INFORMATIE BEVEILIGINGS DIENST

Notitie

Van: Remco Groet, Informatiebeveiligingsdienst (IBD) – remco.groet@VNG.nl
Aan: CISO Gemeente Lochem
Onderwerp: Beschouwing incidentmanagement gemeente Lochem
Vertrouwelijkheid: TLP-WIT[1]: vrij te verspreiden, voor zover de verspreiding niet strijdig is met de wet zoals bijvoorbeeld de wet op het auteursrecht
Status: Definitief

Inleiding

Hoe goed een gemeente de informatiebeveiliging ook op orde heeft, (ICT-)incidenten zullen altijd optreden. Een goed ingericht incidentmanagement- en responsproces zal de impact daarvan verkleinen omdat snel en adequaat gereageerd kan worden en de schade en impact hierdoor minimaal kunnen blijven. Daarnaast leidt een goede evaluatie ertoe dat door de betrokken partijen lering wordt getrokken van incidenten, waardoor de kans op herhaling ook wordt verkleind.

Aanleiding

Bij het incident dd. 6 juni 2019 bij de gemeente Lochem heeft de Informatiebeveiligingsdienst (IBD) ter plaatse assistentie verleend'. Het NCSC heeft de IBD op verzoek ondersteund in de uitvoering van haar taak. De gemeente Lochem verzocht ons om een beschouwing over het gevoerde incidentmanagement. De IBD geeft met deze notitie een observatie over het handelen van de gemeente gezien vanuit de rol en verantwoordelijkheden van de IBD als collectieve voorziening voor alle gemeenten. Dit betreft nadrukkelijk een blik van buiten door de IBD en gaat over het vaststellen van uitgevoerde taken (het 'wat'). De IBD heeft geen zicht op de interne organisatie en / of processen (het 'hoe').

Identificatie

Hoe eerder een incident herkend wordt, hoe beter de schade kan worden beperkt. Naarmate de inbreuk langer duurt neemt ook de kans op uiteindelijke schade toe. In dit geval is de inbreuk op de beveiliging tijdig[2] ontdekt. De IBD heeft op de dag van ontdekking ter plaatse onderzoek kunnen doen naar de aard van de beveiligingsbreuk.

Schade indamming (insluiting en beperking)

In de eerste fase na ontdekking zijn binnen enkele uren maatregelen genomen om de schade in te dammen. De gemeente heeft hierbij niet geschroomd om advies en ondersteuning van anderen, waaronder de IBD te vragen.

---

[1] https://www.informatiebeveiligingsdienst.nl/traffic-light-protocol-tlp-codes/
[2] Voordat significante schade zoals vernietiging of wijziging van informatie heeft plaatsgevonden. Over de (wijze van) detectie kan de IBD op verzoek van NCSC in dit geval geen mededelingen doen.

We merken hierbij op dat dergelijke incidenten verstrekkende(re) gevolgen kunnen hebben en dat de gemeente erin is geslaagd de gevolgen adequaat te beperken.

Herstel
In de herstelfase is de dienstverlening van de gemeente op 12 juni 2019 gedurende enkele uren gestaakt. Deze grondige actie is nodig geweest om zeker te stellen dat het incident niet opnieuw zou kunnen optreden. Verder heeft de gemeente grondig onderzoek gedaan naar de aard en oorzaak van het incident. De getroffen maatregelen zijn hierop beproefd door middel van een penetratietest. We zien hierin duidelijk een proces van plannen, uitvoeren, controleren en bijstellen. Op verzoek van de gemeente heeft de IBD een bijstandsverzoek gedaan bij omliggende gemeenten om assistentie te verlenen en zodoende de druk op de interne organisatie te verlichten. De gemeente heeft hierop gebruik gemaakt van specialistische kennis van andere gemeenten in de herstelfase.

Communicatie
In het gehele traject heeft de gemeente maximale openheid betracht. Hierbij is rekening gehouden met de mogelijke gevolgen voor de informatiebeveiliging. De openheid van de gemeente heeft als gevolg dat de media-aandacht beperkt is geweest en voor het grootste deel zakelijk en feitelijk was. De IBD ziet de procescommunicatie van de gemeente als zorgvuldig en volledig.

Rapportage en evaluatie
De gemeente heeft grondig onderzoek gedaan naar de aard van de beveiligingsinbreuk en de oorzaken. De IBD is hierbij te allen tijde in de gelegenheid geweest om te kunnen meekijken of er mogelijk leerpunten zijn voor andere gemeenten. Gemeente Lochem, de IBD en het NCSC hebben dit incident gezamenlijk geëvalueerd. Zo draagt Lochem bij aan kennisontwikkeling.

Ten slotte
Voor meer informatie over actuele digitale dreigingen voor gemeenten in het algemeen verwijzen wij naar het Dreigingsbeeld Informatiebeveiliging 2019/2020.[3]

[3] Zie: https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2019-2020/