Bestuurlijke 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. Criminelen zijn enkele weken eerder de systemen binnengekomen en konden dat doen door een combinatie van inrichtingsfouten en gebrek aan monitoring. Toen de criminelen eenmaal binnen waren, vernietigden ze de data en 'gijzelden' ze de reservekopieën van die data. Het is de vraag hoe u dit soort situaties als bestuurder voorkomt en hoe u ermee omgaat als dit toch gebeurt. In dit document treft u een beknopt overzicht van de situatie in Hof van Twente met een aantal lessen voor u als bestuurder. De oproep aan burgemeesters luidt dan ook: u bent zelf aan zet, want dit raakt uw veiligheidsportefeuille en uw gemeente als geheel. Het openbaar bestuur, de financiën en het imago van de gemeente staan op het spel. Wat burgemeesters kunnen doen? Oefenen, agenderen en budget vrijmaken.

Situatieschets

Dienstverlening en bedrijfsvoering vallen stil

Vanaf 1 december lagen als gevolg van de hack nagenoeg alle gemeentelijke dienstverlenings- en bedrijfsvoeringsprocessen stil. Zo lag de complete kantoorautomatisering plat en konden inwoners niet terecht voor aanvragen, uittreksels en overige gemeentelijke producten en diensten.

Onduidelijkheid en onrust

Het bleek in de eerste fase moeilijk om de exacte situatie te overzien. De leverancier van de kantoorautomatisering zocht 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.

GRIP-3

Vanaf de eerste dag werkte de gemeente met een crisisorganisatie, tot medio januari in een structuur die volledig is gebaseerd op GRIP-3, onder leiding van de burgemeester. De veiligheidsregio ondersteunde de gemeente tijdens de crisis. De organisatie bewoog continu mee met de actuele stand van zaken en kende vanaf het eerste begin drie tafels: ICT, communicatie en kritische bedrijfsprocessen.

Communicatie

De burgemeester informeerde met een videoboodschap de inwoners snel en zo volledig mogelijk, dit zorgde, in combinatie met een vaste pagina op de website voor vertrouwen en rust.

Plannen

Met het bedrijfscontinuïteitsplan (BCM-plan) en het incident-responseplan kon de gemeente snel 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 in de volgorde van opstarten van processen. Tegelijkertijd lieten de plannen nog veel vragen onbeantwoord.

Van crisisorganisatie naar projectorganisatie

Na de crisisfase konden veel essentiële processen weer worden opgestart 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 voor de inrichting van de informatievoorziening voor de komende jaren.

Lessen voor bestuurders

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

Agendeer het onderwerp digitale veiligheid regelmatig en laat u zich door uw CISO informeren over de risico's en de bijbehorende maatregelen om deze risico's te beheersen. Zorg in elk geval voor voldoende budget voor digitale veiligheid.

Les 2: Het is lastig en noodzakelijk om inzicht te krijgen en overzicht te houden van beveiliging bij leveranciers en ketenpartners

Ken uw belangrijkste toeleveranciers en bespreek ook met hen regelmatig de belangrijkste risico's.

Les 3: Crisismanagement bij informatiebeveiligingsincidenten staat in de kinderschoenen

Richt procedures en processen in voor informatiebeveiligingsincidenten. Oefen deze ook regelmatig.

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

Ken de dilemma's en vragen waarbij de burgemeester en de gemeentescretaris leidend zijn in geval van een digitaal incident. Dit bereikt u door te oefenen. Voorbeelden van dilemma's: 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?

>>

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

Maak gebruik van kennis en capaciteiten van collega gemeenten. Deel ook uw eigen kennis en capaciteiten als andere gemeenten dit nodig hebben. In de resolutie Digitale Veiligheid[1] noemen we deze solidariteit het Gemeentelijk Responsnetwerk (GRN).

Technische adviezen

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. De IBD ondersteunt gemeenten bij de implementatie van deze normen. Op basis van het incident in Hof van Twente adviseert de IBD nadrukkelijk prioriteit te geven aan basisprocessen en -procedures.

2-factorauthenticatie

Als bestuurder heeft u een voorbeeldfunctie bij de implementatie van nieuwe maatregelen. De IBD adviseert met klem om 2-factorauthenticatie in de gemeente in te regelen, deze maatregel zorgt voor een extra bescherming bovenop gebruikersnaam- en wachtwoordcombinaties. Laat u zich informeren over de stand van zaken in uw gemeente.

Meer weten?

Voor meer informatie is de factsheet Lessen uit de hack bij Hof van Twente beschikbaar op de website van de IBD. U treft hier ook de verwijzing naar de onderliggende onderzoeksrapporten en duidingsrapportage van de gemeente.[2]

Bekijk ook de animatie over digitale veiligheid op de website van de VNG.[3]

Verwijzingen en bronnen

1 https://vng.nl/nieuws/meer-prioriteit-voor-beveiliging-digitale-systemen-gemeenten
2 https://www.informatiebeveiligingsdienst.nl/nieuws/lessen-uit-de-hack-bij-gemeente-hof-van-twente/
3 https://vng.nl/nieuws/2-minuten-digitale-veiligheid

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 070 373 8011 of via het e-mailadres info@IBDgemeenten.nl. De CERT van de IBD is 24x7 bereikbaar via 070 373 8011 (instructies voor het piketnummer op de voicemail).