Rekenkamercommissie

Aan de gemeenteraad van Voerendaal

17 februari 2017

Geachte raadsleden,

Hierbij biedt de Rekenkamercommissie het onderzoek Digitale Veiligheid aan.

De Rekenkamercommissie vindt digitale veiligheid belangrijk voor de burgers, voor de organisatie en voor derden en heeft dit onderwerp op eigen initiatief onderzocht.

De wereld digitaliseert en digitale veiligheid moet dan ook hoog en constant op de agenda staan. Door de snelle ontwikkeling van systemen, software en toepassingen is ook sprake van een forse groei in kwetsbaarheden. Gemeenten dragen verantwoordelijkheid als het gaat om informatiebeveiliging en de bescherming van (vertrouwelijke) gegevens en hebben hiervoor een normenkader in de Baseline Informatiebeveiliging Gemeenten (BIG). Dat is het beleid, maar hoe staat het in de praktijk? Kan de Rekenkamercommissie met een onderzoek de Raad en de organisatie een gevoel geven dat men in Voerendaal wel 'veilig' kan mailen of digitaal gegevens kan versturen of ontvangen? En is de organisatie in staat om een externe hackaanval succesvol af te slaan?

Het onderzoek heeft hierop antwoord en aanbevelingen kunnen geven. Maar laten we niet vergeten dat beveiliging een continu aandachtsproces moet blijven.

Hoogachtend,

Lieve Schouterden
Voorzitter Rekenkamercommissie

voerendaal

Onderzoek Rekenkamercommissie

Digitale Veiligheid

December 2016

Colofon

Rekenkamercommissie Voerendaal
Lieve Schouterden,
Voorzitter en enig lid.

Regie onderzoek Digitale Veiligheid: Lieve Schouterden
Onderzoeksbureau Digitale Veiligheid: SlimInICT!/Flaxe

December 2016

Inhoudsopgave

Aanbieding

Hierbij biedt de Rekenkamercommissie het onderzoek Digitale Veiligheid aan. De Rekenkamercommissie vindt digitale veiligheid belangrijk voor de burgers, voor de organisatie en voor derden en heeft dit onderwerp op eigen initiatief onderzocht.

De wereld digitaliseert en digitale veiligheid moet dan ook hoog en constant op de agenda staan. Door de snelle ontwikkeling van systemen, software en toepassingen is ook sprake van een forse groei in kwetsbaarheden.
Gemeenten dragen verantwoordelijkheid als het gaat om informatiebeveiliging en de bescherming van (vertrouwelijke) gegevens en hebben hiervoor een normenkader in de Baseline Informatiebeveiliging Gemeenten (BIG). Dat is het beleid, maar hoe staat het in de praktijk? Kan de Rekenkamercommissie met een onderzoek de Raad en de organisatie een gevoel geven dat men in Voerendaal wel 'veilig' kan mailen of digitaal gegevens kan versturen of ontvangen? En is de organisatie in staat om een externe hackaanval succesvol af te slaan?

De Rekenkamercommissie heeft het bureau SlimInICT!/Flaxe penetratietesten laten uitvoeren op de ICT-infrastructuur van de gemeente.
Hierbij kwam een aantal kwetsbaarheden in de beveiliging bloot te liggen. Van de 10 gevonden kwetsbaarheden kregen 3 de kwalificatie 'hoog', 3 'medium' en 4 'laag'. Om de organisatie te behoeden voor verdere veiligheidsrisico's heeft de Rekenkamercommissie het college de handreiking gedaan om de kwetsbaarheden onverwijld op te lossen tijdens de periode van bestuurlijke reactie. De organisatie heeft dit uitermate professioneel opgepakt en tijdens de hertesten is gebleken dat de aangetroffen kwetsbaarheden zijn opgelost.

Uit veiligheidsoverwegingen heeft de voorzitter van de Rekenkamercommissie op grond van artikel 185 lid 1 van de Gemeentewet de technische rapporten als vertrouwelijk bestempeld. Deze liggen voor raadsleden ter inzage bij de griffier. Wat u hierna aantreft is dus uitsluitend de bestuurlijke rapportage aan de raad.

Het college onderschrijft in haar bestuurlijke reactie het belang van een zo hoog mogelijk ICT-beveiligingsniveau en het periodiek (laten) uitvoeren van penetratietesten.

Beveiliging is een continu proces. Het is aan de raad om digitale veiligheid hoog in het vaandel te willen dragen, daartoe kaders en prioriteiten te stellen en passende middelen toe te kennen.

Lieve Schouterden
Voorzitter Rekenkamercommissie Voerendaal

1. Inleiding

1.1 Aanleiding van het onderzoek

De Rekenkamercommissie vindt digitale veiligheid belangrijk en volgt de publicaties over dit onderwerp met aandacht.
Het belang en de bewustwording van informatiebeveiliging en bescherming van privacygevoelige informatie is regelmatig in het nieuws. Ook zo de casussen DigiNotar en Lektober. Deze hebben aangetoond dat gemeenten digitaal kwetsbaar zijn. Het artikel over 'gemeentelijke e-mail gênant slecht beveiligd', Binnenlands Bestuur 2 juni 2016, waarin werd gesteld dat slechts 3 van de 50 gemeenten voldoen aan de standaarden voor veilige e-mail was de concrete aanleiding voor de Rekenkamercommissie om het onderzoek op de agenda te plaatsen.
Omdat er geen feitelijke aanleiding in de gemeente Voerendaal was om een uitgebreid onderzoek op te zetten, werd er gekozen voor een beperkte Quick scan. Als de uitkomsten hiervan van dusdanige aard zouden zijn, kan er nog overgegaan worden tot een uitgebreid onderzoek.

1.2 Opzet van het onderzoek

Op 27 mei 2016 heeft de voorzitter van de Rekenkamercommissie een eerste verkenning over digitale veiligheid en informatiebeveiliging in een gesprek met de gemeentesecretaris verricht.

Op 31 mei heeft de voorzitter van de Rekenkamercommissie volgend bericht ontvangen:

"Voor onze digitale dienstverlening moeten we jaarlijks een audit afleggen, de zgn. DigiD audit. Deze audit omvat:
Check op de beschikbaarheid, actualiteit en het hanteren in de praktijk van richtlijnen, protocollen op het brede gebied van informatiebeveiliging. Hierbij wordt bij de gemeente gekeken naar hoe informatie en toegang hiertoe beveiligd zijn (zowel digitaal als fysiek), wie welke rechten heeft, hoe deze actueel gehouden worden etc. Hierbij wordt niet alleen gekeken naar de systemen en informatiestromen die met DigiD te maken hebben, maar integraal naar de gehele gemeentelijke informatiebeveiliging. Hierbij moet voldaan worden aan (terecht) zeer strenge eisen.
Dit onderzoek en beoordeling vindt zowel plaats bij de gemeente als bij de leverancier(s) van de voor digitale dienstverlening gebruikte software.
Een zogenaamde TPM (Third Party Mededeling), waarbij onder meer een hacker wordt ingehuurd om eventuele gaten/tekorten in de gebruikte software op te sporen.
Als Voerendaal maken we voor de website gebruik van het CMS (Content Management Systeem) van Simgroep en voor onze digitale dienstverlening van Zaaksysteem.nl. De formulieren op onze website en DigiD-aansluiting maken bij ons onderdeel uit van het zaaksysteem.
De audit hebben we onlangs succesvol afgesloten (100% score). Om onze beveiliging up-to-date te houden zijn we aangesloten bij de IBD (Informatie Beveiligings Dienst), waarbij ontvangen signalen voor zover nodig meteen worden opgepakt."

Met de wetenschap dat de jaarlijkse audits succesvol werden afgesloten, zag de Rekenkamercommissie toen nog geen aanleiding tot uitvoeren van een onderzoek.

In de periode juli-augustus werd een onderzoek bij de gemeente Heerlen opgestart. Daaruit bleek eind september dat er kwetsbaarheden werden aangetroffen bij Parkstad-IT, de organisatie waarvan de gemeente Voerendaal diensten afneemt. Reden om het onderzoek digitale veiligheid alsnog (zeer beperkt) uit te laten voeren. Het opstarten van dit onderzoek is gemeld aan de gemeentesecretaris op 3 oktober en in het presidium van 4 oktober. Op 18 oktober is de opdracht verstrekt aan het bureau SlimInIct!/Flaxe.

Het doel van dit onderzoek was om (gecontroleerd) als een quasi kwaadwillende buitenstaander te zoeken naar kwetsbaarheden in het Voerendaals netwerk en trachten toegang te verkrijgen en/of (vertrouwelijke) informatie te vergaren. De opdracht richtte zich op een zogenaamde Blackbox penetratietest, waarbij er vooraf geen informatie werd verstrekt over de Voerendaalse ICT-omgeving.
Wel is door de voorzitter van de Rekenkamercommissie het Voerendaals e-mailadres van de gemeentesecretaris doorgegeven om dit te 'misbruiken' en phishingmail te versturen naar de griffier. Het hoeft geen betoog dat deze poging geheel 'gecontroleerd' is uitgevoerd.

De kwetsbaarheid van het netwerk vanaf de buitenkant werd getest, waarbij gezocht werd naar open poorten, admin- wachtwoorden, user id's en andere inlogcodes. Vervolgens werden de verkregen inlogcodes gebruikt om dieper in het systeem te komen.

Deze testmethode benadert het meest een reële aanvalssituatie. Het uitgangspunt daarbij blijft dat de aanval gecontroleerd zou plaatsvinden waarbij risico's tot schade nihil tot uiterst beperkt zouden blijven, de kwaliteit van de test zo optimaal mogelijk is en dat de resultaten van het onderzoek bruikbaar zijn om kwetsbaarheden efficiënt te verhelpen.

Afgesproken werd dat de voorzitter van de Rekenkamercommissie bij voortduring op de hoogte werd gehouden zodat, in het geval de Ethical Hacker een groot data lek zou tegenkomen, onmiddellijk kon opgeschaald worden naar de organisatie.

De Rekenkamercommissie wenst te benadrukken dat alle richtlijnen in acht genomen zijn om de vertrouwelijkheid tijdens de uitvoering van de penetratietesten te waarborgen. Aan de opdrachtnemer SlimInICT!/Flaxe werd een vrijwaring van overtreding Artikel 138a Wetboek Strafrecht computervredebreuk ten aanzien van het *.Voerendaal.nl domein verstrekt.

2. Het onderzoek

2.1 Centrale vraagstelling

De centrale vraagstelling in dit onderzoek werd als volgt geformuleerd:
Is de gemeente Voerendaal in staat een externe hackaanval succesvol af te slaan? En kan er misbruik gemaakt worden van oneigenlijk verkregen toegang of informatie?

Gegevens van burgers, bedrijven en instellingen moeten bij de gemeente in veilige handen zijn, zij moeten hierop kunnen vertrouwen. Inbreuken kunnen ernstige gevolgen hebben voor de privacy van burgers, bedrijven en instellingen maar ook voor de gemeente zelf en kunnen leiden tot verlies van vertrouwelijke gegevens, persoonlijke en financiële schade en imagoschade voor de gemeente. Systemen en informatiegegevens kunnen van buitenaf overgenomen worden en enkel met veel moeite (en geld) weer terug verkregen worden.

Er is een wettelijke plicht tot informatiebeveiliging om gegevens *vertrouwelijk*, *betrouwbaar* en *beschikbaar* te houden. En dit op de terreinen *organisatie*, *mensen*, *techniek* en *fysiek*. Vanuit gestelde kaders borgt de gemeente via jaarlijkse audits de digitale veiligheid. Maar werkt dit ook in de praktijk? Wordt de beveiliging gestructureerd, bij voortduring en volgens protocollen getoetst en gewaarborgd?

2.2 Aanpak onderzoek

Om de centrale vraagstelling te beantwoorden zijn de volgende onderzoeks-onderdelen uitgevoerd:

- Vaststellen van het doelwit www.voerendaal.nl waaronder (maar niet beperkt tot) 91.241.7.75 en de IP-range 178.21.216.21 - 178.21.216.43 - 178.21.216.95, 178.21.217.145 t.e.m. 149 en 178.21.223.112.
- Vastleggen welke grenzen er zijn voor de penetratietesters waaronder expliciet het niet overnemen van de systemen.
- In kaart brengen van domein, sub domeinen, e-mailadressen, gebruikte software op de systemen, open poorten, welke informatie gedeeld en/of gelinkt wordt en/of terug te vinden is op social media zoals LinkedIn enz.
- Aan de hand van verkregen informatie uit de vorige fases proberen ‘misbruik’ te maken, pogen toegang te verkrijgen en te onderzoeken of er sprake is van lekken.
- Toepassen van ‘bruteforcing’ op alle systemen waar er inloggegevens gebruikt worden via geautomatiseerde inlogcombinaties.
- Logging van alle uitgevoerde acties en gevonden kwetsbaarheden in een logbestand.
- Prioriteren en rapporteren van aangetroffen kwetsbaarheden en lekken.

2.3 Proces onderzoek

Het opstarten van dit onderzoek is gemeld aan de gemeentesecretaris op 3 oktober en in het presidium van 4 oktober.
Op 18 oktober is de opdracht verstrekt aan het bureau SlimInIct!/Flaxe.
Het onderzoek is uitgevoerd in de maanden oktober en november 2016.
Op 7 december is aan de gemeentesecretaris gemeld dat er geen urgente lekken maar wel enkele kritieke bevindingen zijn geconstateerd.
Op 22 december zijn de testing reports en de managementsamenvatting door de Rekenkamercommissie ontvangen en aansluitend is het onderzoeksrapport door de Rekenkamercommissie opgesteld.
Op 3 januari 2017 is het rapport (via de gemeentesecretaris) aan het college van B&W verstuurd voor bestuurlijke hoor en wederhoor. Daarbij is een handreiking gedaan om de geconstateerde kwetsbaarheden onverwijld op te lossen.
Tussen 4 januari en 3 februari zijn de herstel- en verbeteracties doorgevoerd en is hiervan rapportage verstuurd naar de Rekenkamercommissie.
Op 3 en 8 februari hebben de hertesten plaatsgevonden.
De reactie van het college is ontvangen op 8 februari 2017.

Nog belangrijk te vermelden is dat een substantieel deel van de Voerendaalse ICT-omgeving een verantwoordelijkheid is van, en uitgevoerd wordt door Parkstad-IT. Een gedeelte is de verantwoordelijkheid van de aangesloten gemeenten zelf. Het is uit dit onderzoek maar ook uit het lopende onderzoek bij de gemeente Heerlen gebleken dat zwakheden bij aangesloten gemeenten een kwetsbaarheid (kunnen) vormen voor de andere aangesloten gemeenten.
Het gedeelte waarvoor Parkstad-IT verantwoordelijk is, *is niet meegenomen* in dit zeer beperkte onderzoek dat de Rekenkamercommissie voor de gemeente Voerendaal heeft laten uitvoeren. Het onderzoek in Heerlen is nog in volle gang.
De Rekenkamercommissie heeft kunnen constateren dat de organisatie Voerendaal bij het oplossen van de kwetsbaarheden contact heeft opgenomen met Parkstad-IT om ook daar concrete test-, herstel- en verbeteracties te laten uitvoeren voor de onderdelen die de gemeente Voerendaal afneemt van Parkstad-IT.

De Rekenkamercommissie zal met aandacht de digitale veiligheid blijven opvolgen en op enig moment een aantal hertests laten uitvoeren.

3. Conclusie en aanbevelingen

3.1 Conclusies onderzoek

De gevonden kwetsbaarheden en de bevindingen vormen de basis voor de conclusies en aanbevelingen in dit rapport. Vanwege de risico's voor de informatiebeveiliging worden de bevindingen slechts in algemene termen gepubliceerd. De technische rapporten liggen voor raadsleden ter inzage bij de griffier.

De centrale vraagstelling in dit onderzoek werd als volgt geformuleerd:
Is de gemeente Voerendaal in staat een externe hackaanval succesvol af te slaan? En kan er misbruik gemaakt worden van oneigenlijk verkregen toegang of informatie?

Gezien de strekking van de beperkte Quick scan, de uitsluiting van gedeelten en systemen die onder Parkstad-IT vallen en het gegeven dat absolute veiligheid niet bestaat omdat elke dag nieuwe veiligheidsrisico's ontstaan, kunnen volgende antwoorden op de centrale vraagstelling geformuleerd worden.

Allereerst kunnen we constateren dat het content management system van www.voerendaal.nl (een CMS genaamd SIMsite) up-to-date gehouden lijkt te worden. De CMS bleek niet kwetsbaar voor SQL injection (waarmee de hacker data kan ophalen) en XSS aanvallen (cross site scripting oftewel invoegen van een script in de tekst).

Een aantal van de onderzochte loginpagina's gaven geen onvoorwaardelijke mogelijkheid tot herhaald inloggen met verschillende usernames en/of wachtwoorden, waardoor bruteforcing als aanval geen reële optie is voor deze systemen; bijvoorbeeld https://intranet.voerendaal.nl/ geeft een oplopend tijdsinterval waarop niet ingelogd kan worden bij herhaald gebruik van foutieve login credentials (usernames en wachtwoorden).

Ook is het goed om op te merken dat de software voor de afsprakenmodule op https://afspraken.voerendaal.nl/internetafspraken/ (welke wordt geleverd door JCC Software) niet meer kwetsbaar is voor een beruchte kwetsbaarheid welke afgelopen jaar is gevonden en waarmee een aanvaller onder andere afspraken van burgers kon inzien en annuleren. Ook dit duidt erop dat de systeembeheerder(s) van een aantal van de Voerendaal websites de software met zekere regelmaat updaten.

Kwetsbaarheden:
Tijdens de tests zijn meerdere zwakke plekken en kwetsbaarheden gevonden. Deze zwakke plekken doen zich op meerdere fronten voor en duiden erop dat het binnen de digitale omgeving van Voerendaal (en daarmee ook Parkstad)

(deels) ontbreekt aan structureel ingerichte processen die zich bezighouden met alle facetten van beveiliging.

Gezien de aard en het aantal van de gevonden kwetsbaarheden, is er een reële kans dat iemand die zich als doel stelt schade toe te brengen aan de systemen van de gemeente Voerendaal, daar ook in zal slagen, met name door het feit dat er voor het uitbuiten van een aantal van de geïdentificeerde zwakheden weinig expertise nodig is. Aangegeven werd dat de website www.voerendaal.nl in het onderzoek niet gevoelig is gebleken voor rechtstreekse aanvallen van buitenaf. Maar een hacker die zichzelf toegang wil verschaffen tot het interne netwerk van Voerendaal, met als hoofddoel de website www.voerendaal.nl, zal zijn aanval via een "omweg" trachten uit te voeren middels één van de ontdekte zwaktes, namelijk een social engineering aanval (dit is een aanval op de zwakte/nieuwsgierigheid van de mens) welke gebruikmaakt van bijvoorbeeld email header spoofing (vervalsing), of uploaden van malware via het webformulier, of door een inbraak te plegen op een minder goed beveiligd systeem binnen de geteste IP range (bijvoorbeeld het Gegevenshuis) en dan verder te gaan middels "pivoting" (bij pivoting wordt de zwakste schakel in een netwerk aangevallen, met de bedoeling meer inzicht te verschaffen in het netwerk, en daarmee kansen te creëren om dieper door te dringen in het netwerk.).

In de praktijk worden beide aanvalsmethoden (Social Engineering en Pivoting) vaak gebruikt. Door de in kaart gebrachte zwaktes aan te pakken, wordt de kans van slagen van deze beide typen aanvallen sterk verkleind.

Wat tijdens het onderzoek vooral opviel is dat, ondanks de uitgevoerde audits (zie pagina 7, verkenning mei 2016) waarbij wordt aangegeven dat er met de audit een 100% beveiligingsscore wordt gehaald, het Zaaksysteem één van de meest kritische kwetsbaarheden is (geworden).
Jaarlijkse audits zijn niet zaligmakend en kunnen daarmee een vals gevoel van digitale veiligheid geven en mogen dus enkel als een momentopname beschouwd worden. Veel belangrijker is het om digitaal beveiligingsbeleid te prioriteren, beheersmaatregelen te nemen die risico's zoveel als mogelijk uitsluiten of inperken en te sturen op (zeer) frequente beveiligingstesten (zowel intern uitgevoerd als door externen).

De penetratietesten richtten zich op het domein *.Voerendaal.nl en een willekeurig aantal IP adressen. Daarbij zou de gemeente Voerendaal kunnen aangeven dat bepaalde onderdelen, ressorterend onder Parkstad-IT, niet tot hun verantwoordelijkheid horen, maar deze kunnen wel een risico vormen voor Voerendaal zelf en de overige systemen in dezelfde range. De gemeente, als opdrachtgever en contractuele partner van Parkstad-IT, blijft (mede)verantwoordelijk voor de digitale veiligheid.

Kwetsbaarheidsoverzicht systemen			
Aantal live hosts	**22**		
Gevonden kwetsbaarheden	**10**		
Ernst van de kwetsbaarheden	HOOG	MIDDEN	LAAG
	3	**3**	**4**

Samengevat werd aangetroffen:

- De mogelijkheid tot het verspreiden van malware naar het netwerk van de gemeente middels het uploaden (Trojaans paard);
- De mogelijkheid om e-mails met vervalste headers te versturen; een aanvaller kan iemand@Voerendaal.nl ongecontroleerd gebruiken als afzendadres (dit is aangetoond met het e-mailadres van de gemeente-secretaris);
- Een aantal systemen die SSL certificaten verstrekken maar die niet worden ondertekend door een Certificate Authority;
- Een aantal publieke http servers die geen publieke diensten verlenen;
- Een server met sterk verouderde software.

3.2 Aanbevelingen

Aanbeveling 1:

Er is een aantal bevindingen tijdens de penetratietesten naar voren gekomen die vragen om een oplossing dan wel aanleiding geven tot verder onderzoek.

Geef het college de opdracht om de aangetroffen kwetsbaarheden onverwijld te (doen) oplossen zodat de kansen op geslaagde hacks verkleind worden.

Naschrift RKC 17/02/2017: alle geconstateerde kwetsbaarheden zijn opgelost.

Aanbeveling 2:

In het artikel van Binnenlands Bestuur 2 juni 2016 over *'gemeentelijke e-mail gênant slecht beveiligd'*, werd gesteld dat slechts 3 van de 50 onderzochte gemeenten voldoen aan de standaarden voor veilige e-mail. Het artikel van 19 december 2016 *'gemeenten hard bezig om e-mailbeveiliging te verbeteren'* leert ons dat inmiddels 16 van de 50 onderzochte gemeenten voldoen aan de standaarden voor veilige e-mail. Uit onderhavig onderzoek is gebleken dat de gemeente Voerendaal hier nog niet aan voldoet.

Geef het college de opdracht om gemeentelijke e-mail te beveiligen met de meest moderne beveiligingstandaarden.

Aanbeveling 3:

Het gestructureerd en volgens processen toetsen van de mate van beveiliging dient bij voortduring uitgevoerd te worden. Veelal pas na een inbraak(poging) ontstaat het besef en de noodzaak de beveiliging permanent te waarborgen. Uit dit onderzoek is gebleken dat een frequentie van een jaarlijkse audit onvoldoende is. Voorzie implementatie van cybersecurity van voldoende middelen en adequate formatie. Kies voor 'jong talent' door bijvoorbeeld studenten van Hogeschool Zuyd als trainees in te zetten.

Besluit tot uitvoering van frequente periodieke veiligheidstests op random gekozen issues.

Aanbeveling 4:

Het is belangrijk om te leren van de beveiligingsmeldingen, hierop door te bouwen en te verankeren in beheersmaatregelen. Beveiliging is immers een continu en dynamisch proces waarbij zich dagelijks nieuwe dreigingen aankondigen en waardoor 100% beveiliging nooit bestaat. Een hacker zal alle mogelijkheden benutten om aan informatie te komen.

Omdat het afbreukrisico voor een gemeentelijke organisatie, met veelal vertrouwelijke en privacygevoelige informatie, hoog is (denk aan niet werkende systemen, verlies van vertrouwelijke gegevens, financiële en imago schade en negatieve publiciteit) zou het beveiligingsbeleid naar rato geprioriteerd moeten zijn. De praktijk wijst vaak uit dat dit wel gebeurt in het beleid, maar niet altijd in de (dagelijkse) uitvoering. De informatieveiligheid dient risicogebaseerd te zijn, risicoanalyses dienen frequent doorgevoerd te worden. Niet alleen een mooi plan op papier maar daadwerkelijke uitvoering van periodieke risico- en beveiligingsaudits met verslaglegging en plan van aanpak in rapportages aan college en raad.

Benoem als raad de digitale informatieveiligheid tot een key issue en een expliciet aandachtspunt om een integrale informatiebeveiliging te creëren en geef opdracht aan het college om periodiek informatie over audits en beheersmaatregelen naar de raad te sturen.

Aanbeveling 5:

Een deel van de Voerendaalse ICT-omgeving is een verantwoordelijkheid van en wordt uitgevoerd door Parkstad-IT.

Een gedeelte is de verantwoordelijkheid van de aangesloten gemeenten zelf.

Het is uit dit onderzoek maar ook uit het vergelijkbaar onderzoek bij de gemeente Heerlen gebleken dat zwakheden bij aangesloten gemeenten een kwetsbaarheid vormen voor de andere aangesloten gemeenten.

Laat -via het college- Parkstad-IT de aangesloten gemeenten en de leveranciers van software verplichten om nieuwe updates onverwijld te installeren en de informatieveiligheidsaspecten uitvoerig te testen.

4. Bijlagen

4.0 Bestuurlijke reactie van het College van B&W

4.1 Artikelen

4.1.1 Artikel Binnenlands Bestuur 2 juni 2016 'gemeentelijke e-mail gênant slecht beveiligd'

4.1.2 Artikel Binnenlands Bestuur 19 december 2016 'gemeenten hard bezig e-mailbeveiliging te verbeteren'

4.1.3 Artikel 8 aandachtspunten bij e-mailbeveiliging voor gemeenten

4.2 Vertrouwelijke bijlagen

Deze bijlagen liggen ter inzage bij de griffie

4.2.1 Penetration Testing Report-Voerendaal v1.1 - dd. 22 december 2016 (28 pagina's)

4.2.2 Managementsamenvatting Penetration Testing Report-Voerendaal v1.2 - dd. 22 december 2016 (7 pagina's)

4.2.3 Header spoofing e-mail gemeentesecretaris -> griffier dd. 2/11/2016 en (onwetende) reactie van de griffier dd. 3/11/2016

4.2.4 Security Re-audit Report-Voerendaal v1.1 - dd. 3 februari 2017 (13 pagina's)

4.2.5 Security Re-audit Report-Voerendaal v1.2 - dd. 3 februari 2017 - ontvangen 8 februari 2017 (13 pagina's)

gemeente
voerendaal

Raadhuisplein 1
6367 ED Voerendaal
Postbus 23000
6367 ZG Voerendaal

T 045 – 575 33 99
F 045 – 575 11 95
E info@voerendaal.nl
W voerendaal.nl

Aan de Rekenkamercommissie
t.a.v. mevrouw L. Schouterden

Uw brief van	Uw kenmerk	Ons kenmerk	Voerendaal
		36125	08-februari-2017
Onderwerp		**Behandeld door**	**Bijlagen**
Rapport Digitale Veiligheid		Y. Meertens	

Beste mevrouw Schouterden

Op 3 januari jl. heeft U het rapport Digitale Veiligheid via de gemeentesecretaris aan het college van B&W gestuurd.

De gemeente werkt steeds meer digitaal. Gegevens van burgers bedrijven en instellingen moeten bij de gemeente in goede handen zijn. De gemeente Voerendaal onderschrijft dan ook het belang van een goede informatiebeveiliging.

De in de penetratietest geconstateerde kwetsbaarheden zijn dan ook samen met de verantwoordelijke leveranciers opgepakt en zijn de aanbevelingen overgenomen en grotendeels uitgevoerd. Een door de gemeente Voerendaal aangevraagde tweede penetratietest toont dit dan ook aan. De inhoudelijke antwoorden zijn al per mail met U afgestemd.

Uiteraard streeft de gemeente Voerendaal naar een zo hoog mogelijk beveiligingsniveau, echter 100% veiligheid bestaat niet. De beveiliging is een dynamisch proces dat continu aandacht vraagt om aanscherping van maatregelen door nieuwe "dreigingen". Ook moeten er soms keuzen gemaakt worden tussen wat gewenst is en praktisch realiseerbaar is. Het college onderschrijft dan ook het belang van periodieke penetratietesten en zal deze periodiek laten uitvoeren.

BURGEMEESTER EN WETHOUDERS VAN VOERENDAAL,
de secretaris, de burgemeester,

H.H.M. Timmermans W. Houben

Bijlage 1 – Inhoudelijke reactie op 2e penetratietest ontvangen d.d. 4 februari 2017

In de tweede penetratietest waren nog een aantal niet opgeloste kwetsbaarheden geconstateerd. Hieronder in hoofdlijnen de reactie op deze punten. In verband met beveiliging wordt er geen detail informatie uitgewisseld. Dit is wel afgestemd met het buro (Cybersecurit) dat de penetratietest heeft uitgevoerd.

- High - Mail uit naam van iemand anders sturen – Bevestigd door CybersecurITI, opgelost.
- High & Medium - Het Gegevenshuis heeft 2 steekjes laten vallen – Bevestigd door Het Gegevenshuis als opgelost, tevens ter bevestiging naar CyversecurIT gestuurd.
- Low – Valt helaas niet op te lossen, maar vormt ook geen bedreiging. Geeft de tester ook zelf aan – Onveranderd

Beveiliging Website Gemeente Voerendaal

De beveiliging van de gemeentelijke websites komt de laatste tijd steeds vaker in het nieuws. En terecht, gemeenten hebben ook de verantwoordelijkheid om zorgvuldig met persoonsgegevens om te gaan. In de nieuwsberichten wordt er vooral gesproken over de noodzaak van een beveiligde verbinding. Wat wordt hier eigenlijk mee bedoelt.

Een beveiligde verbinding (https) herken je bijvoorbeeld in bepaalde browsers aan een groen slotje. Een https-verbinding zorgt ervoor dat een kwaadwillende niet kunnen meegluren met welke websitepagina's je bezoekt en welke informatie je verstuurt, zoals je Burgerservicenummer of woonadres.

Op de site www.internet.nl kun je testen hoe veilig een site is. Op deze site kun je testen of een website werkt met moderne internetstandaarden. Wat zijn "internetstandaarden"?

Om wereldwijd gegevens tussen verschillende computers te kunnen uitwisselen, zijn internationale afspraken nodig over de manier waarop de computers met elkaar praten — de digitale "stekkers en stopcontacten" waarmee alles met elkaar verbonden is. Deze afspraken worden internetstandaarden of internetprotocollen genoemd.

De website van Voerendaal bestaat uit verschillende onderdelen, namelijk:

http://www.voerendaal.nl (CMS van Simgroup)

http://mijn.voerendaal.nl (Zaaksyteem.nl)

Alle e-formulieren, DigiD, Pip en andere zaken waar persoonsgegevens bij gebruikt worden gaan via het zaaksysteem (http://mijn.voerendaal.nl). Dit is ook een beveiligde verbinding die via https afgedwongen wordt.

Op de site http://www.voerendaal.nl wordt alleen gebruikt voor het publiceren van nieuws, algemene informatie en communicatie over projecten. Via deze omgeving worden geen persoonsgegevens uitgewisseld.

Het CMS dat wordt gebruikt bij http://www.voerendaal.nl is van Simgroep. Op http://www.intenet.nl wordt op een 3-tal punten getest, namelijk:

IPv6 – Sim geeft aan dat zij dit nog niet ondersteunen. Zij gaan dit medio 2017 opleveren.

DNSSEC – hier voldoet http://www.voerendaal.nl aan

TLS – hiervoor moet een apart certificaat geïnstalleerd worden, Simgroep schrijft voor dat dit certificaat alleen door Simgroep geïnstalleerd mag worden. (terwijl het ook door een andere partij zou kunnen). De prijs die sim hiervoor vraagt staat niet in verhouding met de werkelijke kosten van een certificaat. Ook moeten we dan een verplichting voor 5 jaar aangaan. Dit terwijl ons contract per 31-12-2017 met Sim afloopt en we voornemens zijn om een nieuwe aanbesteding te starten voor onze website. Bij de aanbesteding zal het (blijven) voldoen aan de internetstandaarden uiteraard een eis zijn.

Meerdere klanten van Simgroep zijn in discussie over of het voldoen aan de internetstandaarden binnen het basis hosting bedrag hoort (Simgroep dient immers een veilige site te geven) of dat Simgroep hier een aparte module voor mag aanbieden die je moet afnemen indien je een veilige site wenst.

Waarom voldeed de website van Voerendaal (http://www.voerendaal.nl) eerst aan meer normen?

Medio 2016 zijn de normen waarop de site van internet.nl test aangescherpt. Hierdoor voldoen we nu nog maar aan 1 van de 3 eisen (zie hierboven).

GEMEENTELIJKE E-MAIL 'GÊNANT SLECHT' BEVEILIGD

Sjoerd Hartholt BB 02 jun 2016

Vrijwel geen gemeente voldoet aan de verplichte beveiligingsstandaarden voor e-mail, zo blijkt uit een steekproef bij vijftig gemeenten van *Binnenlands Bestuur.* Criminelen hebben met hun phishingmails vrij spel, terwijl goede beveiliging volgens Internet Society Nederland vrij eenvoudig is te regelen.

Drie van de vijftig gemeenten voldoen
Uit een steekproef met e-maildomeinen van vijftig verschillende gemeenten blijken slechts drie gemeenten van hen aan de moderne standaarden voor veilige e-mail te voldoen: Den Haag, 's-Hertogenbosch en Woerden. Grote gemeenten als Amsterdam, Rotterdam en Utrecht lukt dat niet. Internet Society Nederland spreekt van een 'probleem' en 'een slechte zaak'. De landelijke vereniging van internetprofessionals stelt dat iedere organisatie met een publieke taak in Nederland al lang had kunnen en moeten voldoen aan de minimale standaarden.

E-mails omleiden naar ander adres
Door het niet toepassen van de standaarden blijft het mogelijk om phishingmail te versturen vanuit en naar de gemeenten en zo argeloze ontvangers een bijlage of link met malware te bezorgen. Uit de test van Binnenlands Bestuur blijkt dat bij vijfendertig van de vijftig onderzochte gemeenten het gemeentelijk e-mailadres eenvoudig kan worden omgeleid naar een ander adres. Zo kunnen e-mails van en naar gemeenten bij kwaadwillende personen kunnen terechtkomen. Voor webmail bestaat er zelfs een grotere dreiging. Een ambtenaar die wel eens via wifi in de trein zijn webmail checkt, is zonder adequate beveiliging niet in staat om een nepversie daarvan te onderscheiden. Als gebruikersnaam en wachtwoord eenmaal bekend zijn, heeft een aanvaller de volledige beschikking over de mailaccount.

E-mails controleren op vervalsing
Voor de drie internetstandaarden DKIM, SPF en DMARC die gelden voor het terugdringen van phishing, spam en virussen, zakten zevenenveertig van de vijftig gemeenten bij de test door het ijs. Deze drie standaarden worden meestal gezamenlijk ingezet om te controleren of de afzender (een e-mailadres) en de verzender (een computersysteem) van een e-mailbericht inderdaad kloppen, en of de inhoud van het bericht onderweg niet is veranderd. Ontvangers kunnen zonder deze standaarden niet controleren of een e-mail wel echt van het gemeentelijke e-maildomein komt, waardoor iemand zich bij ontvangers als een ambtenaar of zelfs burgemeester van een gemeente kan voordoen.

Beveiligde verbinding niet mogelijk
Ook een beveiligde gegevensuitwisseling via TLS is voor een flink aantal gemeenten een probleem, omdat er geen STARTTLS-standaard wordt aangehouden. Van de vijftig geteste gemeenten zijn er om die reden veertien die geen beveiligde verbinding kunnen opbouwen. Hierdoor is de communicatie per e-mail niet volledig afgeschermd voor onbevoegden.

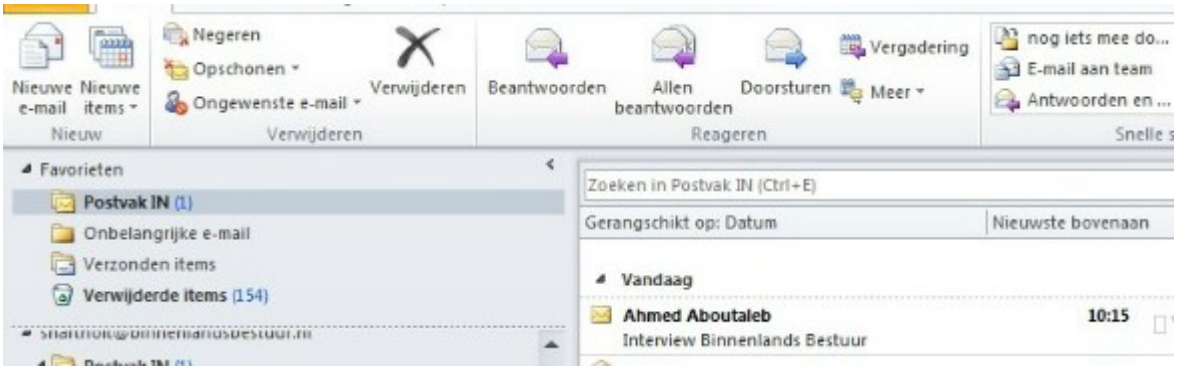
Gemeenten te laat
Michiel Leenaars, directeur van Internet Society Nederland, stelt dat phishingmails met de juiste internetstandaarden allang op de gemeentelijke server geblokkeerd hadden kunnen worden, waardoor die dus de gemeentelijke inbox niet bereiken. 'Zonder deze standaarden kan iedereen zonder problemen een niet van echt te onderscheiden e-mail sturen namens een willekeurige ambtenaar.'

Behoorlijk laks
Leenaars zegt dat veel overheidsorganisaties behoorlijk laks zijn als het op informatiebeveiliging aankomt. 'Ook als ze er al jaren op worden gewezen door externe beveiligingsexperts en organisaties als NCSC en Forum Standaardisatie.' Volgens Leenaars zou iedere organisatie met een publieke taak in Nederland kunnen en moeten voldoen aan de internetstandaarden

die op het platform van Internet.nl getest kunnen worden. Hij vindt het ‘gênant’ dat op Den Haag na ook de grootste gemeenten zakken voor de test. ‘Als het de gemeenten Heerlen, Simpelveld, Nuth, en De Friese Meren lukt om er doorheen te komen, dan ligt de lat echt niet te hoog.’

Verplichte veiligheid eenvoudig te testen
Het voldoen aan internetstandaarden is eenvoudig te testen via de website Internet.nl. De zelftest op de website is opgezet door onder meer het ministerie van Economisch Zaken, het Nationaal Cyber Security Centrum en diverse grote (branche)organisaties die samenwerken in het Platform Internetstandaarden. Deze internetstandaarden, internationale afspraken over de manier waarop de computers ‘met elkaar praten’, zijn inmiddels een aantal jaren oud en zorgen onder meer voor een veilige en betrouwbare manier van internet gebruiken. Verplichte internetstandaarden voor de beveiliging van e-mail die gemeenten niet aanhouden, zoals DNSSEC en DKIM ,staan al jaren op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. De standaarden op deze lijst zijn verplicht gesteld voor Nederlandse overheidsorganisaties. De verwachting is dat andere standaarden zoals STARTTLS daar snel aan toegevoegd worden.

‘GÊNANT SLECHTE’ BEVEILIGING E-MAIL



Sjoerd Hartholt BB 03 jun 2016

Vrijwel geen gemeente voldoet aan de verplichte beveiligingsstandaarden voor e-mail, zo blijkt uit een steekproef van Binnenlands Bestuur. Criminelen hebben met hun phishing mails vrij spel. Terwijl de beveiliging eenvoudig is te regelen.
Drie van vijftig gemeenten voldoen aan verplichte standaarden

Uit een steekproef met e-maildomeinen van vijftig verschillende gemeenten blijken slechts drie van hen aan de moderne standaarden voor veilige e-mail te voldoen: Den Haag, ‘s-Hertogenbosch en Woerden. Grote gemeenten als Amsterdam, Rotterdam en Utrecht lukt dat niet. Internet Society Nederland spreekt van een ‘probleem’ en ‘een slechte zaak’. De landelijke vereniging van internetprofessionals stelt dat iedere organisatie met een publieke taak in Nederland al lang had kunnen en moeten voldoen aan de minimale standaarden (zie kader ‘Verplichte veiligheid eenvoudig te testen’).

Door het niet toepassen van de standaarden blijft het mogelijk om phishing mail te versturen vanuit en naar de gemeenten en zo argeloze ontvangers een bijlage of link met malware te bezorgen. Er is geen grote technische kennis vereist voor het versturen van deze e-mails. Via Emkei’s Fake Mailer, een eenvoudig programma om e-mailadressen te vervalsen en te versturen, slaagde *Binnenlands Bestuur* er in een handomdraai in om een e-mail met verzonnen naam en e-mailadres in de gemeentelijke mailbox van Raalte te bezorgen. De ontvangstbevestiging op de vervalste mail werd vervolgens succesvol omgeleid naar de mailbox van Binnenlands Bestuur. Criminelen kunnen dus phishing mail zonder veel moeite goed laten aankomen in de gemeentelijke e-mailbox.

Aboutaleb
Bovendien is het mogelijk om het gemeentelijke e-maildomein te gebruiken, waardoor iedereen zich voor kan doen als vertegenwoordiger van de gemeente. Eveneens met Emkei’s Fake Mailer lukte het Binnenlands Bestuur om e-mails rond te sturen met de naam en het e-mailadres van Rotterdams burgemeester Ahmed Aboutaleb (zie screenshots).

Uit de steekproef blijkt ook dat bij vijfendertig van de vijftig onderzochte gemeenten het gemeentelijk e-mailadres eenvoudig kan worden omgeleid naar een ander adres. Zo kunnen e-mails van en naar gemeenten bij kwaadwillende personen terechtkomen. Voor webmail bestaat er zelfs een grotere dreiging. Een ambtenaar die weleens via wifi in de trein zijn webmail checkt, is zonder adequate beveiliging (DNSSEC in vaktermen, zie kader ‘Korte cursus’) niet in staat om een nepversie daarvan te onderscheiden. Als gebruikersnaam en wachtwoord eenmaal bekend zijn, heeft een aanvaller de volledige beschikking over de mailaccount.

Door het ijs
Bij de drie internetstandaarden DKIM, SPF en DMARC die gelden voor het terugdringen van phishing, spam en virussen, zakten zevenenveertig van de vijftig gemeenten bij de test door het ijs: zij gebruiken deze niet. De drie standaarden worden meestal gezamenlijk ingezet om te controleren of afzender (e-mailadres) en verzender (computersysteem) van een e-mailbericht inderdaad kloppen, en of de inhoud van het bericht onderweg niet is veranderd. Ontvangers kunnen zonder deze standaarden niet controleren of een e-mail wel echt van het gemeentelijke e-maildomein komt, waardoor iemand zich bij ontvangers als een ambtenaar of zelfs burgemeester van een gemeente kan voordoen.

Ook een beveiligde gegevensuitwisseling is voor een flink aantal gemeenten een probleem, omdat er geen START-TLS-standaard wordt aangehouden. Van de vijftig geteste gemeenten zijn er om die reden veertien die geen beveiligde verbinding kunnen opbouwen. Hierdoor is de communicatie per e-mail niet volledig afgeschermd voor onbevoegden.

Michiel Leenaars, directeur van Internet Society Nederland, stelt dat gemeenten door de juiste internetstandaarden te hanteren de phishing mails allang hadden kunnen blokkeren. ‘Zonder deze standaarden kan iedereen zonder problemen een niet van echt te onderscheiden e-mail sturen namens een willekeurige ambtenaar.’

Het probleem is volgens hem vooral dat phishing wordt gebruikt als opstapje voor grotere en complexere aanvallen. Leenaars: ‘Zo werd er recent een Oost-Europese crimineel opgepakt die tientallen miljoen verdiende met voorkennis dankzij het onderscheppen van nieuwsberichten.’

Leenaars illustreert wat er mis kan gaan. ‘Een Amsterdammer die vanaf zijn thuiscomputer via e-mail persoonlijke informatie uitwisselt met de gemeente, weet nu niet zeker welke buitenstaanders zijn e-mail allemaal onder ogen hebben gehad.’

Behoorlijk laks
Leenaars zegt dat veel overheidsorganisaties behoorlijk laks zijn als het op informatiebeveiliging aankomt. ‘Ook als ze er al jaren op worden gewezen door externe beveiligingsexperts en organisaties als NCSC en het Forum Standaardisatie. Die laksheid wordt tot nu toe bestuurlijk niet afgestraft, maar gaat wel ten koste van privacy en veiligheid van burgers. En het kan ook flinke economische schade voor ondernemingen tot gevolg hebben.’

Volgens Leenaars zou elke organisatie met een publieke taak in Nederland moeten voldoen aan de standaarden die Internet.nl test. Hij vindt het ‘gênant’ dat op Den Haag na ook de grootste gemeenten zakken voor de test. De beveiliging van e-mail is volgens hem eenvoudig te regelen.

In een reactie aan Binnenlands Bestuur laat de gemeente Amsterdam weten dat er inderdaad nog geen gebruik wordt gemaakt van een aantal standaarden, en dat andere ‘in de voorbereidingsfase ten behoeve van implementatie’ zitten of ‘opgenomen zijn in de planning van dit jaar’. ‘Het is de intentie van de gemeente Amsterdam om volledig aan de genoemde internetstandaarden te gaan voldoen. Dit zal waarschijnlijk in de loop van dit jaar zijn gerealiseerd.’

Leenaars: ‘Als het de gemeenten Heerlen, Simpelveld, Nuth en De Friese Meren lukt om er doorheen te komen, dan ligt de lat echt niet te hoog.’

Verplichte veiligheid eenvoudig te testen
Het voldoen aan internetstandaarden is eenvoudig te testen via de website Internet.nl. De zelftest op de website is opgezet door onder meer het ministerie van Economisch Zaken, het Nationaal Cyber Security Centrum en diverse grote (branche)organisaties die samenwerken in het Platform Internetstandaarden. Deze internetstandaarden, internationale afspraken over de manier waarop de computers ‘met elkaar praten’, zijn inmiddels een aantal jaren oud en zorgen onder meer voor een veilige en betrouwbare manier van internet gebruiken. Verplichte internetstandaarden voor de beveiliging van e-mail die gemeenten niet aanhouden, zoals DNSSEC en DKIM ,staan al jaren op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie. De standaarden op deze lijst zijn verplicht gesteld voor Nederlandse overheidsorganisaties. De verwachting is dat andere standaarden zoals STARTTLS daar snel aan worden toegevoegd.

Korte cursus digitale beveiliging
• Zonder **DNSSEC** zijn verzenders van berichten naar een gemeentelijk adres niet beschermd tegen aflevering bij een valse brievenbus.

• **DKIM** zorgt voor de beveiliging van mailberichten door elk uitgaand bericht van een digitale handtekening te voorzien. Zo wordt voorkomen dat kwaadwillenden een bericht namens een ander kunnen verzenden of een bericht onderweg kunnen veranderen.

• **SPF** voorkomt dat elektronische brievenbussen mailberichten accepteren van ongeautoriseerde computersystemen. Alleen berichten van systemen die daadwerkelijk berichten voor een specifiek domein mogen versturen, komen er doorheen.

• **DMARC** is een aanvulling op de andere twee beveiligingsstandaarden voor e-mail, DKIM en SPF. DMARC geeft elektronische brievenbussen een aanwijzing hoe om te gaan met inkomende berichten waarvan de DKIM- of SPF-controle niet in orde blijkt te zijn. Deze worden bijvoorbeeld automatisch weggegooid.

• **START-TLS** is een uitbereiding van TLS, een cryptografische beveiliging van een internetverbinding. START-TLS zorgt ervoor dat e-mailaccounts zonder TLS alsnog via een beveiligde verbinding kunnen communiceren.

GEMEENTEN HARD BEZIG OM E-MAILBEVEILIGING TE VERBETEREN

Sjoerd Hartholt BB 19 dec 2016

Afgelopen zomer beschikten slechts drie van de vijftig geteste gemeentelijke e-mailsystemen over alle moderne standaarden voor beveiliging, zo bleek uit een onderzoek van *Binnenlands Bestuur*. Meer dan de helft van de onderzochte gemeenten ging er afgelopen halfjaar alsnog mee aan de slag.

Meer dan de helft houdt nu meer standaarden aan
Den Haag, Woerden en Den Bosch hadden hun e-mail deze zomer als enige gemeenten goed beveiligd. Een nieuw onderzoek van Binnenlands Bestuur, uitgevoerd op 2 december, leert dat inmiddels zestien van de vijftig onderzochte gemeenten beschikken over alle moderne standaarden voor beveiliging tegen spam en phishing. Van de overige 34 gemeenten voldoen er nu veertien gemeenten aan meer standaarden dan bij de eerste test. Meer dan de helft van de onderzochte gemeenten heeft de afgelopen maanden de beveiliging van de e-mailsystemen dus verbeterd.

Positieve ontwikkeling
Dat is ook hard nodig, vindt het Nationaal Beraad Digitale Overheid, dat zich eind juni al hard maakte voor de implementatie van moderne beveiligingstandaarden bij e-mail: TLS, DKIM, SPF en DNSsec. Het streven is dat alle overheden de standaarden eind 2017 gebruiken. Ook de Informatiebeveiligingsdienst voor gemeenten (IBD) constateert een positieve ontwikkeling. ‘Wat wij zien is dat gemeenten zonder uitzondering de implementatie van de standaarden op de planning hebben gezet’, zo vertelt IBD-woordvoerder Remco Groet. ‘In samenspraak met bureau Forum Standaardisatie hebben we een pakket aan ondersteuning ontwikkeld dat gemeenten helpt om de standaarden te implementeren. Bij enkele standaarden, zoals DMARC, is implementatie geen sinecure. Een te snelle invoering kan leiden tot mails die niet verzonden of ontvangen worden. Dat is voor een gemeente onacceptabel.’

Andere maatregelen
De IBD ziet dat gemeenten op het gebied van e-mailbeveiliging ‘duidelijk voorlopen’ in vergelijking met andere sectoren. Dat blijkt onder meer uit de toepassing van STARTTLS, de standaard die zorgt voor een veilige verbinding met en tussen e-mailservers. ‘Een goede ontwikkeling’, vindt Groet. ‘De e-mailstandaarden bewijzen echter hun grootste nut als zoveel mogelijk organisaties ze geïmplementeerd hebben, dat gaat dus niet alleen over gemeenten maar is een zaak van overheid en niet-overheid.’
Het voldoen aan internetstandaarden is eenvoudig te testen via de website Internet.nl.

Zelftest
De zelftest op de website is opgezet door onder meer het ministerie van Economische Zaken, het Nationaal Cyber Security Centrum en diverse grote (branche)organisaties die samenwerken in het Platform Internetstandaarden. Deze internetstandaarden – internationale afspraken over de manier waarop de computers onderling communiceren – zijn inmiddels een aantal jaren oud en zorgen onder meer voor een veilige en betrouwbare manier van internet gebruiken. Verplichte internetstandaarden voor de beveiliging van e-mail die gemeenten niet aanhouden, zoals DNSSEC en DKIM ,staan al jaren op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie. De standaarden op deze lijst zijn verplicht gesteld voor Nederlandse overheidsorganisaties.

Meer stappen
Overigens is volgens minister Plasterk het gebruik van de beveiligingsstandaarden een belangrijke, maar niet de enige stap bij de herkenning van spam en phishing. ‘Omdat behalve gebruik van deze standaarden ook andere maatregelen genomen worden, onderschrijf ik niet dat door het enkele feit dat deze standaarden niet worden gebruikt persoonsgegevens in verkeerde handen vallen.’

Onderzochte gemeenten die per 2 december 2016 voldoen aan alle standaarden voor moderne e-mailbeveiliging: Amsterdam, Den Bosch, Den Haag, Dronten, Eersel, Katwijk, Oost Gelre, Staphorst, Veendam, Veenendaal, Vlissingen, Winterswijk, Woerden , Woudenberg, Zaanstad, Zutphen.

Gemeenten die hun e-mailbeveiliging de afgelopen maanden verbeterden: Breda, Brielle, Coevorden, Geertruidenberg, Groningen, Haaksbergen, Haarlemmerliede, Hollands Kroon, Hoorn, Putten, Raalte, Waalwijk, Zuidhorn, Deventer.

Gemeenten die op 2 december (nog) niet aan meer standaarden voldoen dan bij de eerste test in juni: Alblasserdam, Alkmaar, Boxtel, Eindhoven, Enkhuizen, Goes, Heemskerk, Heerde, Hillegom, Hilvarenbeek, Hilversum, Leeuwarden, Molenwaard, Nijmegen, Rhenen, Rotterdam, Texel, Urk, Utrecht, Zwolle.

Microsoft

8 aandachtspunten bij e-mailbeveiliging voor gemeenten

Bijna geen enkele gemeente voldoet aan de verplichte beveiligingsstandaarden voor e-mail. Dat blijkt uit een door *Binnenlands Bestuur* uitgevoerde steekproef bij vijftig gemeenten. Door deze nalatigheid zijn cybercriminelen vaak succesvol met hun phishing-mails en ransomware. Met acht aandachtspunten maak je gemeentelijk e-mailverkeer veiliger.

Afgelopen april was het weer raak. Ondanks maatregelen werden voor een tweede keer phising-mails uit naam van de gemeente Apeldoorn verstuurd. Dit incident staat niet op zichzelf en kan gemakkelijk nog een keer plaatsvinden. Binnenlands Bestuur nam een steekproef met e-maildomeinen van vijftig verschillende gemeenten, daaruit blijken slechts drie gemeenten aan de moderne standaarden voor veilige e-mail te voldoen. Vanwege deze onderzoeksresultaten moeten Nederlandse gemeenten uiterlijk eind 2017 verschillende standaarden hebben geïmplementeerd om hun e-mail te beveiligen. Via acht aandachtspunten kun je een eerste sanity-check uitvoeren op de beveiliging van de e-mail binnen jouw gemeente.

1. Hackers sturen uit naam gemeente phishingmails

Mail spoofing komt vaker voor bij gemeenten. Bij deze manier van fraude worden e-mails verzonden waarbij het e-mail adres van de afzender is vervalst. Dit wordt vaak gebruikt voor spam en phishing. De werkelijke afzender verbergt zijn eigen identiteit om het vertrouwen van de geadresseerde te winnen of zich te beschermen tegen een klacht wegens spammen. In zo'n mail wordt de klant gevraagd om via een link in een e-mail in zijn online account in te loggen. De link leidt naar een pagina die lijkt op de login-pagina van de gemeente, maar dat niet is. Als de ontvanger van de mail in de misleiding trapt, zal hij proberen in te loggen waarmee hij zijn gebruikersnaam en wachtwoord aan de vervalser bekend maakt.

Elke website heeft een nummer als adres: het IP-adres. Omdat amsterdam.nl gemakkelijker te onthouden is dan 46.17.25.12, zijn de domeinnamen in het leven geroepen. Het domeinnaamsysteem (DNS) vertaalt het IP-adres naar een domeinnaam in de nameservers. Het is mogelijk die vertaling te dwarsbomen. Hierdoor kunnen bezoekers op een gekloonde site terechtkomen die voor de bezoeker identiek lijkt aan de vertrouwde site. Maar die site is volledig onder controle van een cybercrimineel.

Microsoft

Met DNSSEC krijgt de vertaling van de domeinnaam naar het IP-adres een digitale handtekening. Deze handtekening wordt automatisch gecontroleerd waardoor een websitebezoeker niet misleid wordt naar een frauduleuze website.

2. E-mailauthenticatie tegen phishingmail

Gemeenten kunnen met e-mailauthenticatie hun domeinnamen beschermen tegen betrouwbaar lijkende phishing e-mails. E-mailauthenticatie zorgt dat onbevoegden niet zomaar de domeinnaam van de gemeente als afzenderadres kunnen misbruiken. Het werkt op basis van de standaarden SPF, DKIM en DMARC waarmee e-mails worden gecheckt op betrouwbaarheid van de afzender.

3. Door beveiligde e-mailverbinding kijken derden niet mee

Nog zeker niet alle gemeenten gebruiken een beveiligde gegevensuitwisseling via TLS. Uit de steekproef bleek dat veertien van de vijftig gemeenten geen beveiligde verbinding kunnen opbouwen. Hierdoor is de e-mailcommunicatie niet volledig afgeschermd voor derden. TLS is een protocol voor het opzetten en gebruiken van een versleutelde, beveiligde verbinding tussen twee computersystemen.

TLS wordt gebruikt voor verschillende toepassingen. Bekende voorbeelden zijn HTTPS voor webverkeer en STARTTLS voor e-mailverkeer. Vanaf 2017 zijn gemeenten verplicht de standaarden DNSSEC, DKIM, DMARC, SPF en TLS te gebruiken om hun mailverkeer veiliger te maken.

4. Minder last van ransomware en cryptoware dankzij de CSO

Gemeenten worden niet alleen geplaagd door phishing-mails. Afgelopen jaren zijn onder andere Vianen, Den Haag, Lochem, Amstelveen en een aantal Friese gemeenten slachtoffer geworden van crypto-en ransomware. Cryptoware versleutelt bestanden op een computer en dwingt daarna de gebruiker te betalen om toegang tot de bestanden te herstellen. Ransomware versleutelt geen bestanden, maar blokkeert toegang tot het systeem totdat er een bedrag is betaald. Crypto- en ransomware, wordt naar vele duizenden e-mailadressen gestuurd. Door op een malafide link te klikken of de bijlage te openen, nestelt de malware zich in het systeem. Daar doet het zijn destructieve werk waardoor documenten niet meer benaderd kunnen worden.

Microsoft

Gemeentegegevens worden het best beveiligd door zowel software als personeel op de hoogte te brengen van de nieuwste beveiligingsregels. Het klikken op een onbetrouwbare e-mail was de oorzaak van de eerder genoemde ransomware-infectie. Een Chief Security Officer zal daarom bij alle collega's erbij moeten aandringen toch echt niet op links van dubieuze mails te klikken.

5. Dankzij goede back-ups snel weer aan het werk

Door regelmatig gegevens op te slaan, en die back-ups weer te back-uppen, raak je documenten en gegevens nooit kwijt en kan het werk snel weer worden opgepakt. Back-up tools zijn tegenwoordig vaak in besturingssystemen ingebouwd en er zijn ook tal van andere goede oplossingen te vinden. De hoeveelheid data die wordt gegenereerd stijgt explosief, maar gelukkig dalen de kosten van schijfruimte in de cloud en het on-premise datacenter. Door het maken van back-ups te automatiseren, loop je de minste kans op grootschalig gegevensverlies. De door ransomware getroffen gemeentes hadden de back-ups goed geregeld waardoor na enkele uren de draad weer kon worden opgepakt.

6. Up-to date software en hardware voor betere veiligheid

Veel kwaadwillende software dringt binnen via gaten in verouderde software, daarom is het noodzakelijk om up-to-date te blijven. Door alle computers (automatisch) uit te rusten met de nieuwste versies, bug-fixes en patches van alle programma's loopt data in netwerk het minste risico. Ook verouderde besturingssoftware van de hardware, de firmware, kan openstaan waardoor cybercriminelen kunnen binnendringen.

7. Houd zakelijk en privé zoveel mogelijk gescheiden

Tegenwoordig krijgen steeds meer ambtenaren de mogelijkheid om met hun eigen laptop of smartphone hun werk te doen. Bring Your Own Device (BYOD)-initiatieven brengt ook gevaar met zich omdat de scheidslijn tussen werk en privé steeds verder vervaagt. Daarom zou op zo'n apparaat een beveiligde werkomgeving moeten zijn waarin alle bedrijfsapplicaties en data gescheiden worden van persoonlijke applicaties en data.

Binnen deze digitale omgeving zouden beperkingen ingesteld moeten worden waardoor gebruikers geen data naar hun persoonlijke omgeving kunnen kopiëren of delen buiten de werkomgeving. Hierdoor en door andere veiligheidsmaatregelen wordt voorkomen dat gegevens verloren gaan. Tegelijk wordt voldaan aan diverse regels rond databeveiliging.

Microsoft

8. Monitor verdachte afwijkingen

Aanvallen van buitenaf vertonen vaak een bepaald patroon dat gekenmerkt wordt door een serie van e-mails met malware. Deze schadelijke software zit al dan niet verstopt in bijvoorbeeld Word- en Excel-bestanden. Het is verdacht als je ineens veel e-mail krijgt uit landen als China en Rusland terwijl je daar geen relatie mee hebt. Het inrichten van een goed detectie- en preventiesysteem helpt bij het vroegtijdig signaleren van dit soort afwijkingen.

Aan de slag met e-mailbeveiliging

Wil je de e-mailbeveiliging op orde krijgen? Neem dan contact op met een van de Microsoft Partners die zich hebben gespecialiseerd in de lokale overheid. Zij kunnen in een diepgaandere analyse bepalen welke kwetsbaarheden binnen jouw gemeente aanwezig zijn. Met functionaliteit in onder meer Office 365 E5, Advanced Threat Protection (ATP), Advanced Security Management (ASM) en Microsoft Enterprise Mobility Suite kun je jouw gemeente beter wapenen tegen inbrekers.

Microsoft

Microsoft

Meer informatie? Kijk dan op:
office.microsoft.com