PERSBERICHT

REKENKAMER UTRECHT: INFORMATIEVEILIGHEID GEMEENTE UTRECHT NIET GEWAARBORGD ONDANKS INSPANNINGEN

UTRECHT, 7 april 2021 – De gemeente Utrecht is voldoende beschermd tegen inbraken van buiten via internet. Maar van binnenuit loopt de gemeente risico's op het gebied van informatieveiligheid, zo blijkt uit onderzoek van de Rekenkamer Utrecht. Ondanks de maatregelen die de gemeente heeft getroffen om de beveiliging van informatie en gegevens te verbeteren. Er moeten stappen worden gezet met het uitvoeren van risicoanalyses, permanente aandacht van de organisatie en investeringen in informatiebewustzijn en de beveiliging van gebouwen.

Informatie beter beveiligd tegen digitale inbraken van buitenaf dan van binnenuit
Het externe bureau dat de rekenkamer heeft ingehuurd, slaagde er niet in om vanaf het internet (buitenaf) in de gemeentelijke systemen binnen te dringen. Ook de WiFi-netwerken konden deze zogenoemde penetratietests doorstaan. Toch tonen met name de interne tests een aantal hoge en kritieke risico's aan, waarvan een deel al jarenlang bij de gemeente bekend was maar niet verholpen.

De rekenkamer heeft de uitkomsten met de gemeente gedeeld en inmiddels is een deel van de gevonden kwetsbaarheden verholpen. De rekenkamer beveelt de gemeente aan om de nodige maatregelen te nemen tegen de (nog bestaande) technische risico's en kwetsbaarheden. En daarbij de uitkomsten van de penetratietests van het rekenkameronderzoek te benutten.

Structurele investering in informatiebewustzijn en verbetering beveiliging gebouwen nodig
De tests brachten ook risico's aan het licht op het gebied van informatiebewustzijn van medewerkers. Zo bleken 950 medewerkers (16%) in reactie op een phishing-mail hun inloggegevens af te geven. Er werd slechts 477 keer officieel melding gedaan van de (poging tot) phishing, terwijl er in totaal 5.769 e-mails zijn verstuurd. Ook konden onderzoekers van het externe bureau onbevoegd gebouwen van de gemeente betreden en geheime informatie inzien, zonder hierop te worden aangesproken door medewerkers.

De rekenkamer constateert dat er tussen 2018 en het moment van onderzoek geen centraal programma bestond dat was gericht op het informatiebewustzijn van medewerkers. De rekenkamer beveelt dan ook aan om structureel te investeren in het bewustzijn van medewerkers

Stadhuisbrug 1 Utrecht
Postbus 16200, 3500CE Utrecht
030-286 13 91 | utrecht.nl/rekenkamer

over informatieveiligheid, maar ook de procedure voor het melden van beveiligingsproblemen en -incidenten zoveel mogelijk te structureren, verhelderen en breed onder de medewerkers bekend te maken. Ook vindt de rekenkamer het belangrijk dat de beveiliging van gemeentelijke gebouwen wordt verbeterd, om toegang voor onbevoegden te voorkomen.

Risicogestuurd werken vraagt om risicoanalyses en versnelling uitvoering maatregelen
Het beleid van de gemeente Utrecht over informatieveiligheid is volgens de rekenkamer in opzet goed. De gemeente wil risicogestuurd werken en hanteert daarbij een roadmap waarin de te nemen maatregelen over de tijd staan uitgezet. Maar de uitvoering van het beleid loopt achter op de planning. Een groot deel van de tactische en operationele risicoanalyses is bijvoorbeeld nog niet uitgevoerd, waardoor niet alle risico's in beeld zijn.

De rekenkamer beveelt daarom aan om alle benodigde risicoanalyses uit te voeren. Daarnaast adviseert de rekenkamer om de uitvoering van maatregelen in de roadmap te versnellen. En voor verdere maatregelen is het nodig om te leren van eerdere ervaringen en dus na te gaan of eerder genomen maatregelen hebben gewerkt. De gemeenteraad heeft in 2020 extra middelen beschikbaar gesteld voor informatieveiligheid. Daarmee zijn inmiddels extra mensen aangetrokken. Het extra geld en de extra mensen moeten effectief worden ingezet voor de noodzakelijke versnelling van de uitvoering.

Beperkt zicht op informatieveiligheid van thuiswerkplekken medewerkers
Sinds maart 2020 werken de meeste medewerkers van de gemeente Utrecht thuis. De rekenkamer concludeert dat de gemeente niet van alle medewerkers weet in welke mate zij thuiswerken met veilige apparatuur. De gemeente biedt medewerkers een beveiligde virtuele werkomgeving en leent laptops uit, maar slechts 15% van de uitgeleende laptops is voorzien van de juiste beveiliging. Op de beveiliging van privé-apparatuur en WiFi-netwerken thuis heeft de gemeente geen zicht. Ook brengen vergadertools risico's met zich mee, omdat ze buiten de werkomgeving gebruikt moeten worden. Daarom beveelt de rekenkamer de gemeente aan om het toezicht op en de technische beveiligingsmaatregelen voor informatieveiligheid voor thuiswerken te verbeteren.

Noot voor de redactie
Voor meer informatie kunt u contact opnemen met Gerth Molenaar, secretaris van de rekenkamer, tel. 06-49754300. Het rapport en meer informatie over de Rekenkamer Utrecht vindt u op https://www.utrecht.nl/rekenkamer. Mits met bronvermelding (Rekenkamer Utrecht, 2021) kunt u gebruik maken van de figuren uit het rapport (format PDF beschikbaar). Aanvragen via rekenkamer@utrecht.nl.