de hackende rekenkamer

De impact van een onderzoek naar Informatiebeveiliging

Rekenkamer Rotterdam

PAS conferentie 2 november 2017

Landelijke impact

deVolkskrant

Beveiliging Aboutaleb al jaren onnodig zwak

Willem Feenstra, Huib Modderkolk
Amsterdam

Burgemeester Ahmed Aboutaleb van Rotterdam loopt al jaren een onnodig groot veiligheidsrisico. Ondanks eerdere waarschuwingen verzuimt de gemeente gaten in zijn digitale beveiliging te dichten. Daardoor kunnen kwaadwillenden relatief eenvoudig achterhalen waar Aboutaleb van uur tot uur is. Dit is een van de conclusies uit een nog niet gepubliceerd rapport van de Rotterdamse Rekenkamer, dat in handen is van *de Volkskrant*.

Aboutaleb heeft als mogelijk doelwit van terroristen al jaren persoonlijke beveiliging. Zijn agenda is daarom geheim. Door de tekortschietende informatiebeveiliging, *zoals onversleutelde harde schijven* en verouderde software, kunnen hackers beheerdersrechten krijgen en daarmee toegang tot gevoelige informatie.

Dit leidt volgens de Rekenkamer tot 'reële risico's op fysieke onveiligheid' van Aboutaleb en andere Rotterdamse politici. Daarnaast zouden veiligheidsprotocollen voor evenementen die de burgemeester via mail ontvangt kunnen worden misbruikt om zwakke plekken in de beveiliging op te sporen.

Met name de stevige conclusies over de kwetsbaarheid van Aboutaleb zijn pijnlijk. Twee jaar geleden constateerde beveiligingsbedrijf Fox-IT al dat er gaten zitten in de digitale beveiliging van de burgemeester. Toch zou er weinig tot niets zijn verbeterd. 'Dat dit niet heeft plaatsgevonden, neemt de Rekenkamer de gemeente erg kwalijk', aldus het rapport.

Het Rotterdamse college verzet zich tegen publicatie van het rapport. Afgelopen weekend dreigde de gemeente met een gang naar de rechter als de Rekenkamer openbaarmaking in de huidige vorm zou doorzetten. De Rekenkamer stelde daarop de publicatie uit tot volgende week.

In een schriftelijke reactie laat de gemeente Rotterdam weten niet in te gaan op 'een rapport dat niet openbaar is'. 'Deze week is er een gesprek tussen de gemeente en de Rekenkamer over het – tijdelijk – niet openbaar maken van onderdelen van het rapport in verband met mogelijke risico's voor de Rotterdammers en onze medewerkers', aldus de gemeente.

Rapport van Rotterdamse Rekenkamer hekelt uitblijven van verbeteringen in digitale beveiliging

PAGINA 8-9
De grootste 4 lekken van Rotterdam: wat staat er in het Rekenkamerrapport?

Vorig jaar lekten de persoonsgegevens van duizenden Rotterdammers uit door datalekken bij de gemeente. Het probleem speelt in veel gemeenten: door toenemende digitalisering hebben gemeenten steeds grotere databestanden. De beveiliging daarvan loopt achter op de toename van gevoelige data in handen van de gemeente, mede doordat zij digitalisering als bezuiniging zien en geen geld vrijmaken voor training in de omgang met gevoelige data, geheimhouding, inhuur van kennis en autorisatieprocessen.

Naar aanleiding van het Rotterdamse datalek deed de Rekenkamer onderzoek naar de informatiebeveiliging van de stad. Daaraan blijkt veel te schorten. Zo wisten hackers eenvoudig toegang te krijgen tot vier gemeentelijke gebouwen en achterhaalden ze beheerdersrechten, waarmee nagenoeg alle systemen toegankelijk zijn.

Uit het rapport blijkt hoeveel schade hackers in Rotterdam kunnen aanrichten. 'Door toegang te hebben tot informatiesystemen kunnen bijvoorbeeld bruggen en verkeerslichten op afstand bediend worden en het verkeer worden lamgelegd', aldus de Rekenkamer. 'Dat kan vandalisme zijn, maar ook met het doel van ontwrichting worden gedaan.'

Volgens hoogleraar computerbeveiliging Bart Jacobs heeft de gemeente Rotterdam 'een heel groot probleem'. 'De geconstateerde tekorten zijn ernstig en wijzen op structurele problemen bij de inrichting van ict en de houding van gebruikers. Daarmee overtreedt de gemeente de wet persoonsgegevens.'

De Rekenkamer wil niet inhoudelijk op het rapport ingaan, omdat het nog niet officieel is gepresenteerd.

Succesfactoren onderzoek met impact

- Actuele en relevante onderwerpen
- Kwaliteit van het onderzoek
- Geluk
- Vasthoudendheid
- Media aandacht

aanleiding onderzoek rekenkamer

- steeds meer gevoelige informatie bij gemeenten
- toenemende aandacht voor privacy
- digitale veiligheid weinig bestuurlijke aandacht
- datalek in Rotterdam (en Oegstgeest)
- verzoek gemeenteraad aan rekenkamer

insteek onderzoek rekenkamer

- opzet
- bestaan
- werking: concrete testen

opzet IB (papier) in orde

- risicomanagement
  → risicoanalyses
  → pia's
  → maatregelen
- dataclassificaties
- PDCA-cyclus
- BIG

maar gebrekkig bestaan

- geen systematische en actuele risicoanalyses
  → weet niet welke maatregelen nodig zijn
- dataclassificaties niet volledig
  → onbekend welke gegevens kwetsbaar voor misbruik
- voorgeschreven PDCA-cyclus niet gevolgd
  → gevolg: onvoldoende monitoring; kan niet van fouten leren
- grote verschillen in kwaliteit beveiliging kroonjuwelen
- IB uiteindelijk geen ”chef sache”

en werking dan?

verschillende testen:

- externe penetratietest
- interne penetratietest
- inlooptesten
- social engineering

door wie uit te voeren?

specialistische expertise:

- inhuur extern bureau
- verantwoordelijkheid bij rekenkamer
- rekenkamer aanspreekbaar

door wie uit te voeren?

specialistische expertise:

- inhuur extern bureau
- verantwoordelijkheid bij rekenkamer
- rekenkamer aanspreekbaar

externe penetratietest

hoe:

- vanaf internet (“zolderkamer”)

mogelijke kwetsbaarheden:

- niet-versleutelde websites
- verouderde webmailinstallaties
- lekkende systemen

interne penetratietest (1)

hoe:

- vanaf binnenuit
- zonder kennisgeving vooraf
- vrijwaringsverklaring!

interne penetratietest (2)

700 kwetsbaarheden, waarvan 46 uniek, zoals:

- geen netwerkauthenticatie
- onvoldoende filtering netwerk
- niet versleutelde werkstations
- verouderde systemen en applicaties

inlooptesten (1)

hoe:

- ongeautoriseerd fysiek toegang proberen te verkrijgen
- vrijwaringsverklaring!

inlooptesten (2)

- in elk pand ongeautoriseerd toegang
- vervolgens toegang tot gevoelige informatie en ruimtes
- geen enkele keer aangesproken (soms zelfs begeleid)

social engineering (1)

hoe:

- besmette usb-sticks achterlaten (in combinatie met inlooptesten)
- spear phishing

social engineering (2)

- aantal usb-sticks geopend
- verdachte link met spear phishing werd geopend (maar geen schade)

concluderend

- **combinatie van :**
  - tekortschietende beveiliging aanvallen van binnenuit
  - falende fysieke beveiliging kantoorlocaties
  - tekort “awareness” medewerkers

- **daardoor reële risico’s op:**
  - identiteitsfraude
  - fysieke onveiligheid ambtsdragers
  - verstoring openbare orde
  - verstoring publieke dienstverlening
  - misbruik publieke middelen

openbaar maken of niet?

college: niet openbaar, want

- brengt hackers op ideeën
- gebruiksaanwijzing voor hackers
- beroep op principe responsible disclosure

rekenkamer: wel openbaar, want

- testmethoden volkomen gangbaar en bekend
- gebreken waren al jaar bekend
- burgers hebben recht op deze informatie
- brengt extra urgentie in verhelpen gebreken
- bovenal: Gemeentewet vereist openbaarheid

afloop

- kort geding van baan, na lek in Volkskrant
- raad neemt alle conclusies en aanbevelingen over
- investeringsplan € 3 mln.
- hertest eind 2017