als gevolg van uitgevallen dienstverlening en additionele maatregelen naar aanleiding van de penetratietest zorgden voor hoge incidentele (en niet begrote) kosten bij de gemeente. De kosten waren zelfs vele malen hoger geweest wanneer de malware wel actief was geworden. De IBD heeft namens Lochem een bijstandsverzoek ingediend bij omliggende gemeenten om de capaciteit tijdelijk met gerichte expertise aan te vullen. Een aantal gemeenten heeft om niet de gevraagde expertise en capaciteit aangeboden. Omdat een dergelijk incident al snel te veel vraagt van een individuele gemeente zal de IBD ook in de toekomst de hulp inroepen van dit gemeentelijke responsnetwerk (GRN).

## Communicatie

Snelle, transparante en open communicatie over het incident heeft positieve effecten. De gemeente plaatste op 7 juni, de dag na ontdekking, een nieuwsbericht op de website over de ontdekking van de beveiligingsinbreuk. Op de dag dat de dienstverlening werd gestaakt kon worden terugverwezen naar dit eerdere bericht. Het onderzoek en alle onderliggende documenten zijn in september 2019 openbaar gemaakt. De openheid van de gemeente heeft als gevolg dat de berichtgeving gebaseerd kan worden op feiten en minder op speculaties.

## Lessen uit Lochem

- **Een informatiebeveiligingsincident kan iedere organisatie treffen.** Het incident bij de gemeente Lochem laat zien dat aanvallers lang de tijd nemen om een aanval uit te voeren, zelfs bij een relatief kleine organisatie als Lochem. In dit geval waren de motieven financieel van aard en was het de aanvallers niet te doen om het verkrijgen van vertrouwelijke informatie.
- **De herstelkosten zijn hoog, ook in het geval van een niet geslaagde ransomware aanval.** De kosten zijn nog hoger wanneer de malware wel actief wordt.
- **Een incident komt altijd onverwacht en de vereiste respons overvraagt al snel de interne organisatie.**
- **Een informatiebeveiligingsincident kan langdurig onontdekt blijven.** Als aanvallers eenmaal ‘binnen’ zijn kan het maanden duren tot ze ontdekt worden.
- **Hoe langer een incident voortduurt, hoe hoger de kans op schade.** De aanvallers proberen verschillende methoden en technieken uit en komen zo steeds een stapje dichterbij hun doel.
- **Eenvoudige en structurele basismaatregelen beperken de schade of voorkomen die in het geheel**. In het geval van Lochem bleken rechtenbeheer en antivirus effectief in het voorkomen van activiteit van malware.
- **Snel, open en transparant communiceren over een informatiebeveiligingsincident loont**. Zorgvuldige en complete informatievoorziening wordt gewaardeerd door pers, politiek en publiek.

**De meeste informatiebeveiligingsincidenten ontstaan onbedoeld door menselijke fouten. Opzettelijke aanvallen komen minder vaak voor en zijn in veel gevallen ongericht, aanvallers zijn op zoek naar kwetsbare systemen of configuratiefouten en maken misbruik van elke gelegenheid. Voor onbedoelde en bedoelde maar ongerichte incidenten heeft de IBD onderstaande set adviezen opgesteld.**

## Specifieke adviezen ter verlaging van het risico op incidenten.

- **Zorg voor een vast budget voor informatiebeveiliging.** Bijvoorbeeld als percentage van het ICT-budget. De CISO is de eerste adviseur voor de risicogebaseerde verdeling van tijd en geld. Geef beheerders structureel tijd en gelegenheid om aandacht te geven aan beveiliging.
- **Zorg ervoor dat alle systemen up-to-date zijn.** Dit is makkelijker gezegd dan gedaan. Hier is voor nodig dat alle hard- en software in beeld is (configuratie management), wijzigingen worden bijgehouden (change management) en bekend is wat de meest recente versie van de systemen is (patch management).[2] Gemeenten die hun ICT-foto hebben ingeleverd, krijgen van de IBD kwetsbaarheidsmeldingen voor de gebruikte systemen. Lever deze foto in en houd deze actueel.
- **Zorg voor 2-factorauthenticatie op alle accounts.** Gebruikersnaam en wachtwoord kunnen worden buitgemaakt, een extra factor (bijvoorbeeld een One Time Password (OTP) code maakt het vele malen moeilijker om misbruik te maken van buitgemaakte inloggegevens. NB. Begin met de beheeraccounts.
- **Beveilig Server Message Block (SMB) in Windows**
  - Patch de SMB-kwetsbaarheden in Windows: patch MS17-010 (CVE-2017-0147)
  - Beperk het gebruik van SMB
  - Schakel SMBv1 uit en gebruik alleen SMBv2 en SMBv3
  - Beveilig Remote Desktop Protocol (RDP) in Windows
- **Patch RDP-kwetsbaarheden in Windows: patch MS-12-020 (CVE-2019-0708)**
  - Gebruik RDP (port 3389) alleen wanneer strikt noodzakelijk, en gebruik whitelisting om de toegang te beperken.
  - Plaats elk RDP systeem achter de firewall en zorg dat gebruikers alleen door middel van een VPN kunnen verbinden.
  - Controleer regelmatig of RDP niet via internet toegankelijk is.
- **Beperk toegang tot risicovolle zaken, zorg voor een veilig en makkelijk alternatief**
  - **Schakel macro's in office documenten uit.**
  - **Blokkeer directe bijlagen bij e-mail, maak gebruik van makkelijke en beveiligde bestandsdeling.** Sta gebruikers toe om deze ook in de prive sfeer te gebruiken voor het verzenden van vertrouwelijke bestanden.
  - **Blokkeer prive webmail van diensten als gmail, hotmail, ziggo etc. op het bedrijfsnetwerk.** Sta gebruikers toe om prive-mail op hun smartphone te raadplegen.
  - **Installeer een adblocker en blokkeer scripts in de internetbrowser.**
- De vervolgstap op deze basismaatregelen is een sterkere focus op detectie en actieve preventie van incidenten.[3]

## Specifieke adviezen ter verlaging van de impact van een incident

- **Zorg voor een bedrijfscontinuiteitsplan.** Stel vast welke processen in welke volgorde en op welke wijze kunnen doorgaan bij uitval of onbeschikbaarheid van systemen.
- **Maak gebruik van de 3-2-1 methode bij backups.[4] 3 verschillende kopieën, 2 verschillende media en 1 kopie offline / off site**. Test deze ook regelmatig.

## Specifieke adviezen wanneer zich toch een incident voordoet

- **Zorg voor een goed ingericht incidentmanagement-proces**. beleg verantwoordelijkheden en zorg dat u elkaar snel weet te vinden.
- **Meld ieder incident aan de IBD.** Ook wanneer u zelf niet direct hulp nodig heeft. Zo houdt de IBD een actueel overzicht van dreigingen en incidenten.
  - De IBD kan uw gemeente helpen bij het inschatten van de ernst van het incident, het bepalen van vervolgstappen en communicatie naar inwoners, bedrijven en politiek.
- **Aarzel niet om hulp te vragen aan andere gemeenten.** De IBD kan hierin voor u bemiddelen met behulp van het gemeentelijke responsnetwerk (GRN).

### Links in dit document

1 De analyse van gemeente Lochem en alle onderliggende documenten zijn beschikbaar via www.lochem.nl

2 De IBD biedt een uitgebreid ondersteuningspakket ter verhoging van de digitale weerbaarheid, zie: https://www.informatiebeveiligingsdienst.nl/vdw

3 Zie voor meer informatie: https://www.informatiebeveiligingsdienst.nl/product/vdw-module-2-monitoring-response/

4 Zie voor meer informatie: https://duckduckgo.com/?q=3-2-1+backup+rule

### Meer informatie

Meer informatie over onze dienstverlening vindt u in de andere factsheets van de IBD en op de website www.informatie-beveiligingsdienst.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).

VNG Realisatie