Mededeling aan de raad

Van	:	Burgemeester en wethouders
Datum B&W	:	27 januari 2026
Onderwerp	:	Vervolgreactie op toezegging 425: veiligheid van hardware
Portefeuillehouder	:	Jack Werkman
Domein	:	Planning & Control

Kennis te nemen van
De vervolgreactie van het college op toezegging 425: veiligheid van hardware.

Inleiding
In de commissie Samenleving van 8 oktober 2025 is naar aanleiding van het rekenkamerrapport over informatieveiligheid de vraag gesteld hoe wordt omgegaan met de veiligheid van de hardware die wordt gebruikt binnen en rondom het gemeentehuis, evenals de apparatuur die zowel op het gemeentehuis als privé wordt gebruikt. Hierop heeft het college mededeling #2017 naar de raad verzonden.

Naar aanleiding van deze mededelling heeft de fractie VPO per mail richting het college aangegeven dat de mededeling voorbij gaat aan de beveiliging van talloze netwerk-verbonden randapparaten die binnen de gemeentelijke muren opereren. De VPO verzoekt het college om opdracht te geven voor een integrale en onafhankelijke audit, uitgevoerd door een gespecialiseerd extern ICT-beveiligingsbedrijf. De audit moet de gehele digitale infrastructuur van de gemeente omvatten met specifieke aandacht voor inventarisatie en analyse van alle randapparatuur, penetratietesten, firmware en software analyse en netwerkarchitectuur review.

Hieronder vindt u de reactie van het college op dit verzoek.

Kernboodschap
Wij staan positief tegenover onafhankelijke audits, we werken daar graag aan mee en doen dat nu ook al. De onderdelen van een dergelijke audit zoals die benoemd zijn door de fractie VPO doen wij al en/of laten wij uitvoeren en zijn daarmee onderdeel van de reguliere werkzaamheden in de organisatie. Het is daarom niet nodig om nu een extra audit uit te voeren.

Hieronder staan een aantal voorbeelden (niet limitatief):

- Jaarlijks laten wij penetratietesten uitvoeren (norm vanuit de BIO2) waarbij ook een risicoregister wordt opgemaakt waarin de (mogelijke) kwetsbaarheden van software zijn vastgelegd.
- We hebben een externe leverancier die het netwerkbeheer voor ons uitvoert, daarvoor is recent een netwerkarchitectuur review uitgevoerd. Daarnaast is met deze partij afgesproken dat ze meewerken aan audits en pentesten, o.a. ENSIA. Interne audits (maandelijks) en externe audits (halfjaarlijks ISAE3402 en Jaarlijks ISO 27001/BIO) zijn verplicht. Vulnerability scans en rapportages zijn onderdeel van de SLA (overeenkomst).
- Jaarlijks worden de DigiD-aansluitingen door een onafhankelijke IT auditor getoetst.
- Er zijn maatregelen getroffen om IoT-randapparatuur (Internet of Things), zoals printers, onder te brengen in een afzonderlijk netwerksegment zonder enige verbinding naar backend-servers. Deze maatregel volgt uit de bevindingen uit eerder uitgevoerde interne pentesten, waarin onder meer is vastgesteld dat in de oude inrichting printers en andere apparaten toegang hadden tot interne serversegmenten en gebruikmaakten van standaard-SNMP-instellingen, wat onnodige risico's opleverde. Door deze apparatuur te isoleren wordt voorkomen dat kwetsbaarheden in dergelijke systemen misbruikt kunnen worden om toegang te krijgen tot achterliggende infrastructuur.
- Er is een DPIA uitgevoerd over de 365-omgeving, de aanbevelingen die hieruit komen worden opgepakt.
- Elke dag wordt er een back-up gemaakt van onze Microsoft 365-omgeving. Dit doen we o.a. om de continuïteit van het werk te waarborgen. Als er een storing of probleem optreedt, kunnen we gegevens snel terugzetten. Zo voorkomen we dat belangrijke informatie verloren gaat en blijft de

dienstverlening aan inwoners doorgaan. Deze afspraken met de leverancier zijn contractueel vastgelegd en worden periodiek getoetst.

Vervolg

De rapporten van de audits maken wij in het kader van veiligheid nooit openbaar. Natuurlijk nodigen wij u bij vragen graag uit om met een aantal ambtenaren hier verder over door te praten.