Onderzoek Informatieveiligheid A2-gemeenten

Rekenkamercommissie Cranendonck, Heeze-Leende, Valkenswaard

December 2020

Rekenkamercommissie
Karin van den Berg
Coen Cransveld
Trude Rietveld

Inhoudsopgave

Deel 1 Kern van het onderzoek

Deel 2 Het onderzoek naar informatieveiligheid

Deel 1 Kern van het onderzoek

1 Samenvatting

De rekenkamercommissie heeft een onderzoek gedaan naar de informatieveiligheid van de gemeenten Cranendonck, Heeze-Leende en Valkenswaard. Er is gekeken naar de beleidskaders rondom informatieveiligheid en de uitvoering daarvan. De rekenkamercommissie keek naar de menselijke kant, de bewustwording van de mensen werd getest door een phishing mail en mystery guest bezoeken. De technische kant is onderzocht door diverse testen (externe en interne pentest, pentest van de werkplek en een pentest van WiFi-Netwerk).
De structuur van informatieveiligheid is op orde. Er kunnen nog wel technische verbeteringen worden doorgevoerd en aandacht voor het onderwerp voor medewerkers blijft belangrijk. Ook kan de rol van de raad nog scherper.

2 Aanbevelingen

- Voor de gemeenteraad:
    1. Ook voor de raadsleden is het van belang dat zij bewuster worden van hun bijdrage aan een veilige dienstverlening van de gemeente ten aanzien van privacy en informatie. Ook zij zullen dus zorgvuldig met bijvoorbeeld wachtwoorden en het delen van informatie moeten omgaan.
    2. Het is aan de raad te controleren dat de informatie die het college verstrekt, voldoende inzicht geeft in de verbeterslagen die noodzakelijk zijn. De rekenkamer is van mening dat dit onderzoek aanleiding geeft om ook als raad meer betrokken te zijn op het thema, bijvoorbeeld door vragen te stellen, door periodiek in gesprek te gaan met de uitvoerend medewerkers over dit thema of door eisen te stellen aan de informatievoorziening op dit vlak. De raad kan een meer gedetailleerd beeld van de acties vanuit het college vragen in een uitgebreide raadsinformatiebrief.
    3. De raad kan doet er goed aan zich te laten inspireren op dit onderwerp door bijvoorbeeld een spreker uit te nodigen.

- Voor de organisatie:
    1. Technische verbeteringen invoeren, zoals multifactorauthenticatie (zo wel intern als extern).
    2. Regelmatig naast zelfaudits ook een externe partij laten kijken naar de wijze waarop de informatiebeveiliging geregeld is.
    3. Bewustwording versterkende maatregelen doorvoeren: nog sterkere wachtwoorden afdwingen, verplicht stellen van het gebruik van een wachtwoordmanager, verbeterde toegangscontrole en fysieke beveiligingsmaatregelen gemeentehuizen.
    4. Blijvend aandacht voor het onderwerp houden; aanbieden van e-learning modules aan medewerkers (en raadsleden), een communicatietraject op intranet, het nog meer uitdragen door de managers en agenderen op werkoverleggen, medewerkers (en raadsleden), persoonlijk aanspreken op verkeerd handelen.
    5. De onderlinge bekendheid vergroten en de anonimiteit van medewerkers verminderen door iedereen op intranet zijn of haar foto te laten plaatsen en door in het digitale profiel in Outlook een foto te laten hangen.
    6. Een bezoekersregister bij laten houden en bezoekers een bezoekerspas laat dragen.

3 Proces in de organisatie

Op 12 augustus 2020 heeft de Rekenkamercommissie de rapportage voor ambtelijke wederhoor aangeboden. De feiten zijn gecheckt en akkoord bevonden. Op 3 november 2020 is de rapportage aangeboden voor bestuurlijke wederhoor. Stand van zaken 9 december 2020:

- Het college van B&W van Heeze-Leende is akkoord conform voorstel
- Het college van B&W van Valkenswaard is akkoord conform voorstel
- Het college van B&W van Cranendonck heeft het voorstel niet besproken

Vanwege de voortgang wordt de rapportage op 9-12-2020 via de griffiers aan de raden aangeboden.

4 Zienswijze vanuit de organisatie

Geachte leden van de Rekenkamer,

Bij deze sturen wij u onze zienswijze op uw onderzoek naar Informatieveiligheid.

Algemene opmerking

De centrale vraag van het rekenkamer onderzoek was of de A2-gemeenten de informatiebeveiliging adequaat ingericht hebben en of voldaan wordt aan de Baseline Informatiebeveiliging Overheid (BIO). Het gaat hierbij om beleid, systemen en de mensen die ermee werken.

Als we het geheel van de bevindingen overzien kunnen we een aantal zaken concluderen:

1. Beleidsmatig zijn al grote stappen gezet door de implementatie van de BIG. De implementatie van de BIO loopt, deze dient in 2020 geïmplementeerd te zijn.
2. De phishing mail verstuurd naar medewerkers en raadsleden, de toegankelijkheid van wachtwoorden en het bezoek van de mystery guest laten het verschil tussen beleid en daadwerkelijke bewustwording zien. Het rapport laat zien dat ongeautoriseerde bezoekers zowel digitaal als fysiek kunnen binnenkomen. En zoals het rapport ook aangeeft, mensen zijn daarin doorgaans de zwakste schakel van elk beveiligingssysteem. Om deze tekortkomingen te beperken willen we inzetten op intensievere bewustwording voor de medewerkers, uitgebreidere fysieke beveiliging, wegwerken analoge dossiers en technische aanscherping in de digitale toegang.

Mogelijke vervolgacties

1. Bewustwording. Hoewel de percentages vergelijkbaar zijn met andere gemeenten, moet de bewustwording binnen onze organisaties sterk verbeterd worden. En dat is bewustwording op alle fronten: van het aanspreken van onbekenden in de afgeschermde ruimtes tot het zorgvuldig opbergen van je documenten. De huidige vrijwillige e-learning over informatie veiligheid zal verplicht gesteld worden. Daarnaast zal deze in het introductieprogramma voor nieuwe medewerkers opgenomen worden en periodiek zullen organisatiebreed opfristrainingen gegeven worden. Er wordt daarnaast een – digitale – wachtwoordkluis voor de medewerkers ingericht die verplicht gebruikt moeten gaan worden.

2. Fysieke beveiliging. De fysieke deur verstevigen en dicht zetten kan door een aantal verbeteringen door te voeren bij de drie panden.
3. Wegwerken analoge dossiers. De inlooptest laat zien dat (vertrouwelijke) fysieke informatie te bereiken is. In de periode januari t/m september 2020 is er in Valkenswaard en Heeze-Leende flink veel werk verzet qua het wegwerken van de ongestructureerde archiefvoorraad met behulp van een inhuurkracht. Het budget dat hiervoor beschikbaar was is verbruikt. Voor het opruimen van de paternosterkasten (dynamische dossiers) is geen budget meer voor inhuur en wordt nu naast het reguliere werk extra opgepakt.
4. Het grondig dichtzetten van de digitale deur kan door het gaan toepassen van MFA (multifactor authenticatie) zoals ook genoemd wordt in het onderzoek. Het traject voor de invoering van MFA is reeds gestart. Verwachte afronding is eerste kwartaal 2021. Het technisch 'aanzetten' van deze authenticatie is niet de uitdaging voor de organisatie. Wel de omvang en de consequenties van dit aanzetten, bv dat hierdoor het benaderen van werkinformatie via eigen apparatuur (bv privé telefoons) niet zondermeer meer mogelijk is. De verschillende scenario's om dit volledig in te voeren worden momenteel uitgewerkt en voorgelegd aan de directieraad. De overig genoemde technisch aanbevelingen uit het rapport zijn of doorgevoerd of worden op korte termijn doorgevoerd. Aanvullend gaan we borgen dat structureel (technische) penetratietesten doorgevoerd worden.

Conclusie

Naast de genoemde positieve punten van de voortgang op beleidsmatig niveau, delen we de hierboven genoemde aanbevelingen.

Directieraad A2

5 Nawoord van de Rekenkamercommissie

De rekenkamercommissie is blij dat de conclusies en aanbevelingen van ons onderzoek naar informatieveiligheid herkend worden, en dat er stappen zijn en worden gezet om met de aanbevelingen aan de slag te gaan. Deze reactie geeft vertrouwen. Informatieveiligheid is in onze ogen een belangrijk onderwerp wat alle 3 de gemeenten aangaat en wat ook belangrijk is voor de inwoners.
Dit was het eerste onderzoek van de nieuwe rekenkamer. Gaandeweg leerden en leren we elkaar kennen en we kijken uit naar een verdere samenwerking.

Rekenkamercommissie A2 gemeenten

Deel 2 Onderzoek Informatieveiligheid

1 Inleiding

Als Rekenkamercommissie ondersteunen we de gemeenteraden bij hun taakstellende en controlerende taak. Dit doen wij door een of twee keer per jaar een onderzoek te doen en daarover een rapport uit te brengen aan de raad. Het eerste onderzoek van de nieuwe rekenkamercommissie is het onderzoek naar Informatieveiligheid in alle drie de gemeenten. Als eerste onderzoek hebben we een onderwerp gekozen wat zeer relevant is voor alle drie de gemeenten.
Onder informatieveiligheid of informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.
Informatie is voor elke organisatie van groot belang, daarbij is het belangrijk dat die informatie veilig is. Onder veiligheid van informatie wordt verstaan dat deze vertrouwelijk (exclusief), betrouwbaar (integer) en beschikbaar is. Het is niet de bedoeling dat deze informatie op straat komt te liggen. Ook is het niet de bedoeling dat derden onbevoegd toegang hebben tot de informatiesystemen van gemeenten en zo het dingen kunnen aanpassen of de voortgang van lopende projecten beïnvloeden. Inbreuken kunnen leiden tot financiële en/of materiële schade en tot reputatieschade voor de gemeenten.
Informatieveiligheid richt zich op de beheersing van bovenstaande risico's. Het onderzoek naar informatieveiligheid vond plaats bij de Gemeenschappelijk Regeling A2.

Samenwerking met Hoffmann

Voor de uitvoering van het onderzoek hebben we gebruik gemaakt van de diensten van Hoffmann, gespecialiseerd in cybersecurity. De rapportage van Hoffmann bevat gevoelige informatie. De rapportage is bij de CISO van de A2 gemeenten bekend. In deze rapportage hebben we in de bijlage informatie van Hoffmann opgenomen, zonder de details van de gevoeligheden weer te geven.

Doelstelling en vraagstelling

Het doel van dit onderzoek was: Inzicht geven in de huidige staat van de informatiebeveiliging bij de A2-gemeenten en de gevolgen hiervan alsmede het – indien nodig - formuleren van concrete verbeteracties.

De centrale vraag van dit onderzoek luidde dan ook:
Hebben de A2-gemeenten de informatiebeveiliging adequaat ingericht? En voldoet het systeem aan de normen van het Baseline Informatiebeveiliging Overheid?

We onderzochten daartoe enerzijds de mate waarin het systeem voor onbevoegden toegankelijk is en anderzijds de mate waarin de medewerkers handelen op een manier die de informatieveiligheid bewaakt. Ook onderzochten we het beleid en de organisatie van de informatiebeveiliging.

De Rekenkamercommissie doet met haar onderzoek aanbevelingen die bijdragen aan een verbetering van de informatieveiligheid van de samenwerkende A2 gemeenten; Cranendonck, Heeze-Leende en Valkenswaard.

Leeswijzer

In ons onderzoek naar informatieveiligheid richtten we ons op het beleid, het systeem en de mensen. In de volgende hoofdstukken behandelen we de drie velden. In hoofdstuk 5 staan de conclusies genomen, in hoofdstuk 6 de aanbevelingen. In de bijlage is een samenvatting van het rapport van Hoffmann opgenomen en een verklarende lijst met afkortingen.

2 Onderzoeksterrein beleid

Voor het beleid onderzochten we de opgestelde documenten en hielden we gesprekken met personen die verantwoordelijk zijn voor de informatieveiligheid binnen de gemeenten. We brachten in kaart in hoeverre de gemeenten de sturing op, de beheersing van en de verantwoordelijkheid voor informatieveiligheid goed heeft verankerd. Ook keken we op welke wijze de gemeenteraden worden geïnformeerd over informatieveiligheid.

Baseline Informatiebeveiliging Overheid

Gemeenten, Rijk, waterschappen en provincies zijn op 1 januari 2020 overgegaan op een nieuw uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Voor gemeenten was 2019 een voorbereidingsjaar. Op 1 januari 2020 is de BIO de officiële richtlijn op het gebied van informatiebeveiliging die alle gemeenten volgen.
De A2 gemeenten werken volgens de BIO. Het beleid is vastgesteld door de colleges. Er is een gedragscode opgesteld, en deze is ook vastgesteld. In de code is aandacht voor alle facetten van informatieveiligheid. De code geeft aan hoe medewerkers om moeten gaan met informatie, wachtwoorden, melden van datalekken et cetera.
Ook is een governacestructuur opgezet waarin duidelijk de taken en rollen omtrent de informatieveiligheid zijn beschreven. De functies uit het Governance document zijn ingevuld.
Er is een procedure datalekken.

Het informatiebeveiligingsbeleid in de gemeenten

Voor de vier A2-organisaties (de drie gemeenten en de A2-Samenwerking (GRSA2)) is op basis van de BIG/BIO een Chief Information Security Officer (CISO) opgenomen in de organisatie, die optreedt als spin in het web als het gaat om de beveiliging van informatie binnen de gemeente. Hij is verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid binnen de gemeente, alsmede het gevraagd en ongevraagd adviseren van het management betreffende de noodzaak van te nemen maatregelen.
Voor de A2-organisaties is op basis van de AVG een Functionaris Gegevensbescherming (FG) opgenomen in de organisatie, die als onafhankelijke deskundige optreedt op het gebied van gegevensbescherming en is aangewezen om te adviseren, informeren en toezicht te houden op de naleving van de AVG. De FG richt zich dus met name op privacy, wat geen onderdeel uitmaakt van dit onderzoek.
Ook is een ENSIA-coördinator aangewezen. Ensia houdt in Eenduidige Normatiek Single Information Audit en heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus.
Alle gemeenten dienen jaarlijks verantwoording af te leggen middels een zelfevaluatie ENSIA. De ENSIA Coördinator verzorgt de verantwoording over informatiebeveiliging en privacy en Waar Staat Je Gemeente, onderdeel informatiebeveiliging. In deze zelfevaluatie zit tevens de verantwoording verwerkt over de volgende informatiesystemen:

- DigiD
- Suwinet
- BAG (Basisregistratie Adressen en Gebouwen
- BGT (Basisregistratie Grootschalige Topografie)
- PUN (Paspoort Uitvoeringsregeling Nederland, reisdocumenten)
- BRP (Basisregistratie Personen)
- BRO (Basisregistratie Ondergrond).

De ENSIA Coördinator houdt overzicht over de lopende acties rondom het ENSIA traject, de vragen die nog beantwoord dienen te worden en de onderlinge afstemming. Daarnaast is hij aanspreekpunt voor collega's bij vragen over ENSIA, en onderhoudt hij contacten met de IT-auditor, de ministeries van BZK en SZW, de beheerder van ENSIA en VNG-Realisatie. De rol van ENSIA Coördinator wordt op dit moment ingevuld door de CISO en hij rapporteert over de voortgang en uitkomsten van de zelfevaluatie ENSIA aan het OGON.

Toetsing van het normenkader gebeurt via ENSIA. Dit is natuurlijk een zelfevaluatie waarbij gemeenten zichzelf toetsen. In tegenstelling tot de BIG is voldoen aan de BIO een stuk complexer. De BIO bestaat uit een aantal generieke basismaatregelen, ook O-maatregelen of overheidsmaatregelen genoemd. Deze worden via de ENSIA getoetst en komen voor een groot deel overeen met de maatregelen uit de BIG waardoor de meeste maatregelen al zijn geïmplementeerd. Daarnaast dient elke gemeente, voor al haar processen, op basis van risicoanalyses aanvullende beveiligingsmaatregelen te nemen. Het toetsen van deze beveiligingsmaatregelen zou een rol kunnen zijn van de CISO, die hiervoor input krijgt van gebruikers, applicatie- en gegevensbeheerders en ICT. In de praktijk gebeurt dit nog nauwelijks doordat implementatie nog plaats vindt, beperkte capaciteit en andere prioriteiten.

Gedragen beleid in de organisatie

Privacybescherming en informatiebeveiliging binnen alle processen en systemen vallen onder de verantwoordelijkheid van de afdelingsmanagers. De afdelingen zijn zich daarvan bewust. Directie, bestuur en afdelingsmanagement kennen het beleid op het gebied van informatieveiligheid en geven hieraan invulling. Er wordt zorgvuldig gekeken naar de niveaus van toegang van digitale informatie die medewerkers nodig hebben om hun werk te kunnen doen. Medewerkers worden geschoold, bijvoorbeeld door workshops, webinars en e-learning, en in teamoverleggen wordt hieraan aandacht besteed. Er wordt gewerkt met een 'druppel' om de gebouwen te kunnen betreden. Medewerkers krijgen een telefoon en laptop van de gemeenten in gebruik. Daarnaast wordt er zo weinig mogelijk gewerkt met papieren dossiers en zijn de ruimten waar papieren dossiers worden bewaard afgesloten.

Betrokkenheid gemeenteraden

Aan alle drie de raden is een presentatie gegeven over informatieveiligheid en privacy. Door de verschillende fracties wordt de informatie en bekendheid met het onderwerp divers beleefd, van 'een prima beleid' tot 'we kennen het beleid niet'.
De raden worden ook via een Raadsinformatiebrief op de hoogte gehouden van diverse zaken. Jaarlijks wordt de ENSIA verantwoording gedeeld met de raad en in het jaarverslag wordt de raad geïnformeerd over het onderwerp informatieveiligheid. Ook hierover zijn de meningen van de fracties verdeeld. Een aantal lijkt de brief niet te kennen, een aantal is hierover goed te spreken, een van de fracties is ook goed op de hoogte door de ENSIA verantwoording.

3 Onderzoeksterrein systeem

Tijdens het technische onderzoek is door Hoffmann getoetst of de informatiesystemen van de gemeenten voldoende beveiligd zijn tegen het risico van hacken. De techniek is getest door middel van de volgende vier testen:

1. Externe penetratietest (hierna genoemd: pentest), uitgevoerd vanaf het internet. Hierbij is op zoek gegaan naar systeemnamen en netwerkcomponenten van de gemeente. De uiteindelijke reikwijdte is afgestemd met de CISO (coördinator informatieveiligheid) van de A2-Samenwerking;
2. Pentest werkplek; de onderzoekers hebben de pentest uitgevoerd op 'werkplek.a2samenwerking.nl' vanaf het internet. Hierbij is een gebruikersaccount aangeleverd door de A2-Samenwerking. Dit gebruikersaccount is representatief voor de verkregen inloggegevens die bemachtigd zijn tijdens de mail phishing en password spraying. Vervolgens zijn verschillende pogingen ondernomen om privilege escalation (verhoogde toegang) te krijgen tot de server en de infrastructuur van de organisatie;
3. Pentest intern; de onderzoekers hebben op een flexwerkplek bij de gemeente Cranendonck, representatief voor de overige twee gemeenten, een intern onderzoek uitgevoerd. Hierbij zijn meegebrachte laptops op het netwerk aangesloten. Vervolgens zijn verschillende kwetsbaarhedenscans uitgevoerd en pogingen ondernomen om de aangetroffen kwetsbaarheden te misbruiken;
4. Pentest WiFi-Netwerk; de onderzoeker heeft tijdens de test een 'Rogue Acces Point' opgezet en een Man In the Middle (MITM)-aanval uitgevoerd op het SSID 'govroam'.

Externe pentest

Om de kwetsbare websites van de gemeente in kaart te brengen is extern (vanaf het internet) gestart met het uitvoeren van een geautomatiseerde kwetsbaarhedenscan. Hierbij kwamen geen bijzondere kwetsbaarheden naar boven. Wel is er een aantal verbeterpunten om de beveiliging van de digitale infrastructuur verder te optimaliseren. Zo is er via een wachtwoordaanval op de webmail toegang verkregen tot diverse mailboxen. Doordat er geen gebruik van multifactorauthenticatie (MFA) wordt afgedwongen, is het zeer eenvoudig om achterhaalde inloggegevens te misbruiken.

Pentest werkplek

De onderzoekers zijn erin geslaagd (met een verstrekt representatief medewerkersaccount) binnen 24 uur de controle te krijgen over de digitale infrastructuur van A2-Samenwerking. Om gebruik te maken van de werkplek is extern (vanaf het internet) MFA nodig. Intern op locatie is dit niet het geval, waardoor onbevoegde personen toegang kunnen krijgen tot het netwerk. De macro-instellingen voor Microsoft Office bleken correct ingesteld. Veel malware (schadelijke software) wordt namelijk verspreid via documenten met daarin een macro. Uiteindelijk is het wachtwoord verkregen van een serviceaccount. Met dit serviceaccount is vervolgens toegang verkregen tot nagenoeg het hele netwerk van A2-Samenwerking. Zo was het bijvoorbeeld in theorie mogelijk om de wachtwoorden van de burgemeesters aan te passen. Het bleek verder dat een significant aantal medewerkers zeer zwakke wachtwoorden in gebruik heeft, waardoor van 705 gebruikers (69% van de 1029) het wachtwoord in korte tijd achterhaald kon worden aan de hand van een woord uit het woordenboek. Ook in de persoonlijke homefolders van de medewerkers zijn wachtwoorden van gemeenteapplicaties aangetroffen in leesbare tekst.
Daarnaast waren er enkele digitale kopieën aanwezig van identiteitsbewijzen en waren er configuratiebestanden aanwezig met daarin wachtwoorden.

Interne pentest

Om nog meer kwetsbare systemen in de digitale infrastructuur van de gemeentes in kaart te brengen is een geautomatiseerde kwetsbaarhedenscan op locatie bij de gemeente Cranendonck uitgevoerd. Door het ontbreken van netwerkauthenticatie was het mogelijk om de eigen laptop aan te sluiten op het netwerk van de gemeente, zonder authenticatie. De laptop komt overigens wel in een afgesloten netwerk terecht. Door het MAC-adres van een thin client te hergebruiken was het mogelijk om in een ander (opener) netwerksegment te komen en een kwetsbaarhedenscan toe te passen. Verder bleek een aantal beveiligingsupdates niet te zijn toegepast. Daarnaast wordt er gebruik gemaakt van verouderde besturingssystemen, waarvan Microsoft de ondersteuning heeft gestopt. Het gevolg hiervan is dat er geen beveiligingsupdates meer beschikbaar worden gesteld.

Pentest WiFi-netwerk

Het was mogelijk om een vals WiFi access point op te zetten en gebruikersnaam en wachtwoord van een gebruiker te achterhalen. Het valse access point werd wel door een systeembeheerder gedetecteerd. Indien het access point zich buiten de gebouwen van de gemeente bevind, bijvoorbeeld in de supermarkt, is deze technische manier van detecteren echter niet mogelijk.

4 Onderzoeksterrein de mens

Mensen zijn doorgaans de zwakste schakel van elk beveiligingssysteem. Het bewustzijn van de medewerkers is getest door middel van de volgende twee manieren:

1. Mail phishing, waarbij er een e-mail is verstuurd die uitnodigde om op een link te klikken en de gebruiker te verleiden om persoonlijke inloggegevens af te geven;
2. Mystery guest bezoek, waarbij een medewerker van Hoffmann heeft geprobeerd om zonder toestemming toegang te krijgen tot de gemeentelijke werkplekken.

Mail phishing

Met het versturen van een phishing e-mail is het bewustzijn van de medewerkers en raadsleden ten aanzien van het herkennen van een nepmail getoetst. Naar aanleiding van 864 verstuurde phishing e-mails hebben 198 gebruikers (23%) de unieke link in de e-mail geopend. In totaal zijn er 157 inlogpogingen van unieke gebruikers met geldige e-mailadressen geregistreerd (18%). De genoemde percentages zijn vergelijkbaar met andere gemeenten waar dit scenario is toegepast, maar laat tegelijkertijd zien dat een significant deel van medewerkers gevoelig is voor dergelijke aanvallen.

Mystery guest bezoek

Een medewerker van Hoffmann heeft een fysieke inlooptest bij de gemeentes Cranendonck, Heeze-Leende en Valkenswaard uitgevoerd, met als doel toegang te krijgen tot vertrouwelijke informatie. Vastgesteld is dat het voor onbevoegden mogelijk is om de panden van de gemeentes te betreden en om toegang te verkrijgen tot ruimtes die niet toegankelijk zijn voor publiek (kantooromgeving). Tijdens de inlooptesten werd de onderzoeker nauwelijks op zijn aanwezigheid aangesproken.

5 Conclusies

De structuur van informatieveiligheid is op orde

De A2 gemeenten werken volgens de regels van de Baseline Informatiebeveiliging Overheid (BIO). Het beleid en gedragscodes zijn vastgesteld. In de code is aandacht voor alle facetten van informatieveiligheid. De code geeft aan hoe medewerkers om moeten gaan met informatie, wachtwoorden, melden van datalekken et cetera. Ook is een governancestructuur opgezet waarin duidelijk de taken en rollen omtrent de informatieveiligheid zijn beschreven.

Er is een procedure datalekken. Voor de vier A2-organisaties is op basis van de BIG/BIO een governancesturctuur opgesteld en deze is ingevuld. Alle gemeenten leggen jaarlijks verantwoording af middels een zelfevaluatie ENSIA. Sinds 2019 wordt jaarlijks een penetratietest uitgevoerd. De ENSIA-coördinator stuurt op informatiebeveiliging, hierin ondersteund door de externe IT-auditor die onderzoekt in hoeverre de noodzakelijke beveiligingsmaatregelen zijn genomen rondom het gebruik van DigiD en Suwinet. Op basis van eventueel geconstateerde tekortkomingen stuurt de CISO op het oplossen van deze tekortkomingen, in overleg met het verantwoordelijk management en ICT. De gemeenten hebben niet te maken met grote datalekken, een enkele keer met een klein lek. De raden worden over de aard en omvang van datalekken op hoofdlijnen geïnformeerd via de paragraaf in het jaarverslag. Als er een datalek van grotere omvang plaatsvindt, worden de raden direct geïnformeerd, middels e-mail of een raadsinformatiebrief.

Directie, bestuur en afdelingsmanagement kennen het beleid op het gebied van informatieveiligheid en geven hieraan invulling. Er zijn vooralsnog voldoende middelen beschikbaar.
Er is aandacht voor de niveaus van toegang van digitale informatie die medewerkers nodig hebben om hun werk te kunnen doen. Medewerkers worden geschoold, bijvoorbeeld door workshops, webinars en e-learning, en in teamoverleggen wordt hieraan aandacht besteed. Er wordt gewerkt met een ‘druppel’ om de gebouwen te kunnen betreden. Er wordt zo weinig mogelijk gewerkt met papieren dossiers en de ruimten waar papieren dossiers worden bewaard zijn afgesloten, al blijkt het mogelijk hier toegang tot de krijgen.

De informatievoorziening is kwetsbaar

Ondanks de inspanning op gebied van informatieveiligheid blijkt er uit de uitgevoerde tests door Hoffmann dat er nog ruimte is voor verbetering.
Het toetsen van de beveiligingsmaatregelen gebeurt in de praktijk nog nauwelijks doordat implementatie nog plaatsvindt, beperkte capaciteit en andere prioriteiten.

Er zijn geen bijzondere kwetsbaarheden naar boven gekomen via de ‘externe pentest’. Uit de ‘pentest werkplek’ kwam naar voren dat medewerkers soms teveel rechten hebben, een groot aantal medewerkers zwakke wachtwoorden gebruikt en wachtwoorden opslaan in leesbare tekst in homefolders.

Uit de ‘interne pentest’ kwam dat er beveiligingsmaatregelen genomen zijn maar dat er aandachtspunten blijven, met name het gebruik van verouderde besturingssystemen en het toepassen van beveiligingsupdates. Via de ‘pentest wifi netwerk’ bleek het mogelijk om via het WiFi-netwerk de inloggegevens en wachtwoorden van gebruikers te achterhalen.
Het resultaat van de phishing mail laat zien dat een deel van de medewerkers zich bewust was dat de mail een phishing mail betrof maar dat er nog ruimte is voor verbetering.

Vastgesteld is dat het voor onbevoegden mogelijk is om de panden van de gemeentes te betreden en om toegang te verkrijgen tot ruimtes die niet toegankelijk zijn voor publiek (kantooromgeving). Een mysteryguest is er op eenvoudige wijze in geslaagd om diverse (vertrouwelijke) fysieke informatie te bereiken bij de gemeentes Cranendonck, Heeze-Leende en Valkenswaard. Het is mogelijk om de eigen laptop aan te sluiten op het netwerk van de gemeente, zonder authenticatie.

De phishing mail, de toegankelijkheid van wachtwoorden en het bezoek van de mystery guest laten het verschil tussen beleid en daadwerkelijke bewustwording zien.

6 Aanbevelingen

Technische verbeteringen invoeren

Ter verbetering van de informatieveiligheid kan technisch gedacht worden aan multifactorauthenticatie (zo wel intern als extern), nog sterkere wachtwoorden afdwingen, verplicht stellen van het gebruik van een wachtwoordmanager, verbeterde toegangscontrole en fysieke beveiligingsmaatregelen gemeentehuizen.

Blijvend aandacht voor het onderwerp houden

Bewustwording van informatieveiligheid is een blijvend belangrijk aandachtspunt. Er wordt al veel aandacht aanbesteed, maar we signaleren nog een aantal kwetsbaarheden. De e-learning modules leveren zeker een bijdrage aan de bewustwording. Gezien de bevindingen zal een combinatie gevonden moeten worden met andere bewustwording versterkende maatregelen gecombineerd met technische maatregelen. Dit moet natuurlijk nog worden uitgewerkt op basis van deze bevindingen, maar te denken valt aan een communicatietraject op intranet, het nog meer uitdragen door de managers en agenderen op werkoverleggen, medewerkers (en raadsleden) persoonlijk aanspreken op verkeerd handelen en dergelijke
De controles die op dit moment zijn ingericht op de informatiebeveiliging, zijn zelfaudits. We raden aan om periodiek ook een externe partij mee te laten kijken naar de wijze waarop de informatiebeveiliging geregeld is.

Vergoot de onderlinge bekendheid

Vergroot de onderlinge bekendheid en verminder de anonimiteit van medewerkers door iedereen op intranet zijn of haar foto te laten plaatsen en door in het digitale profiel in Outlook een foto te laten hangen.
Laat een bezoekersregister bijhouden en laat bezoekers een bezoekerspas dragen.

De rol van de raad kan scherper

De raadsleden zijn niet allemaal op de hoogte van de stand van zaken van informatiebeveiliging. Ook voor de raadsleden is het van belang dat zij bewuster worden van hun bijdrage aan een veilige dienstverlening van de gemeente ten aanzien van privacy en informatie. Ook zij zullen dus zorgvuldig met bijvoorbeeld wachtwoorden en het delen van informatie moeten omgaan.
De informatieverstrekking lijkt op orde, maar dat wordt door de raadsleden niet zo ervaren. De raad stelt weinig vragen over informatieveiligheid. De rekenkamer is van mening dat dit onderzoek aanleiding geeft om ook als raad meer betrokken te zijn op het thema, bijvoorbeeld door vragen te stellen, door periodiek in gesprek te gaan met de uitvoerend medewerkers over dit thema of door eisen te stellen aan de informatievoorziening op dit vlak. De raad kan een meer gedetailleerd beeld van de acties vanuit het college vragen in een uitgebreide raadsinformatiebrief.
Aandacht van de raad kan gewekt worden door een bijeenkomst specifiek over dit onderwerp. Omdat het onderwerp niet leeft, is het goed om een inspirerend spreker uit te nodigen. Dit kan raadsleden inspireren om hun rol te pakken op dit onderwerp.

Bijlage 1 Samenvatting onderzoek Hoffmann

Mens (Social Engineering)

Bevinding	Risico	Impact	Aanbeveling
Kwetsbaarheid voor phishing e-mails	Hoog	Hierbij wordt getracht inloggegevens te achterhalen. Wanneer een kwaadwillende over deze gegevens beschikt kan hij zich daar toegang mee verschaffen tot de systemen van de A2-gemeenten.	Leer medewerkers hoe zij phishing e-mails kunnen herkennen. Zorg dat medewerkers weten hoe te handelen in geval van twijfel. Maak gebruik van MFA voor alle met het internet verbonden systemen.
Het was mogelijk om ongeautoriseerd het beveiligde gedeelte van de drie gemeentes te betreden.	Hoog	Er bleken (vertrouwelijke) documenten fysiek toegankelijk te zijn op verschillende werkplekken / kasten.	Maak medewerkers bewust van inlooptechnieken door bewustwording en gedrags-veranderingsprogramma's. Maak daarnaast medewerkers bewust van hoe om te gaan met waardevolle informatie. Bewaar vertrouwelijke informatie op afgesloten plaatsen en zie er ook op toe dat dit gebeurt. Verbeter de toegangscontrole van de gemeentes.

Externe pentest

Bevinding	Risico	Impact	Aanbeveling
Ontbreken van security headers op diverse websites.	Gemiddeld	Maken bezoekers vatbaar voor mogelijke aanvallen.	Configureer de ontbrekende security headers op de verschillende websites.
Exchange Admin Center en Web Service toegankelijk	Gemiddeld	Via het beheercenter kunnen beheertaken uitgevoerd worden, zoals het aanmaken, wijzigen en verwijderen van gebruikersaccounts, het wijzigen van wachtwoorden van gebruikers et cetera.	Maak Exchange Admin Center en Web Services niet publiek toegankelijk vanaf het internet. Beperk de toegang tot bekende IP-adressen.
Password Spraying mogelijk op Outlook Web App.	Kritiek	Bij een geslaagde aanval heeft de aanvaller toegang tot de mailbox.	Monitor veelvuldige (foutieve) inlogpogingen om te detecteren wanneer dergelijke aanvallen plaatsvinden, zodat de gebruikte IP-adressen geblokkeerd kunnen worden. Dwing daarnaast MFA af.
Ontbreken van MFA.	Kritiek	Het is voor een kwaadwillende mogelijk om alleen met een gebruikersnaam een wachtwoord in te loggen.	Wij adviseren dringend om overal waar mogelijk, met name voor systemen die benaderbaar zijn vanaf het internet, MFA af te dwingen.
Toegang tot mailbox klantcontactcentrum (KCC).	Hoog	Een kwaadwillende met het juiste wachtwoord kan vertrouwelijke informatie uit de mailbox halen van het KCC.	Maak gebruik van MFA; Maak medewerkers bewust van het risico dat het opslaan van wachtwoorden in leesbare tekst met zich meebrengt.
Monitoring externe server 'srv-mbg03' inzichtelijk.	Laag	Gedetailleerde informatie van de server is inzichtelijk. Zo was het mogelijk om de belasting van het netwerkverkeer en het geheugen uit te lezen.	Stel de monitoring server niet beschikbaar voor het internet en beperk de toegang tot bekende IP-adressen.

Pentest werkplek

Bevinding	Risico	Impact	Aanbeveling
MFA op Citrix extern aanwezig, maar intern niet.	Gemiddeld	Kwaadwillenden die beschikken over geldige logingegevens kunnen intern in het gemeente-huis inloggen op Citrix zonder gebruik te maken van MFA.	Maak ook intern gebruik van MFA.
Command Shells uitvoerbaar.	Kritiek	Het is mogelijk om via Command shellprogramma's de controle te krijgen over het hele netwerk.	Beperk de toegang tot de Command shellprogramma's zoals PowerShell en Command Prompt met behulp van Application Control.
Koadic Command Shell uitvoerbaar.	Hoog	Kwaadwillenden kunnen door een Command Shell opdracht tot op een beperkte hoogte de controle krijgen over de Citrix-server.	Beperk de toegang tot de Command shellprogramma's zoals PowerShell en Command Prompt met behulp van Application Control.
Kerberoasting mogelijk vanuit Command Shell.	Kritiek	Een aanvaller kan offline brute force-aanvallen uitvoeren om het wachtwoord te trachten te kraken en dit wachtwoord gebruiken voor verdere exploitatie van het netwerk.	Stel zeer lange wachtwoorden in (meer dan 25 karakters), geef serviceaccounts geen domain administrator-rechten. Overweeg daarnaast het gebruik van Managed Service Accounts.
Toegang tot Domain Controller.	Kritiek	Het aanmaken van een account maakt het simpeler voor een kwaadwillende om terug te keren.	Monitor de activiteiten in 'Active Directory Users and Computers'
Zeer zwakke wachtwoorden in gebruik.	Kritiek	Kwaadwillenden kunnen de wachtwoorden eenvoudig raden doordat de woorden voorkomen in het woordenboek.	Maak medewerkers bewust van het risico dat gebruik van zwakke wachtwoorden met zich meebrengt. Promoot het gebruik van 'wachtzinnen'.
Wachtwoorden aanwezig in persoonlijke homefolders.	Hoog	Aanvallers met voldoende rechten kunnen in de persoonlijke homefolders van de medewerkers op zoek gaan naar wachtwoorden en deze lezen omdat ze opgeslagen zijn in leesbare tekst.	Maak medewerkers bewust van het risico dat het opslaan van wachtwoorden in leesbare tekst met zich meebrengt. Laat medewerkers hun wachtwoord opslaan in een wachtwoordkluis.
Wachtwoorden aanwezig in Active Directory notities.	Gemiddeld	Elke gebruiker kan het wachtwoord van accounts lezen.	Zet geen wachtwoorden in de beschrijving van de Active Directory-gebruiker of andere velden, maar sla deze op in een password manager.
Macro's in Microsoft Office staan uitgeschakeld	Informatief	Sommige macro's kunnen beveiligingsrisico's vormen. Voor deze configuratie niet van toepassing.	Handhaaf het gebruik van het niet automatisch starten van Macro's.
Export Outlook gegevensbestand inzichtelijk.	Hoog	Inhoud van mailbox van andere gebruiker kon ingezien worden.	Kijk kritisch naar de bestanden die beschikbaar zijn gesteld. Pas waar nodig de rechten aan van de netwerk-share.
Key2-applicaties benaderbaar.	Hoog	Kwaadwillenden kunnen toegang krijgen tot de applicaties 'Key2financien', 'Key2Burgerzaken', 'Key2Betalen'.	Zorg ervoor dat de medewerkers geen wachtwoorden in leesbare tekst opslaan.

Gevoelige informatie aanwezig in homefolder en netwerkshares.	Hoog	Door misbruik te maken van het gebruikersaccount 'Front KCC1' is er gevoelige informatie benaderbaar. Zoals kopie van identiteitsbewijzen en wachtwoorden in configuratie bestanden.	Maak medewerkers bewust van het risico dat het opslaan van identiteits-bewijzen met zich meebrengt; Gebruik geen logingegevens in (configuratie bestanden).

Interne pentest

Bevinding	Risico	Impact	Aanbeveling
Geen netwerkauthenticatie aanwezig.	Gemiddeld	Kwaadwillenden met fysieke toegang kunnen ongeautoriseerde apparatuur met het netwerk verbinden om verkenningen en aanvallen uit te voeren.	Maak gebruik van netwerkauthenticatieprotocol 802.1AE/MACsec, schakel ongebruikte netwerkpoorten uit.
Hergebruik MAC-adres mogelijk.	Gemiddeld	Kwaadaardige software kan vrij communiceren. Op het interne netwerk is het aanvals-oppervlak onnodig groot.	Maak gebruik van netwerk-authenticatievoorzieningen, zoals 802.1AE/ MacSec; Schakel ongebruikte netwerkpoorten uit en/of monitor het gebruik van onbekende MACadressen.
Beveiligingsupdates niet toegepast.	Kritiek	Ontbrekende beveiligings-updates kunnen in veel gevallen leiden tot ongeautoriseerde toegang tot systemen en/of gegevens.	Pas de ontbrekende beveiligings-updates toe aan de hand van de resultaten uit de kwetsbaarhedenscan.
Verouderd besturingssysteem aangetroffen.	Kritiek	Er komen geen beveiligings-updates meer beschikbaar voor systemen die niet langer ondersteund worden door de leverancier, waardoor deze kwetsbaar blijven.	Maak uitsluitend gebruik van door de leverancier ondersteunde software.

Pentest WiFi-netwerk

Bevinding	Risico	Impact	Aanbeveling
Rogue Access Point (gebruikersnaam en wachtwoord van een enkele gebruiker is achterhaald).	Hoog	Gebruikersnamen en wachtwoorden kunnen opgevangen worden.	Maak gebruik van EAP-TLS met client certificaten en zorg dat de client /server beide elkaars certificaten valideren.

Bijlage 2 Lijst met afkortingen

AVG	Algemene verordening gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CISO	Chief Information Security Officer. Centrale persoon als het gaat om de beveiliging van informatie
E-learning	Online opleiden
Ensia	Eenduidige Normatiek Single Information Audit (het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus)
FG	Functionaris Gegevensbescherming
Govroam	Govroam wifinetwerk voor medewerkers in de publieke sector bij de eigen organisatie of op de gastlocatie
Mail phishing	Vorm van digitale oplichting waarin via de mail naar gegevens wordt gevraagd
MFA	Multifactorauthenticatie is een controlemethode waarbij de online gebruiker meerdere stappen succesvol moet doorlopen om ergens toegang tot te krijgen
MITM	Man in the middle aanval is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Hierbij bevindt de computer van de aanvaller zich tussen de twee communicerende partijen
Mysteryguest	Onaangekondigde bezoeker
OGON	Opdrachtgever-opdrachtnemer overleg
Password spraying	Aanval met een veelheid aan veel voorkomende wachtwoorden om systeem binnen te komen
Pentest	(Penetratie)test om te onderzoeken of ICT-infrastructuur veilig is
Rogue Acces Point	Een draadloos toegangspunt dat is geïnstalleerd op een beveiligd netwerk zonder uitdrukkelijke toestemming van een lokale netwerkbeheerder.
SSID	Service Set Identifier is een naam ter identificatie van een specifiek draadloos netwerk waarmee je verbonden bent
SZW	Ministerie van Sociale Zaken en Werkgelegenheid
VNG	Vereniging van Nederlandse Gemeenten