



Van: Archana Ramkhelawan

Telefoon: 14 010

Uw kenmerk: 22bb007152

Ons kenmerk: M2211-452 - 22bo006668

Bijlage(n): 1

Onderwerp: Bescherm leden bibliotheek tegen
identiteits- of financiële fraude

Datum: B&W 22november 2022

Aan de gemeenteraad

Op 2 november 2022 stelden D.A. van Groningen - de Haas (VVD), R.G.C. Segers-Hoogendoorn (CDA Rotterdam) en S. Soytekin (DENK) ons schriftelijke vragen over het beschermen van leden Bibliotheek Rotterdam tegen identiteits- of financiële fraude.

Inleidend wordt gesteld:

'De bibliotheken in Rotterdam hadden in de week van 17 oktober een week lang storing. Daar hebben het CDA Rotterdam afzonderlijk en vervolgens DENK met het CDA Rotterdam al schriftelijke vragen over gesteld. Nu bericht RTV Rijnmond1 dat deze storing een cyberaanval betrof en criminelen hiermee persoonlijke gegevens van Rotterdammers hebben buit gemaakt, waaronder adressen en bankrekeningnummers. De bibliotheek waarschuwt dat mensen waarvan hun persoonlijke gegevens zijn gestolen, slachtoffer kunnen worden van identiteits- of financiële fraude. DENK, het CDA en VVD Rotterdam maken zich grote zorgen en stellen daarom bij deze aanvullende schriftelijke vragen.'

Hieronder volgen de vragen en onze beantwoording:

Vraag 1:

Kan het college uitleggen wat de (financiële en machts)relatie is tussen de gemeente en de bibliotheek Rotterdam? Wat betekent dat voor de zeggenschap dat de gemeente Rotterdam heeft over de werkwijze en de veiligheid van de bibliotheken in Rotterdam?

Antwoord:

Bibliotheek Rotterdam is een zelfstandige stichting, die wordt gesubsidieerd door gemeente Rotterdam. De subsidie dient tot uitvoering van het meerjarenbeleidsplan dat door het college is vastgesteld. Het meerjarenbeleidsplan is gebaseerd op de uitgangspunten voor het meerjarenbeleid, zoals door de gemeenteraad vastgesteld. Het college heeft, conform de statuten van Bibliotheek Rotterdam, de bevoegdheid tot het benoemen van leden van de Raad van Toezicht. Als zelfstandige stichting draagt Bibliotheek Rotterdam een eigen verantwoordelijkheid voor de operationele werkwijze en veiligheid van bibliotheken in Rotterdam.



Tevens wordt gesteld:

'Wij ontvangen signalen dat nog niet alle leden van de bibliotheek op de hoogte zijn gesteld van het voor hen mogelijke gevaar van identiteitsfraude of financiële fraude.'

Vraag 2:

Kan het college achterhalen of de bibliotheek alle mensen die mogelijk gevaar lopen om slachtoffer te worden van identiteitsfraude of financiële fraude op de hoogte heeft gesteld? Zo nee, waarom niet? En als blijkt dat dit niet het geval is, de bibliotheek hulp aanbieden in de communicatie hierover? Zo nee, waarom niet?

Antwoord:

Bibliotheek Rotterdam doet onderzoek naar de gestolen data, om ervoor te zorgen dat de juiste mensen worden geïnformeerd. Tijdens het onderzoek zijn meerdere groepen gedupeerden gedefinieerd van wie er data zijn ontvreemd, variërend van alleen een gelekte naam tot een groep met uitgebreide NAW-gegevens. De bibliotheek heeft zich ingespannen en blijft zich inspannen om alle getroffen personen te informeren en te adviseren in het nemen van preventieve maatregelen om cybercriminaliteit te voorkomen. Bibliotheek Rotterdam heeft inmiddels een grote groep getroffen personen geïnformeerd.

Vraag 3:

Volgens RTV Rijnmond heeft de bibliotheek Rotterdam een speciaal emailadres aangesteld voor het stellen van vragen over deze hack. Het medium deelt dat mailadres niet. Kan de gemeente de bibliotheken helpen in de communicatie wat betreft dit e-mailadres, zodat alle leden van de bibliotheek hiervan op de hoogte zijn? Zo nee, waarom niet? Ouderen beschikken niet altijd over een e-mailadres. Kan de gemeente bij de bibliotheek aandringen dat ook een telefoonnummer voor vragen betreffende de hack noodzakelijk is en ook in de communicatie hiervan haar hulp aanbieden? Zo nee, waarom niet?

Antwoord:

Bibliotheek Rotterdam heeft het e-mailadres, dat RTV Rijnmond niet bekend heeft gemaakt, gedeeld met haar leden middels een brief. Inhoud uit de brief is terug te vinden via: [Bibliotheek Rotterdam getroffen door cyberaanval - De Bibliotheek Rotterdam](#). Via dit e-mailadres privacy@bibliotheek.rotterdam.nl kunnen leden contact opnemen met de Functionaris Gegevensbescherming. De klantenservice is nu en was tijdens de hack, telefonisch bereikbaar voor het beantwoorden van vragen.

Vraag 4:

Kan het college aangeven wat de gemeente Rotterdam kan en gaat doen om de internetveiligheid van haar burgers die lid zijn van de bibliotheek Rotterdam te garanderen? Zo nee, waarom niet?

Antwoord:

Bibliotheek Rotterdam is zelf verantwoordelijk voor de digitale veiligheid van hun eigen systemen en netwerken. Bibliotheek Rotterdam geeft aan dat er altijd veel aandacht geweest is bij de bibliotheek voor de veiligheid van de systemen. Men werkt o.a. regelmatig met externe adviseurs en ethical hackers om dit soort aanvallen te voorkomen. De bibliotheek werkt volgens strakke veiligheidsprotocollen. Doorlopend wordt het beveiligingsniveau van de systemen geoptimaliseerd; daarmee probeert men criminelen voor te zijn. Alle systemen voldoen volgens Bibliotheek Rotterdam aan de huidige veiligheidseisen. Daarnaast organiseert gemeente Rotterdam diverse projecten en campagnes op cyberveerbaarheid voor Rotterdamse burgers. Hierin werken wij



regelmatig samen met Bibliotheek Rotterdam. Op 24 november organiseren we samen een theatervoorstelling ter bewustwording op digitale criminaliteit bij senioren om slachtofferschap te voorkomen. Volledige internetveiligheid is niet te garanderen, daarom is het van essentieel belang dat wij als gemeente blijven inzetten op de digitale weerbaarheid van onze stad, haven, inwoners en ondernemers.

Vraag 5:

Nu blijkt dat de bibliotheek Rotterdam gehackt kan worden, zijn het CDA, Denk en VVD Rotterdam ook bezorgd over de kwaliteit van de cyberveiligheid bij de gemeente zelf en de gevolgen daarvan in de toekomst. Wil het college de kwaliteit van de cyberveiligheid van de gemeente Rotterdam checken door ethische hackers te laten proberen haar systemen aan te vallen? Zo nee, waarom niet?

Antwoord:

De gemeente Rotterdam zet zich in om een gezonde balans te houden tussen investeringen en cyberveiligheid. Vanuit het oogpunt van informatiebeveiliging werken we er altijd aan om onze cyberweerbaarheid zo hoog mogelijk te houden binnen het steeds veranderende en complexe cyber dreigingslandschap. Als gemeente Rotterdam voeren wij verschillende audits uit op onze ICT-omgeving. We gebruiken het om onze technische, procedurele en organisatorische maatregelen te testen en eventuele verbeteringen te identificeren en te implementeren. In samenwerking met landelijke organisaties als NCSC (National Cyber Security Center) en IBD (Information Security Services van VNG) streven wij er voortdurend naar om cybercriminelen voor te blijven. Als gemeente werken we al geruime tijd samen met ervaren externe partners op het gebied van security en hebben een SOC (Security Operations Centre), van waaruit we dagelijks eventuele kwetsbaarheden opsporen en verhelpen. Om u een idee te geven hoe wij onze systemen regelmatig testen, volgt hier een overzicht van enkele kernactiviteiten;

- Periodieke kwetsbaarheidsscans (vulnerabilityscans) van onze totale ICT-infrastructuur (in samenwerking met externe partners).
- Dagelijkse monitoring van verdachte activiteiten door ons Security Operations Center (SOC).
- Penetratietesten op (nieuwe) systemen en oplossingen.
- Het uitvoeren van crisisoefeningen om de impact van een eventueel cyberincident te minimaliseren en te isoleren.
- Periodiek toetsen we op de naleving van de basisnorm informatiebeveiliging overheid van de Rijksoverheid (BIO), vanuit de applicaties (RIA's)

Dit doen we niet alleen vanuit onze eigen beveiligingsorganisatie, maar ook in samenwerking met diverse externe partners. Uiteraard zetten we ook in op de samenwerking met ethical hackers, zoals afgelopen maand juni hebben we een groot cyberevent gehouden, genaamd HACK-010. Tijdens dit event hebben we met ongeveer 40-tal ethical hackers onze ICT-infrastructuur laten toetsen. We hanteren binnen Rotterdam ook een Responsible Disclosure waarin we de hacking community aanmoedigen (met beloning) om eventuele kwetsbaarheden bij onze securityorganisatie te melden.

Vraag 6:

Kan het college gezien de urgentie deze en de twee eerdergenoemde setjes aan schriftelijke vragen gezamenlijk en dringend – het liefst binnen een week - beantwoorden? Zo nee, waarom niet?



Antwoord:

Dat is niet mogelijk, omdat de beantwoording via het college verloopt. Ze zijn zo snel mogelijk beantwoord.

Burgemeester en wethouders van Rotterdam,

De secretaris,

V.J.M. Rozen

De burgemeester,

A. Aboutaleb