Oorzaak ransomware-aanval gemeente Buren bekend

15 JUNI 2022, 12:38
De gemeente Buren is op 1 april getroffen door een ransomware-aanval. Bij de hack zijn gegevens van de gemeente gestolen. Vervolgens is een set van 130GB aangeboden op het darkweb, een afzonderlijk en anoniem deel van het internet.

Misbruik inloggegevens leverancier

Uit onderzoek is gebleken dat de ransomware-aanval kon ontstaan doordat criminelen initieel toegang hebben verkregen door misbruik te maken van inloggegevens van een leverancier. Omdat 2-factorauthenticatie op dit account ontbrak, konden de hackers binnen komen in de ICT-omgeving van de gemeente.

Burgemeester Josan Meijers: “Bij onze beveiliging volgen we de richtlijnen van de Baseline Informatiebeveiliging Overheid (BIO). De gemeente kon na de ransomware-aanval meteen doordraaien, omdat de back-upstrategie op juiste wijze is ingericht. Ten aanzien van de monitoring liep ten tijde van de hack nog een inkooptraject dat nog niet was afgerond. Samen met de experts hebben we inmiddels de monitoring van systemen ingericht.”

Meteen na het ontdekken van de hack heeft de gemeente:

- aangifte gedaan bij de politie en het Openbaar Ministerie;
- de Informatiebeveiligingsdienst van de VNG en externe specialisten ingeschakeld om te assisteren met de beperking van verdere schade, het herstellen van systemen en onderzoek te doen naar de daders en de oorzaak van het datalek en;
- een melding gedaan bij de Autoriteit Persoonsgegevens.

Hulp van specialisten

Experts van Hunt & Hackett, een bedrijf dat is gespecialiseerd in cybersecurity en betrokken bij diverse andere digitale onderzoeken, hebben deze week het onderzoek

naar de oorzaak van de ransomware-aanval afgerond. Dinsdag 14 juni is de gemeenteraad hierover geïnformeerd.

De gemeente Buren is op advies van specialisten niet ingegaan op verzoeken tot contact. Naar alle waarschijnlijkheid zou er om losgeld zijn gevraagd. Er is daarover niet met de hackers onderhandeld. Ook omdat de Rijksoverheid zich uitgesproken heeft tegen betaling van losgeld bij datadiefstal.

Identiteitsbewijzen vervangen

Inmiddels is het duidelijk dat er op onze systemen kopieën van 1.331 geldige identiteitsbewijzen stonden. Om ieder risico van misbruik uit te sluiten biedt de gemeente betrokkenen aan om hun identiteitsbewijs kosteloos te vervangen.

Op dit moment zijn er al ruim 1.000 inwoners aangeschreven met het aanbod hun identiteitsbewijs te laten vervangen. De verwachting is dat voor het begin van de zomervakanties er duidelijkheid is voor alle betrokkenen. De hackers zelf hebben aangegeven 5 TB aan gegevens in hun bezit te hebben.

Burgemeester Josan Meijers: “Helaas kunnen we niet uitsluiten dat meer gegevens opduiken op het darkweb. De gemeente is alert op signalen van schendingen van vertrouwelijkheid van gegevens als gevolg van de hack.”

Momenteel wordt gewerkt aan een openbare versie van het onderzoeksrapport.