Voorstel van de rekenkamer

Gemeente Utrecht

Opgesteld door	Rekenkamer
Vergadering	Commissie Mens en Samenleving
Vergaderdatum	@@ 2021
Jaargang en nummer	2021, nr. @@
Geheim	Nee

Rekenkameronderzoek: 'Zo sterk als de zwakste schakel. Een onderzoek naar de informatieveiligheid in de gemeente Utrecht'

De rekenkamer stelt de raad voor te besluiten om het college van burgemeester en wethouders te verzoeken:

1. De benodigde maatregelen te nemen tegen de technische risico's die bekend zijn. En daarbij ook de uitkomsten van (interne en externe) pentesten van het rekenkameronderzoek te benutten.
2. Structureel te investeren in het bewustzijn van medewerkers over informatieveiligheid. Daarbij ook aandacht aan tijdelijke en externe medewerkers te besteden.
3. De procedure voor het melden van beveiligingsproblemen en -incidenten zoveel mogelijk te structureren en verhelderen. Deze breed bekend te maken en (nogmaals) de urgentie ervan te benadrukken.
4. De beveiliging van gemeentelijke gebouwen te verbeteren om de toegang voor onbevoegden te voorkomen.
5. Het uitvoeren van de maatregelen in de roadmap te versnellen. Voor verdere maatregelen is het ook nodig om na te gaan of eerder getroffen maatregelen hebben gewerkt. Daarbij het extra geld voor gegevensbescherming en de uitbreiding van de DISO-capaciteit effectief in te zetten. Ook binnen de organisatieonderdelen te zorgen voor voldoende capaciteit.
6. Alle benodigde risicoanalyses uit te voeren om een totaalbeeld op te kunnen maken van de huidige stand van de risico's. Daarbij de inzet van de extra DISO-capaciteit te benutten.
7. Het toezicht op en de technische beveiligingsmaatregelen voor informatieveiligheid in de thuiswerksituatie te verbeteren.
8. De raad binnen zes weken door middel van een plan van aanpak te informeren over de wijze waarop deze aanbevelingen worden uitgevoerd.

De rekenkamer,

De secretaris,

dr. G. Molenaar

De voorzitter,

drs. P.W.D. Venhoeven

Bijlagen

Rapport '*Zo sterk als de zwakste schakel. Een onderzoek naar de informatieveiligheid in de gemeente Utrecht'.* Rekenkamer Utrecht, 7 april 2021

Eerdere besluitvorming

Uitvoering

Context

Informatieveiligheid is een onderwerp dat met de toenemende digitalisering steeds belangrijker wordt. Gemeenten verwerken grote hoeveelheden gegevens in een veelvoud aan systemen en programma's. Veel van deze gegevens betreffen (bijzondere) persoonsgegevens of andere belangrijke gegevens die goed beschermd moeten zijn. Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude, oplichting en ondermijning op de loer.

Rekenkamer Utrecht heeft onderzoek gedaan naar de informatieveiligheid in de gemeente Utrecht. Het onderzoek is uitgevoerd in de periode september – december 2020. We hebben de relevante beleidsdocumenten, documenten uit de begrotingscyclus en andere raadsinformatie over informatieveiligheid bestudeerd. Voor het inzicht in de risico's die zijn geïdentificeerd en de beheersmaatregelen hebben wij onder andere de risicorapportages van de gemeente ingezien. We hebben tien interviews gehouden met de medewerkers van de gemeente die nauw betrokken zijn bij informatieveiligheid. De testen of het mogelijk was om op een oneigenlijke manier toegang te krijgen tot informatie bij de gemeente zijn uitgevoerd door Hoffmann B.V. We beoordeelden in het onderzoek drie aspecten: (1) organisatie en proces, (2) mens en (3) techniek. Het doel van het onderzoek is de gemeenteraad inzicht geven in de manier waarop de gemeente Utrecht invulling geeft aan de informatieveiligheid en te beoordelen of de informatieveiligheid voldoende is gewaarborgd.

De hoofdconclusie van de rekenkamer is als volgt:

De gemeente Utrecht is voldoende beschermd tegen inbraken van buitenaf. Het lukte de extern onderzoekers namelijk niet om van buitenaf in te breken in de gemeentelijke systemen. Toch tonen interne testen op het gebied van techniek en menselijk handelen risico's aan die het beeld van de informatieveiligheid minder rooskleurig maken. Sommige technische kwetsbaarheden in software en hardware blijven jarenlang bestaan en medewerkers geven in phishing mails hun inloggegevens af. Ook zijn onbevoegde 'inlopers' eenvoudig gemeentelijke gebouwen binnengekomen en hebben zij daar geheime informatie kunnen bemachtigen zonder te zijn aangesproken door medewerkers.

Het beleid om de informatiebeveiliging te verbeteren is in opzet goed. Maar door een combinatie van een gebrek aan personeel, middelen en prioriteit loopt de uitvoering van het beleid achter op de oorspronkelijke planning. Risicogestuurd werken – het uitgangspunt van het beleid – wordt topdown ingevuld en is door het ontbreken van de benodigde risicoanalyses nog niet mogelijk. Daarnaast ontbreekt een centraal programma om medewerkers informatiebewust te maken.

De gemeente Utrecht heeft sinds 2018 al diverse maatregelen getroffen om de informatiebeveiliging te verbeteren. Zo is de governance versterkt, de bemensing uitgebreid en heeft de gemeenteraad in 2020 extra middelen beschikbaar gesteld voor gegevensbescherming. Ook zijn de risico's op het gebied van informatieveiligheid in kaart gebracht. Toch wijzen de testresultaten en de stand van het beleid uit dat er bij de gemeente verbetering noodzakelijk is. De recente voorbeelden van digitale aanvallen op publieke instellingen laten zien hoe kwetsbaar en afhankelijk de samenleving is van digitale middelen. Zeker nu thuiswerken de norm is en de overheid snel (digitaal) moet kunnen handelen. Om te kijken of verbeteracties voortvarend zijn uitgevoerd zal de rekenkamer de informatieveiligheid bij de gemeente Utrecht in de toekomst verder onderzoeken.

De hoofdconclusie met deelconclusies, aanbevelingen en toelichtingen hierop zijn opgenomen in het bestuurlijk rapport. De onderliggende bevindingen zijn na te lezen in de nota van bevindingen. De rekenkamer doet 7 aanbevelingen, die zijn verwoord in de voorliggende beslispunten.

Beslispunt

1. De benodigde maatregelen te nemen tegen de technische risico's die bekend zijn. En daarbij ook de uitkomsten van (interne en externe) pentesten van het rekenkameronderzoek te benutten.

Argumenten

1.1 Uit de testen van het externe bureau om van buitenaf binnen te dringen in de gemeentelijke systemen kwam een zestal kwetsbaarheden naar voren.
1.2 De interne pentesten hebben binnen de beschikbare tijd 17 kwetsbaarheden aangetoond.
1.3 Verschillende kwetsbaarheden waren al langer bekend bij de gemeente, maar (nog) niet opgelost.
1.4 De interne situatie rondom informatieveiligheid kwalificeert de rekenkamer als ernstig.
1.5 Een deel van de gevonden kwetsbaarheden is inmiddels verholpen, maar vanwege de ernst en urgentie moeten alle uitkomsten van het onderzoek benut worden.

Beslispunt

2. Structureel te investeren in het bewustzijn van medewerkers over informatieveiligheid. Daarbij ook aandacht aan tijdelijke en externe medewerkers te besteden.

Argumenten

2.1 Er is bij de gemeente geen centraal programma of plan voor informatiebewustzijn.
2.2 Van 2015-2018 was er wel een centrale bewustwordingscampagne, maar deze is vanwege gebrek aan budget en het vertrek van de projectleider beëindigd. Sindsdien worden er ad hoc acties uitgevoerd.
2.3 De organisatieonderdelen besteden op hun eigen manier aandacht aan informatiebewustzijn. Zo wordt de introductie op het onderwerp informatieveiligheid voorafgaand aan het dienstverband niet organisatiebreed, maar door sommige organisatieonderdelen afzonderlijk ingevuld.
2.4 Ook is de introductie vaak alleen gericht op vaste en niet op tijdelijke of externe medewerkers.
2.5 De gemeente heeft aangegeven te willen intensiveren op dit thema en bereidt sinds oktober 2020 een nieuw centraal bewustwordingsprogramma voor.

2.6 Bij de mail-phishing hebben 950 medewerkers (16%) gebruikersnaam en wachtwoord verstrekt, 121 gebruikers deden dit zelfs na de waarschuwing die door de gemeente is afgegeven na de eerste testdag.

2.7 Vaak heeft een kwaadwillende al aan één combinatie van gebruikersnaam en wachtwoord genoeg om zich toegang te verschaffen tot systemen van de gemeente.

2.8 Uit een mail-phishing simulatie die de gemeente in januari 2020 zelf uitvoerde, bleek ook al dat een deel van de medewerkers niet alert is op pogingen van phishing.

2.9 Tijdens ons onderzoek werd door medewerkers van twee van de vier verspreide USB-sticks de inhoud geopend.

Beslispunt

3. De procedure voor het melden van beveiligingsproblemen en -incidenten zoveel mogelijk te structureren en verhelderen. Deze breed bekend te maken en (nogmaals) de urgentie ervan te benadrukken.

Argumenten

3.1 Het is van belang dat medewerkers melding doen van incidenten.

3.2 Hoe eerder iets door medewerkers gesignaleerd en gemeld wordt, hoe korter een kwaadwillende schade kan aanrichten en hoe sneller verdere stappen kunnen worden voorkomen.

3.2 Bij de mail-phishing test van de rekenkamer werd slechts 477 keer officieel melding van phishing gedaan, terwijl er in totaal 5.769 e-mails zijn verstuurd.

3.3 Meer algemeen geldt dat het aantal meldingen van datalekken tussen 2019 en 2020 is afgenomen. Medewerkers lijken daarom niet altijd te weten wat zij moeten doen bij incidenten zoals mail-phishing en datalekken. De meldingsbereidheid ten opzichte van het totaalaantal beveiligingsincidenten is echter niet te achterhalen.

Beslispunt

4. De beveiliging van gemeentelijke gebouwen te verbeteren om de toegang voor onbevoegden te voorkomen.

Argumenten

4.1 De beveiliging van en sociale controle op het Stadskantoor en het Stadhuis kunnen niet voorkomen dat onbevoegden gemakkelijk en ongestoord binnen kunnen komen.

4.2 Ondanks dat de gemeente aangeeft dat er een open cultuur heerst waarin medewerkers elkaar aanspreken, blijkt uit de voor de rekenkamer uitgevoerde inlooptesten (‘mystery guest bezoek’) dat de onderzoekers niet werden aangesproken op hun aanwezigheid.

4.3 Onderzoekers konden ongestoord dossierkasten openen en informatie inzien. Zij hebben daarnaast een laptop van een medewerker mee kunnen nemen waarop een post-it met bijbehorend wachtwoord was bevestigd. Hierdoor kon eenvoudig toegang worden verkregen tot de laptop.

4.4 De onderzoekers hebben bij deze testen zowel op papier als digitaal geheime informatie kunnen inzien.

Beslispunt

5. Het uitvoeren van de maatregelen in de roadmap te versnellen. Voor verdere maatregelen is het ook nodig om na te gaan of eerder getroffen maatregelen hebben gewerkt. Daarbij het extra geld voor gegevensbescherming en de uitbreiding van de DISO-capaciteit effectief in te zetten. Ook binnen de organisatieonderdelen te zorgen voor voldoende capaciteit.

Argumenten

5.1 Voor de implementatie van het nieuwe beleid is een roadmap opgesteld.
5.2 De gemeente heeft al een aantal algemene maatregelen genomen.
5.3 Ook zijn er in 2020 extra middelen beschikbaar gesteld.
5.4 De uitvoering loopt bij een aantal cruciale onderdelen achter op de oorspronkelijke planning.
5.5 Deze achterstand moet mede worden ingelopen door het extra personeel en de extra middelen die in 2020 beschikbaar zijn gesteld.
5.6 Er is urgentie en daadkracht nodig bij het management en de proceseigenaren, en er is ruimte vereist voor uitvoerende medewerkers om, naast hun reguliere werkzaamheden, aan het uitvoeren van de roadmap te werken.
5.7 In de testen zijn verschillende risico's gevonden die al jaren bij de gemeente bekend waren, maar niet zijn verholpen. Daardoor heeft de gemeente al langere tijd onnodig risico gelopen.
5.8 Sinds 2018 zijn de risico's op het gebied van informatieveiligheid in kaart gebracht en geprioriteerd. Van de in totaal 60 risico's die in 2020 in de ICT zijn geïdentificeerd, staan er januari 2021 nog 24 (40%) open.

Beslispunt

6. Alle benodigde risicoanalyses uit te voeren om een totaalbeeld op te kunnen maken van de huidige stand van de risico's. Daarbij de inzet van de extra DISO-capaciteit te benutten.

Argumenten

6.1 Het uitgangspunt van het nieuwe *Beleid voor gegevensbescherming 2019-2022* is risicogestuurd werken. Om risicogestuurd te kunnen werken is het cruciaal om risicoanalyses en Data Protection Impact Assessments (DPIA's) uit te voeren.
6.2 Het plan is om deze risicoanalyses op alle niveaus – strategisch, tactisch en operationeel – uit te voeren.
6.3 De gemeente werkt sinds 2019 met een strategisch risico-overzicht. Maar van de benodigde 21 tactische risicoanalyses zijn er slechts 6 gereed.
6.4 Op het gebied van privacy zijn ruim 150 DPIA's afgerond, maar de overige operationele risicoanalyses voor informatieveiligheid zijn – met uitzondering van 6 operationele risicoanalyses als pilot bij Stadsbedrijven – nog niet uitgevoerd.
6.5 Omdat risicoanalyses en DPIA's cruciaal zijn om risicogestuurd te werken, is dit nog niet volledig mogelijk.

Beslispunt

7. Het toezicht op en de technische beveiligingsmaatregelen voor informatieveiligheid in de thuiswerksituatie te verbeteren.

Argumenten

7.1 Sinds het begin van de coronacrisis in maart 2020 werkt het merendeel van de medewerkers van de gemeente Utrecht thuis.

7.2 De gemeente Utrecht weet niet van alle medewerkers of zij thuiswerken met veilige apparatuur.

7.3 In februari 2021 waren in totaal bijna 2.500 laptops door de gemeente uitgegeven. Sinds november 2020 worden beveiligde laptops uitgeleverd die beschermd zijn tegen aanvallen op onveilige netwerken en bij diefstal en verlies. Het gaat hier om ongeveer 375 laptops (15%). De bijna 2.100 eerder verstrekte laptops zijn daarentegen niet allemaal voorzien van de juiste beveiligingsmaatregelen. Op een deel van deze laptops is sprake van achterstallig onderhoud: er ontbreekt harddiskencryptie en USB-poorten zijn nog toegankelijk.

7.4 Daarnaast werken medewerkers die geen laptop van de gemeente in bruikleen hebben thuis waarschijnlijk op eigen apparatuur. De gemeente heeft geen zicht op de beveiliging van deze apparatuur, maar biedt medewerkers een beveiligde virtuele werkomgeving aan om zoveel mogelijk te voorkomen dat gegevens lokaal worden opgeslagen.

7.5 De gemeente stelt geen eisen aan de beveiliging van WiFi-netwerken bij mensen thuis.

7.6 Een ander risico op het gebied van thuiswerken ontstaat door het gebruik van vergadertools. De gemeente heeft maatregelen genomen om drie vergadertools zo veilig mogelijk aan te bieden. Deze vergadertools moeten echter buiten de werkomgeving worden gebruikt.

Beslispunt

8. De raad binnen zes weken door middel van een plan van aanpak te informeren over de wijze waarop deze aanbevelingen worden uitgevoerd.

Argumenten

8.1 Bij de formulering van de aanbevelingen heeft de rekenkamer concrete voorstellen gedaan om invulling te geven aan de aanbevelingen en tegelijkertijd ruimte gelaten aan het college om de aanbevelingen nader in te vullen.

8.2 In artikel 11 (lid 8) van de Verordening Rekenkamer Utrecht 2018 is opgenomen dat het college binnen zes weken na besluitvorming over de aanbevelingen van de rekenkamer een plan van aanpak opstelt over de implementatie van de raadbesluiten.

8.3 In artikel 11 (lid 9) is opgenomen dat het college jaarlijks (bij de Jaarstukken) aan de raad rapporteert over de stand van zaken van de uitvoering van de raadsbesluiten die genomen zijn naar aanleiding van rekenkamerrapporten.

8.4 Indien nuttig kan via een expliciet besluit van de gemeenteraad van de standaardtermijn van zes weken worden afgeweken.

Raadsbesluit

Opgesteld door	Raadsorganen
Vergadering	Gemeenteraad
Vergaderdatum	@@ 2021
Jaargang en nummer	2021, nr. @@

Rekenkameronderzoek: ‘Zo sterk als de zwakste schakel. Een onderzoek naar de informatieveiligheid in de gemeente Utrecht’

Besluit:

1. De benodigde maatregelen te nemen tegen de technische risico’s die bekend zijn. En daarbij ook de uitkomsten van (interne en externe) pentesten van het rekenkameronderzoek te benutten.
2. Structureel te investeren in het bewustzijn van medewerkers over informatieveiligheid. Daarbij ook aandacht aan tijdelijke en externe medewerkers te besteden.
3. De procedure voor het melden van beveiligingsproblemen en -incidenten zoveel mogelijk te structureren en verhelderen. Deze breed bekend te maken en (nogmaals) de urgentie ervan te benadrukken.
4. De beveiliging van gemeentelijke gebouwen te verbeteren om de toegang voor onbevoegden te voorkomen.
5. Het uitvoeren van de maatregelen in de roadmap te versnellen. Voor verdere maatregelen is het ook nodig om na te gaan of eerder getroffen maatregelen hebben gewerkt. Daarbij het extra geld voor gegevensbescherming en de uitbreiding van de DISO-capaciteit effectief in te zetten. Ook binnen de organisatieonderdelen te zorgen voor voldoende capaciteit.
6. Alle benodigde risicoanalyses uit te voeren om een totaalbeeld op te kunnen maken van de huidige stand van de risico’s. Daarbij de inzet van de extra DISO-capaciteit te benutten.
7. Het toezicht op en de technische beveiligingsmaatregelen voor informatieveiligheid in de thuiswerksituatie te verbeteren.
8. De raad binnen zes weken door middel van een plan van aanpak te informeren over de wijze waarop deze aanbevelingen worden uitgevoerd.

Aldus besloten in de vergadering van de raad, gehouden op @@

De griffier	De voorzitter gemeenteraad
Merel van Hall	Sharon A.M Dijksma