



College van B&W

Uw contact Meral Aktan

T (020) 540 7189

F (020) 540 7189

m.aktan@amstelveen.nl

AAN
de heer Slump, raadslid

Postbus 4, 1180 BA Amstelveen

Vermeld bij reactie ons kenmerk en datum
van deze brief

Datum 24 december 2024
Uw brief van 17 december 2024
Uw kenmerk n.v.t.
Ons kenmerk Z24-134354

Betreft Schriftelijke vragen van het raadslid de heer Slump van GroenLinks over Hack JCC Software & datalekken

Geachte heer Slump,

Op 17 december 2024 heeft u ons, op grond van artikel 44 Reglement van orde voor de raad van Amstelveen 2024, schriftelijke vragen gesteld over Hack JCC Software & datalekken. In deze brief gaan wij in op de door u gestelde vragen (cursief) met daaronder onze beantwoording.

Onlangs kwam ons ter ore dat in de gemeente Amersfoort een datalek is ontstaan. Onder meer in Computable (10 december 2024 is te lezen dat als gevolg van de hack bij JCC Software de persoonsgegevens van duizenden Amersfoortse burgers op straat zouden zijn komen te liggen.

Data konden naar verluidt weglekken doordat een testserver nog was gekoppeld aan het productiesysteem. Hackers kregen zo een springplank om binnen te dringen en wisten alleen al uit het bestand van de gemeente Amersfoort honderdduizend gewone persoonsgegevens en zeventuizend burgerservicenummers te stelen. Ook de gemeenten Dinkelland en Tubbergen waren dupe van de hack.

1. *Heeft Amstelveen vergelijkbare producten van JCC software draaien?*

Ja, de gemeente Amstelveen neemt meerdere producten af van JCC Software. Het gaat om de volgende (actieve) producten: JCC-bezoekregistratie, JCC-afspraken, JCC-klantgeleiding, JCC-personeelsplanning en JCC-assistent.

2. *Zo ja, is de geschetste situatie en een dergelijk lek ofwel een risico daarop ook op de gemeente Amstelveen voorstelbaar?*

Ja, alhoewel de gemeente maatregelen treft om deze risico's te beheersen, is dit risico nooit uit te sluiten. Wat betreft leverancier JCC Software is in juli 2023 is een Data Protection Impact Assessment (DPIA) uitgevoerd op alle producten van JCC Software die we binnen de gemeente in bezit hebben. Hierin hebben we mogelijke risico's in



kaart gebracht en de mitigerende maatregelen beschreven die genomen moeten worden om de risico's te verkleinen.

De gemeente had reeds, naar aanleiding van deze DPIA in 2023, multifactorauthenticatie (MFA) ingesteld op alle JCC Software-producten. Daarnaast worden persoonsgegevens na 10 dagen geanonimiseerd. Tot slot verwerken we niet meer gegevens dan nodig is in de JCC Software-producten, om zo te voldoen aan het beginsel dataminimalisatie.

Na de hack op 31 oktober 2024 is leverancier JCC Software een nader onderzoek gestart. Op 5 november 2024 zijn we als klant op de hoogte gesteld van het resultaat van het onderzoek middels een brief. Uit het onderzoek van JCC Software is gebleken dat de aanvallers geen andere gegevens in hun bezit hebben gekregen. Tevens heeft JCC Software extra maatregelen getroffen om herhaling te voorkomen.

3. *Zijn er op basis van het gebruik van vergelijkbare producten van andere softwareproducenten dergelijke situaties voorstelbaar in Amstelveen?*

Ja, zie ook antwoord 2. Hoewel de gemeente maatregelen treft om deze risico's te beheersen, is dit risico nooit uit te sluiten. Bij inkoop van software en applicaties vindt vooraf een DPIA (Data Protection Impact Assessment) plaats. Tijdens een DPIA worden de mogelijke risico's geïnventariseerd en van beheersingsmaatregelen voorzien. Deze risico's kunnen echter nooit teruggebracht worden naar nul. (Onontdekte) kwetsbaarheden in software, onbedoelde menselijke handelingen en fouten bij een leverancier kunnen nooit worden uitgesloten. Om deze laatste categorie te beheersen sluiten we met leveranciers een verwerkersovereenkomst af. Hierin staan de normen en maatregelen vermeld waaraan de leverancier moet voldoen om de gegevens van de gemeente veilig te verwerken.

4. *Hebben zich in het afgelopen jaar in Amstelveen vergelijkbare datalekken voorgedaan?*

In het afgelopen jaar hebben twee externe leveranciers een incident bij ons gemeld. Deze incidenten hadden een zeer beperkte impact. Uit onderzoek bleek dat de leveranciers deze incidenten, gezien de geringe impact, niet hoefden te melden bij de Autoriteit Persoonsgegevens (toezichthouder).

5. *Wat zijn de technische voorzorgsmaatregelen die de gemeente Amstelveen genomen heeft, neemt en kan nemen om dergelijke datalekken te voorkomen?*

De gemeente Amstelveen hanteert voor het eigen datacentrum en voor externe leveranciers (inter)nationale standaarden en normen om de gemeentelijke informatie te beveiligen. Deze normen worden ook jaarlijks geaudit door zowel de IT-auditor (tijdens het accountantsonderzoek) als tijdens de jaarlijkse ENSIA-audit. De maatregelen uit deze normenkaders bevatten vele technische, procedurele en personele maatregelen. Voorbeelden van de technische maatregelen zijn onder andere de inzet van multifactorauthenticatie (MFA), firewall, netwerk virtualisatie, MS Defender op werkplek en voor serverbeveiliging, interne netwerk toegangsbeveiliging en mailfiltering. Daarnaast wordt gevoelige informatie via een beveiligd mailsysteem verzonden.

Wij gaan ervan uit u hiermee voldoende te hebben geïnformeerd.



Hoogachtend,
burgemeester en wethouders van de gemeente Amstelveen,
de secretaris, de burgemeester,

Bert Winthorst

Tjapko Poppens

Dit document is elektronisch ondertekend. Zie de elektronische handtekening(en) rechtsboven op pagina 1.

Bijlagen <https://www.computable.nl/2024/12/10/jcc-software-geeft-klassiek-datalek-pas-na-drie-weken-toe/#:~:text=Data%20konden%20weglekken%20doordat%20een,en%20zevenduizend%20burgerservicenummers%20te%20stelen>