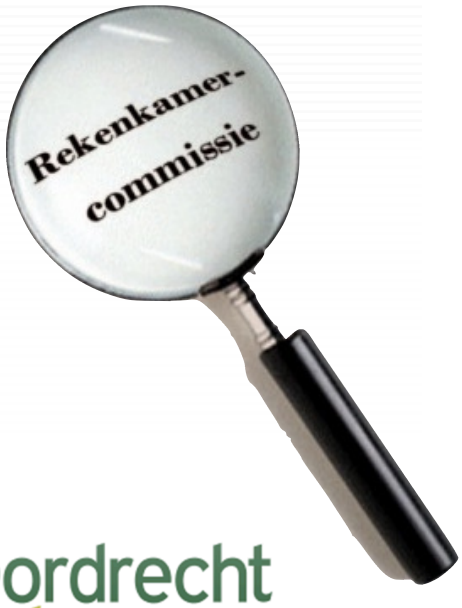
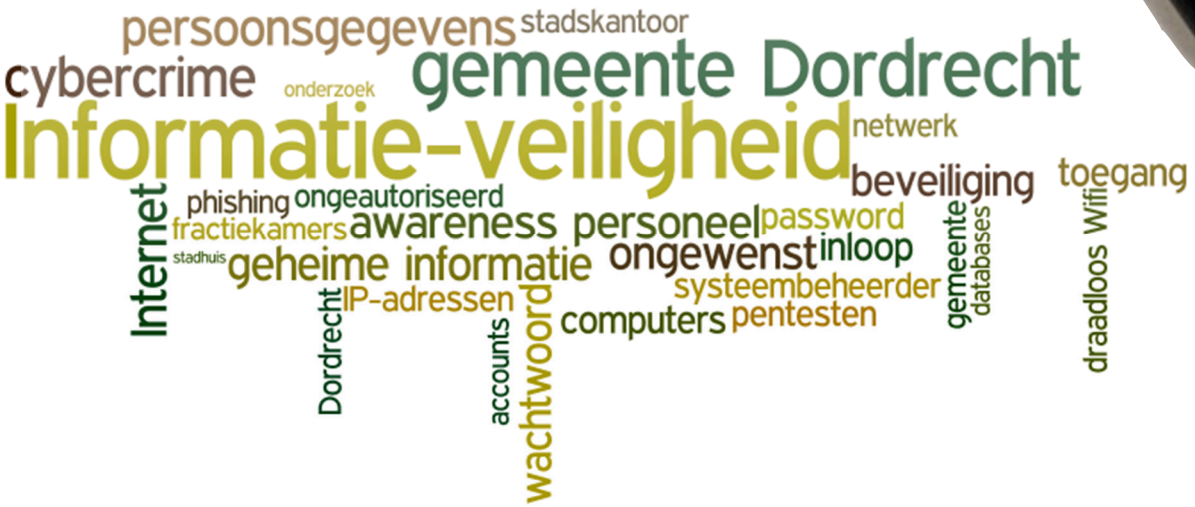
Informatieveiligheid in de gemeente Dordrecht

Bestuurlijke boodschap





COLOFON

Samenstelling
Rekenkamercommissie
Jeroen Kerseboom | voorzitter
Karin Meijer | lid
Coen Cransveld | lid

Secretariaat RKC
Postbus 8, 3300 AA Dordrecht
rekenkamercommissie@dordrecht.nl
dordrecht.nl/rekenkamercommissie

Twitter @RKCDordrecht
www.facebook.com/
rekenkamercommissiedordrecht

Femke Lagerveld | Secretaris
Tel: 078 7704984
E-mail: fm.lagerveld@dordrecht.nl

Sylvia Khadjé | Bestuursassistent
Tel: 078 7704998
E-mail: s.khadje@dordrecht.nl

Dit onderzoek is uitgevoerd door
Hoffmann
Hofmann BV
onder verantwoordelijkheid van de
Rekenkamercommissie

Opmaak | Sylvia Khadjé
Publicatie 29 augustus 2017

Inhoudsopgave

1. Over dit onderzoek

1.1. Inleiding

Bij de uitvoering van overheidsbeleid nemen data een steeds belangrijkere rol in. Bijna alle informatie die de overheid verzamelt, wordt digitaal opgeslagen. Veel van die informatie wordt gekoppeld en gedeeld. Voor een belangrijk deel bevordert dat een vlotte uitvoering van de werkzaamheden. Burgers hoeven hun gegevens bijvoorbeeld nog maar één keer in te vullen. Deze ontwikkeling vraagt wel om aandacht voor de bescherming van de (persoons)gegevens; onbevoegden moet geen toegang tot deze gegevens kunnen krijgen.

Ook de gemeente Dordrecht verzamelt veel informatie (zowel intern als extern). Mede als gevolg van de decentralisaties in het sociaal domein heeft de gemeente steeds meer (bijzondere) persoonsgegevens in beheer.

Recentelijk zijn verschillende gemeenten genoodzaakt geweest om datalekken te melden bij de Autoriteit Persoonsgegevens. Daarnaast bleek uit verschillende recente rekenkameronderzoeken dat de beveiliging van gemeentelijke datasystemen soms te wensen overlaat (Rotterdam, Den Haag, Arnhem). Deze voorbeelden leren dat ook lokale overheden zich weerbaar moeten maken tegen dreigingen als cybercrime. Alleen privacy-wetgeving is onvoldoende om de privacy van burgers te beschermen. Daarvoor moeten overheden ook zorgen voor een adequate beveiliging van hun ICT systemen. Die beveiliging dient te bestaan uit zowel adequaat opererende computersystemen, als een organisatie waarin medewerkers zich bewust zijn van hun rol in het bewaken van de toegang tot die systemen.

1.2. Vraagstelling

Met deze ontwikkelingen in het achterhoofd heeft de rekenkamercommissie Dordrecht een onderzoek laten uitvoeren naar de kwaliteit van de beveiliging van de (vertrouwelijke) informatie van de gemeente Dordrecht. Drie vragen stonden hierin centraal:

- Zijn de gegevens van de gemeente Dordrecht in de praktijk voldoende beschermd tegen toegang door onbevoegden via het internet en via de fysieke gebouwen van de gemeente?
- Wat zijn de risico’s en kwetsbaarheden bij de gebouwen, systemen en gedragingen van medewerkers of leveranciers?
- Welke passende beveiligingsmaatregelen zijn er mogelijk om de beveiliging te optimaliseren?

1.3 Aanpak

De informatiebeveiliging van de gemeente Dordrecht is met behulp van een zogenaamde pentest ('penetratietest') onderzocht door het in dit soort testen gespecialiseerde onderzoeksbureau Hoffmann BV. De pentest was als volgt opgebouwd:

- Een externe pentest, waarbij de onderzoekers zonder enige voorkennis de aan het internet gekoppelde systemen van de gemeente Dordrecht onderzochten op kwetsbaarheden en hebben getracht deze te misbruiken;
- Een interne pentest, waarbij de onderzoekers zonder enige voorkennis interne systemen onderzochten op kwetsbaarheden en getracht hebben kwetsbaarheden te misbruiken. Hierbij is gebruik gemaakt van een door de gemeente ter beschikking gestelde netwerkaansluiting op een tweetal werkplekken;
- Een spear phishing test, waarbij de onderzoekers een medewerker van de gemeente, via e-mails, hebben getracht te bewegen tot het uitvoeren van een handeling, zoals het klikken op een link of het inschakelen van een script, waardoor de onderzoekers toegang zouden kunnen verkrijgen tot het systeem;
- Een inlooptest, waarbij de onderzoekers zonder vooraankondiging hebben getracht de niet-publiekelijke ruimten van de gemeente te betreden.

1.4 Reikwijdte van het onderzoek

Bij de start van het onderzoek bleek het niet mogelijk om een duidelijk om overzicht te ontvangen van systemen die in beheer zijn bij de gemeente Dordrecht. Dit heeft onder andere te maken met de samenvoeging van het netwerk van de Drechtstedengemeenten. Op basis van een door de gemeenten aangeleverde lijst met URL's is de precieze scope van dit onderzoek bepaald, zodat alleen de systemen van de gemeente Dordrecht daarbinnen vielen.[1]

1.5 Testperiode

De pentest heeft plaatsgevonden in de periode van 11 december 2016 tot en met 30 december 2016. Daarbij zijn de interne testen uitgevoerd op 14 tot en met 16 december 2016, de inlooptesten op 16 en 20 december 2016 en de externe pentest en de spear phishing over de gehele periode

[1] Het iBabs-systeem, dat onder andere de vergaderstukken van de gemeenteraad bevat, is buiten het onderzoek gelaten omdat dit systeem bij een externe leverancier is ondergebracht.

1.6 Disclaimer

Vanwege de kritieke bevindingen die ons onderzoek heeft opgeleverd, hebben we de gemeentelijke organisatie enige tijd gegeven om de nodige reparaties uit te voeren.

Naar aanleiding van dit onderzoek valt echter niet uit te sluiten dat niet iedere kwetsbaarheid in de IT-infrastructuur daadwerkelijk is gedetecteerd. Het onderzoek is immers uitgevoerd met een budget- en tijdslimiet. Daarnaast worden (met het verschijnen van software updates om kwetsbaarheden te reduceren) ook regelmatig nieuwe kwetsbaarheden ontdekt. Honderd procent zekerheid is nooit te geven en daarom is het verstandig om periodiek een soortgelijk onderzoek als dit te herhalen.

2 Conclusies

De belangrijkste conclusie uit dit onderzoek is dat het relatief eenvoudig bleek om fysiek toegang te krijgen tot het niet-publieke deel van het stadskantoor, om vervolgens een eigen laptop aan te sluiten op het interne netwerk van de gemeente, via een van de vele netwerkaansluitingen in het stadskantoor. Eenmaal aangesloten, kon ook relatief eenvoudig toegang worden verkregen tot alle accounts van medewerkers van de gemeente Dordrecht, inclusief die van de systeembeheerders. Dat betekent dat toegang kon worden verkregen tot alle computers in het stadskantoor en dat alle handelingen die vanaf Dordtse accounts werden gedaan niet alleen konden worden ingezien, maar ook gewijzigd.

Moeilijker bleek het om van buitenaf, vanaf het internet, zonder voorkennis en binnen een korte tijd, volledige toegang te verkrijgen tot systemen van de gemeente Dordrecht. Dat wil echter niet zeggen dat dit niet mogelijk is. Hetzelfde geldt voor het draadloze wifi-netwerk van de gemeente: de onderzoekers slaagden er niet in om hier ongeautoriseerd toegang tot te krijgen.

Hieronder lichten we de bevindingen kort toe.

2.1 Externe pentest

Tijdens het vooronderzoek hebben de onderzoekers een groot aantal webapplicaties, IP-adressen en IP-ranges aangetroffen die gelinkt kunnen worden aan de gemeente Dordrecht. De externe pentesten zijn beperkt gebleven tot een beperkte range van IP-adressen waarvan zeker was dat de gemeente Dordrecht eindverantwoordelijke was. Hierbij zijn IP-adressen die behoren tot Drechtsteden expliciet buiten beschouwing gelaten.

De onderzoekers zijn er zonder voorkennis en binnen de beschikbare tijd niet in geslaagd om vanaf het internet volledige toegang te verkrijgen tot systemen van de gemeente Dordrecht. Vanaf het internet was het echter wel mogelijk om toegang te krijgen tot een database die onder andere persoonsgegevens bevat.

Bij de externe pentest bleek een database achter een website gevoelig voor een zogenaamde “Blind SQL injectie” waardoor de database toegankelijk gemaakt kan worden. Dit lek is inmiddels gedicht. Ook heeft men inlogschermen aangetroffen die over een niet-beveiligde verbinding communiceerden.

2.2 Interne pentest

Bij de interne pentest hebben onderzoekers met meegebrachte systemen (laptops) getracht ongeautoriseerd toegang te krijgen tot systemen en gegevens via twee flexwerkplekken met netwerkaansluiting. Eenmaal toegang tot het interne netwerk, bijvoorbeeld vanaf een flexplek op het stadskantoor, lukte het de onderzoekers binnen korte tijd om beheerrechten te verkrijgen op alle Windows systemen binnen een bepaald domein. Hierdoor werd alle informatie waar beheerders toegang toe hebben toegankelijk:

- Bij deze tests is een groot aantal systemen en applicaties aangetroffen dat niet meer wordt ondersteund door de leverancier en/of waarvoor beschikbare beveiligingsupdates niet bleken te zijn toegepast.

- Doordat hashes (cryptografische versleutelingen) en wachtwoorden vaak in het geheugen achterblijven als gebruikers inloggen op systemen bleek het mogelijk om wachtwoorden van beheerders te verzamelen en deze te hergebruiken op andere systemen.
- Voor verschillende diensten bleek geen wachtwoord vereist te zijn of bleken er standaardwachtwoorden gebruikt te worden.
- Er is een FTP-server (= een server die gebruikt wordt om bestanden tussen computers uit te wisselen via het zogenaamde file transfer protocol) aangetroffen waarop niet werd gecontroleerd op logingegevens.
- Er zijn enkele webcams aangetroffen die vrij toegankelijk zijn, er was geen gebruikersnaam en wachtwoord voor nodig.
- Diverse printers waren op het interne netwerk toegankelijk door het ontbreken van een beveiliging.

Bij de interne pentesten zijn ook de draadloze (WiFi-)netwerken onderzocht. De onderzoekers zijn er niet in geslaagd om ongeautoriseerde toegang (zonder wachtwoord) te verkrijgen of andere systemen op deze netwerken succesvol aan te vallen.

2.3 Spear phishing test

De onderzoekers hebben een tweetal “spear phishing” (specifiek aan bepaalde werknemers gerichte) e-malis verstuurd. Het ging om gepersonaliseerde e-mails die trachten de ontvanger te verleiden om kwaadaardige links te volgen of bestanden te openen.
Deze tests hebben geen toegang opgeleverd. Hierbij wordt wel aangetekend dat het mogelijk is dat de e-mails zijn tegengehouden door een Antivirus-oplossing.

2.4 Inlooptest

Gelet op de geconstateerde kwetsbaarheden bij de interne pentest, is het zaak om onbevoegden buiten de niet-publieke ruimten van het stadskantoor en het stadhuis te houden. De onderzoekers hebben op twee locaties (Stadskantoor en Stadhuis) ongeautoriseerde toegang verkregen tot gemeentelijke panden.

Op het *stadskantoor* is een onderzoeker, zonder gebruik te maken van een toegangspas, achter een medewerker aan door de personeelsingang/tourniquets gelopen (deze techniek staat ook bekend als “tailgating”). Aansluitend heeft de onderzoeker verschillende etages betreden. In het *stadhuis* waren de raadszaal en de gangen waar de fractiekamers aan grenzen vrij toegankelijk. De fractiekamers zelf waren niet toegankelijk. De onderzoekers schatten het risicobewustzijn van de tijdens de inlooptest in beide panden aanwezige personen in als onvoldoende.

3. Aanbevelingen

3.1 Aanbevelingen aan de raad

1. Bespreek met het college wanneer u welke informatie over informatieveiligheid (binnen de gemeente en bij samenwerkende partijen) van het college verwacht.
2. Bespreek met het college of u voldoende informatie ontvangt over privacybescherming en welke informatie u hierover verder van het college nodig acht.
3. Investeer voldoende in cybersecurity.
4. Vraag aan het college een kadernota over informatieveiligheid en laat deze ter besluitvorming voorleggen aan de raad.
5. Vraag aan het college of er een calamiteitenplan is opgesteld voor ingrijpen bij aanvallen op de informatiebeveiliging.
6. Overweeg om in een volgende collegeformatie bij de portefeuilleverdeling rekening te houden informatiebeveiliging apart te benoemen (en niet als sub onderwerp van ICT).

3.2 Aanbevelingen aan het college

1. Verhelp de aangetroffen technische kwetsbaarheden op korte termijn en laat een hertest uitvoeren om de effectiviteit van de genomen maatregelen te toetsen.
2. Voer op regelmatige basis kwetsbaarhedenscans uit in samenwerking met andere Drechtsteden en instanties die gekoppeld zijn aan de IT-infrastructuur
3. Voer met enige regelmaat pentesten uit door onafhankelijke derden, op alle IP-adressen waar de gemeente Dordrecht eindverantwoordelijke voor is.
4. Toets regelmatig of medewerkers (en leveranciers) voldoende weerbaar zijn, gewenst gedrag vertonen en waar nodig interventies plegen op het vlak van mens, organisatie en/of techniek om daadwerkelijk verbeteringen te bevorderen.
5. Breng alle webapplicaties en systemen die met het Internet verbonden zijn en die gelinkt kunnen worden aan de gemeente Dordrecht in kaart. Alleen dan kan tijdig imagoschade worden voorkomen in geval van misbruik.
6. Een groot gedeelte van de technische aanbevelingen die betrekking hebben op de kwetsbaarheden die voort zijn gekomen uit de technische scans kan eenvoudig worden opgelost door:

    - Systemen tijdig voorzien van beveiligingsupdates;
    - Het uitschakelen van kwetsbare en/of ongebruikte component(en);
    - Systemen te “hardenen” en voorzien van sterke onvoorspelbare wachtwoorden; Componenten af te schermen door middel van firewalls en Access Control Lists op netwerkapparatuur.

4. Bestuurlijke reactie

DORDRECHT

Retouradres: Postbus 8 3300 AA DORDRECHT

Aan

de voorzitter Rekenkamercommissie
de heer J.S. Kerseboom
Postbus 8
3300 AA DORDRECHT

Gemeentebestuur
Spuiboulevard 300
3311 GR DORDRECHT

T 14078
F (078) 770 8080
www.dordrecht.nl

Contactpersoon
M.C.A. Bakx /
J.D.H. Verschoor
T (078) 770 3912 /
(078) 770 4177
E mca.bakx@dordrecht.nl /
jdh.verschoor@dordrecht.nl

Datum 11 juli 2017
Ons kenmerk SBC/1888804
Betreft Rekenkamercommissiebrief onderzoek Informatieveiligheid

Geachte heer Kerseboom,

Wij hebben met belangstelling kennis genomen van uw rekenkamercommissiebrief en de hierin opgenomen conclusies en aanbevelingen. Het verheugt ons dat de rekenkamercommissie dit onderwerp onder de loep heeft genomen en beseft dat informatie in algemene zin en informatieveiligheid in het bijzonder een steeds grotere rol speelt in het efficiënter en effectiever handelen van onze gemeente. Informatieveiligheid is een randvoorwaarde voor ons handelen geworden.

Uw onderzoek onderstreept voor ons het belang van een helder en krachtig informatie(veiligheids)beleid. De belangrijkste conclusie uit uw onderzoek, dat het relatief eenvoudig is om fysiek toegang te krijgen tot het niet-publieke deel van het stadskantoor is een punt van zorg dat onze aandacht heeft. Wij nemen dit mee in het door ons ingezette informatie(veiligheids)beleid. Het stemt ons positief dat de onderzoekers vanaf het internet en onze wifi-voorziening geen toegang hebben kunnen krijgen tot systemen van de gemeente Dordrecht. Ook geeft uw onderzoek aan dat er in onze fysieke ICT omgeving en op het vlak van bewustwording nog kwetsbaarheden zijn geconstateerd.

U geeft het college van B&W zes aanbevelingen mee. Wij nemen deze aanbevelingen integraal over En werken de aanpak verder uit in een implementatieplan. Wel willen we met nadruk vermelden dat de maatregelen voor de aanbevelingen met een hoge prioriteit inmiddels al zijn doorgevoerd om beveiligingsincidenten te voorkomen.

Wij danken u voor het onderzoek en hopen met deze bestuurlijke reactie op een goede manier aan uw aanbevelingen tegemoet te zijn gekomen.

Hoogachtend,

Het college van Burgemeester en Wethouders
de secretaris de burgemeester

M.M. van der Kraan P.A.C.M. van der Velden

5. Nawoord

Voorkomen is beter dan genezen. Dat geldt ook voor het beveiligen van de informatie waar de gemeente Dordrecht de beschikking over heeft, en voor de uitwisseling van de informatie in Drechtstedenverband. Het is van belang om periodiek de informatieveiligheid van de verschillende systemen te onderzoeken en eventuele kwetsbaarheden op te sporen en te verhelpen, voordat cybercriminelen die vinden.

We nemen met instemming kennis van de reactie van het college op onze bevindingen en van het feit dat het college onze aanbevelingen integraal overneemt. Wij hopen een verbetering te zien in de dagelijkse praktijk bij het bewustzijn van de medewerkers. Voortdurende alertheid is noodzakelijk, gegeven de nieuwe technische mogelijkheden en de kansen en bedreiging die deze met zich meebrengen.

We wijzen in dit verband op de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG) die op 25 mei 2018 in werking treedt. De Autoriteit Persoonsgegevens kan forse boetes opleggen bij het niet nakomen van de uit de AVG voortvloeiende verplichtingen of bij het overtreden van beginselen of grondslagen van de AVG.