INFORMATIEVEILIGHEID, SMART & SAFE?

Rekenkamerrapport

EINDHOVEN

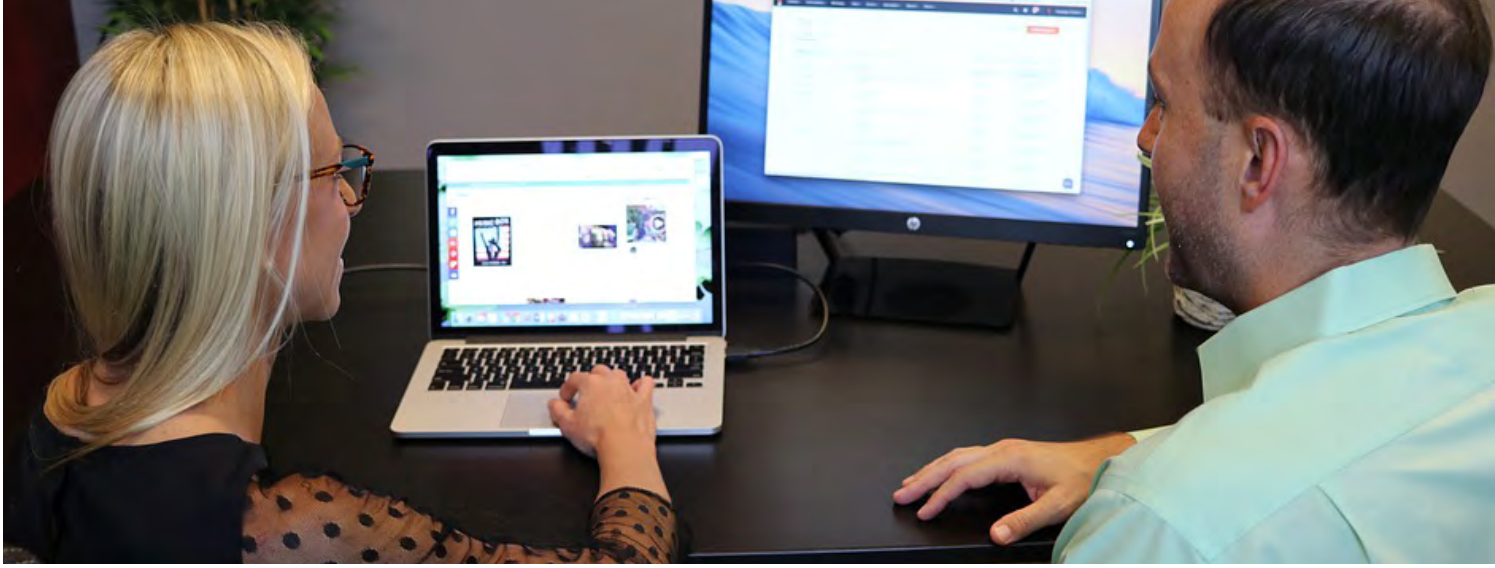
REKENKAMERCOMMISSIE

November 2021

INHOUDSOPGAVE

COLOFON

November 2021
W. Hartmann voorzitter
J. Verhagen vicevoorzitter
E. de Bruijn lid
W. van Haalen lid
H. Jager lid
A. Topdag lid
T. van den Biggelaar secretaris/onderzoeker



INLEIDING

Informatieveiligheid binnen de gemeente is van groot belang. Voor inwoners om te garanderen dat de gemeentelijke dienstverlening doorgaat, dat paspoorten verstrekt worden, dat inwoners kunnen vertrouwen op inkomensondersteuning met waarborg van hun persoonsgegevens. Maar ook van groot belang is de bescherming van gegevens over ruimtelijke projecten, financiën en veiligheid in de stad. Recente hackincidenten en de impact bij lokale overheden en bedrijven onderstrepen dit belang. Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude, ondermijning en ontwrichting op de loer.

Informatiebeveiliging heeft tot doel te borgen dat de informatie van de gemeente beschikbaar (op moment dat het nodig is), vertrouwelijk (alleen toegankelijk voor geautoriseerden) en integer (de gegevens kloppen en zijn actueel) is. Sinds de Algemene Verordening Gegevensbescherming (AVG) in 2018 en de Baseline Informatiebeveiliging Overheid(BIO) in 2020 is de druk nog groter om de informatie van en over de inwoners te beveiligen.

Met dit rapport beoogt de rekenkamercommissie inzicht te geven in de opgaven, de stand van zaken, de doelmatigheid en doeltreffendheid van de informatieveiligheid van de gemeente en aanbevelingen te doen voor mogelijke verbeteringen.

1. CONCLUSIES, AANBEVELINGEN EN CONCEPTRAADSBESLUIT

1.1 CONCLUSIES

De doelmatigheid en doeltreffendheid van maatregelen om de informatiebeveiliging te waarborgen zijn niet eenduidig.

1. Middelen zijn onvoldoende om de ict maatregelen en -systemen bijdetijds te houden. Recentelijk is besloten een inhaalslag te maken.
2. De monitoring op systemen en op het geheel van informatiebeveiliging en gegevensbescherming is fragmentarisch.
3. De sturing op informatiebeveiliging en gegevensbescherming èn wisselwerking tussen bestuur en organisatie zijn onvoldoende. Taken en verantwoordelijkheden zijn niet helder belegd. Er is geen business continuity plan. Sectoren zijn verantwoordelijk voor aanschaf van software, daardoor is onvoldoende regie op onderhoud, beveiliging en de aanwezigheid van schaduw-IT[1].
4. Bescherming van persoonsgegevens krijgt de benodigde aandacht, de resultaten blijven achter. Het belang van informatiebeveiliging en gegevensbescherming wordt onvoldoende onderkend. De organisatie start met risicovolle verwerkingen zonder (afgeronde) Data Protection Impact Assessments.
5. Na aanpassing van de spamfilter reageert op een phishing mail (met Eindhovense opmaak) zo'n 20% van de medewerkers. Penetratietesten wijzen uit dat de informatiebeveiliging op ict gebied op een aantal vlakken kwetsbaar is. Uit de test blijkt de bescherming van buitenaf tegen onbevoegden relatief het beste.

1.2 AANBEVELINGEN

De rekenkamercommissie beveelt aan:

Aan de gemeenteraad:

1. Vraag het college om periodieke rapportages over de voortgang en effecten van de informatiebeveiligingsmaatregelen en gegevensbescherming.
2. Investeer in de benodigde capaciteit om de informatiebeveiliging en gegevensbescherming structureel op peil te houden.

Aan het college:

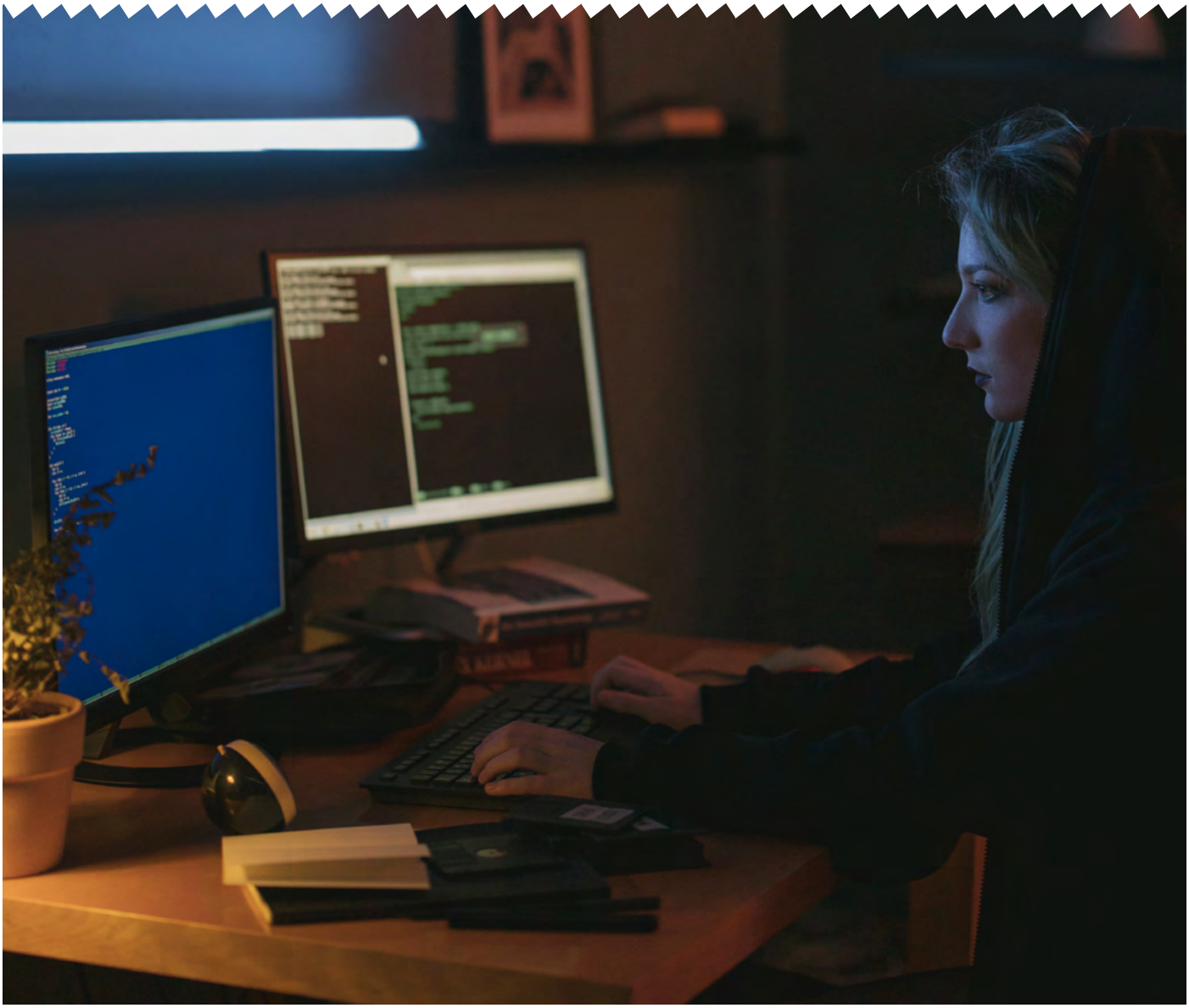
1. Zorg voor een actueel integraal informatiebeveiligingsbeleid met een heldere organisatiestructuur, structurele middelen en een implementatieplan.
2. Zorg voor overzicht en inzicht in kritische bedrijfsprocessen.
3. Beleg de IT governance (mandaat en beslissingsbevoegdheden) eenduidig. Maak een business continuity plan.
4. Zorg voor voldoende capaciteit om daadwerkelijk aan de wettelijke vereisten te voldoen, zorg voor afgeronde DPIA's bij risicovolle verwerkingen. Investeer in bewustwording, kennis, capaciteit en draagvlak.
5. Oefen met behulp van experts scenario's die kunnen optreden bij verstoringen van de ICT (met deelname van ketenpartners).

1 Schaduw -IT is zowel soft- als hardware die niet officieel is goedgekeurd.

1.3 CONCEPT RAADSBESLUIT

De rekenkamercommissie stelt de raad voor om het college op te dragen:

- de aanbevelingen aan het college 1 t/m 4 uit te voeren;
- de raad hier eens per half jaar over te informeren; en
- de aanpak en resultaten jaarlijks te evalueren.



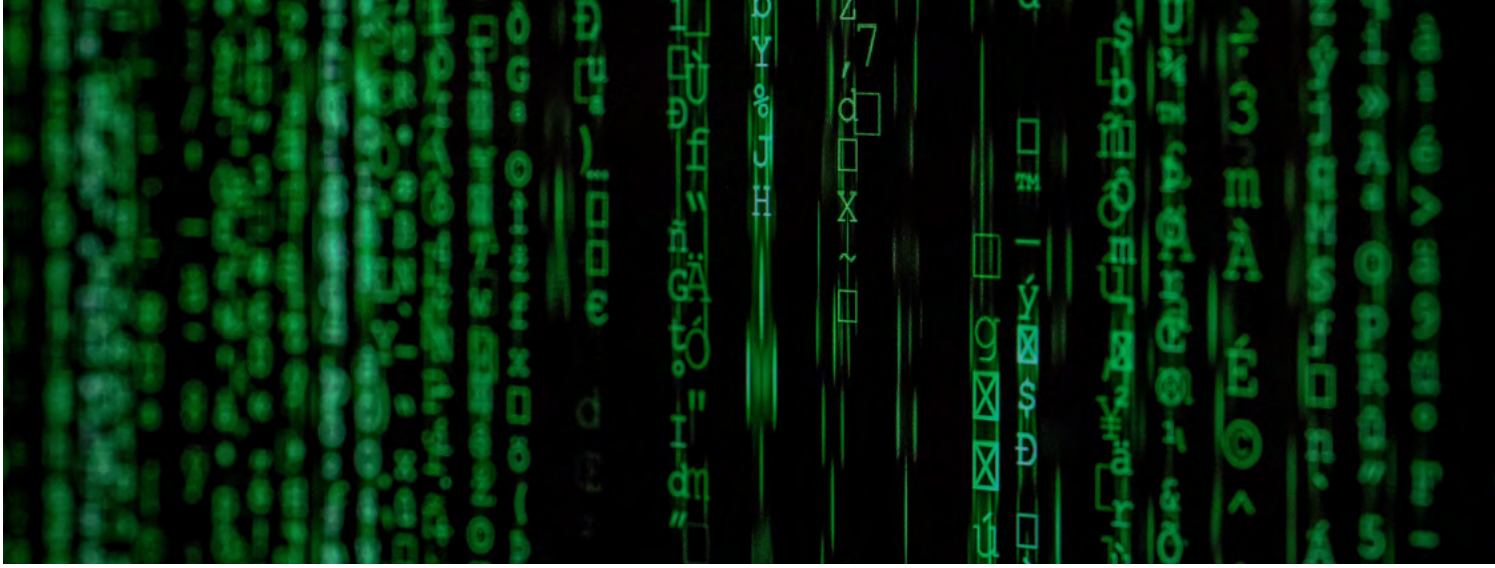
2. PROBLEEMSTELLING

De centrale vraag is:

Hoe doelmatig en doeltreffend is de gemeente Eindhoven om de informatieveiligheid te waarborgen?

En meer specifiek:
- Wat zijn beleidsdoelen, -kaders en middelen?
- Hoe is de stand van zaken? Wat zijn risico's?
- Wat is (verder) mogelijk om de informatieveiligheid te optimaliseren?
- Hoe is de privacy van inwoners geborgd binnen de gemeente?
- Wat zijn condities voor succes?

In het vervolg lichten we de bevindingen toe.



3. BEVINDINGEN

KADERS EN DOELEN

Informatiebeveiligingsbeleid

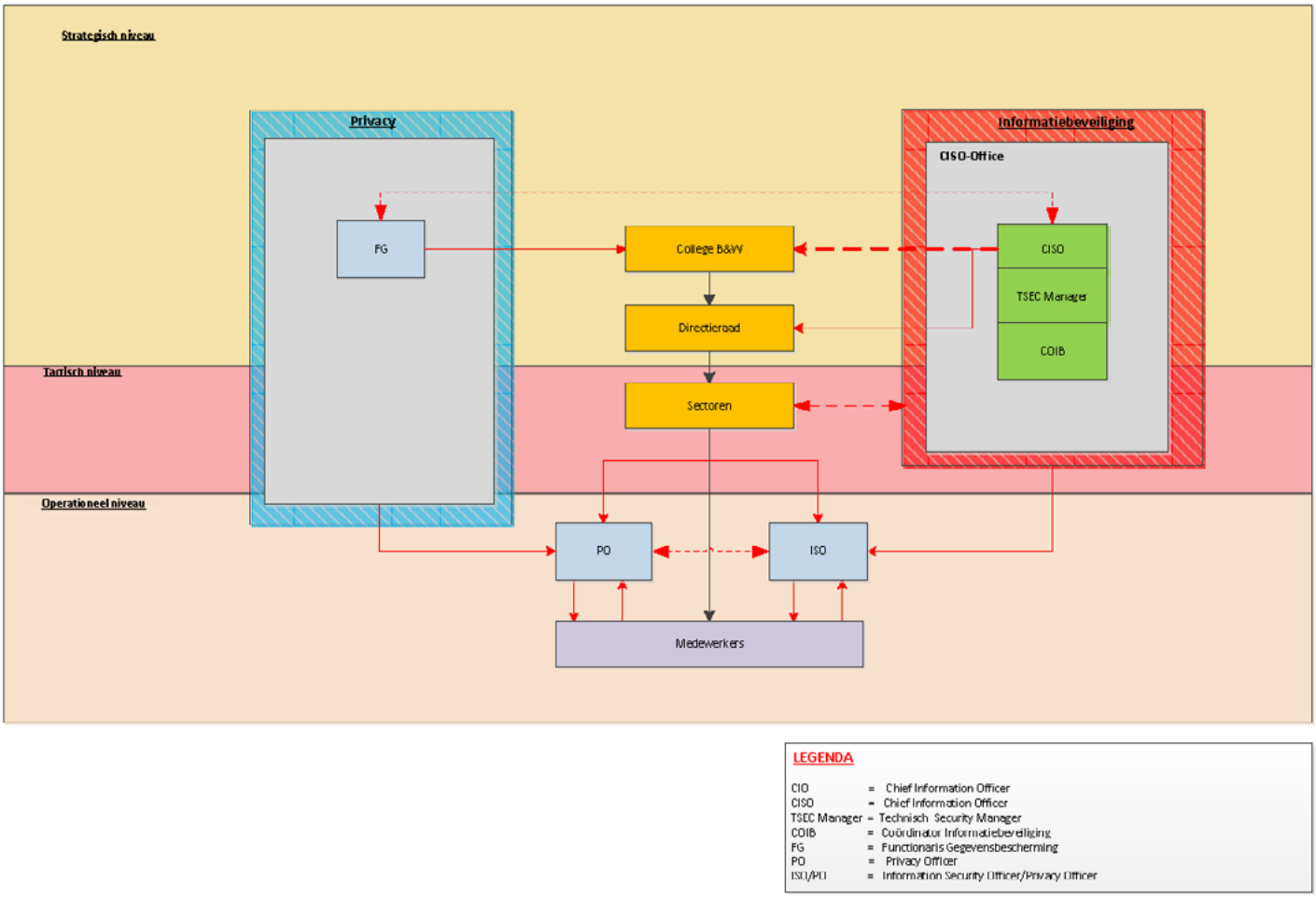
Doelen in het huidige informatiebeveiligingsbeleid (2019) zijn het beschermen en in control zijn van de gemeentelijke informatie, het mogelijk maken van (digitale) dienstverlening op een verantwoorde innovatieve manier. Het beleid is door een externe partij opgesteld. Het beschrijft strategische uitgangspunten en randvoorwaarden, de organisatie van de informatiebeveiligingsfunctie, de toewijzing van de verantwoordelijkheden, gemeenschappelijke betrouwbaarheidseisen en normen en de bevordering van het beveiligingsbewustzijn. De aanpak is 'risk based' (risicobeheersende benadering). De verschillende onderdelen zijn:

Figuur 1 Samenhang componenten uit Informatiebeveiligingsbeleid 2019

Uit interviews blijkt dat het beleid minder aansluit bij de uitvoeringspraktijk. Het nieuwe beleid, intern opgesteld, is volgens verwachting in Q1 2022 gereed.

Privacybeleid

Doel van het privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy rechten van personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). De AVG vormt het centrale kader voor het geactualiseerde privacybeleid (2021). Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. Het privacybeleid geldt voor alle aspecten van de gemeentelijk bedrijfsvoering (voor zover hierbij sprake is van de verwerking van persoonsgegevens). De kern van de AVG is transparantie, doelbinding, dataminimalisatie, kwaliteit/juistheid van de gegevens en rechtmatige en behoorlijke verwerking. De gemeente is 'accountable', de gemeente moet uitleggen en aantonen wat is gedaan om aan de regelgeving te voldoen. De Autoriteit Persoonsgegevens (AP) als externe toezichthouder kan een boete opleggen van € 20 mln.



Figuur 2 Rollen en samenhang Informatiebeveiliging en privacy (Informatiebeveiligingsbeleid, 2019)

DE STAND VAN ZAKEN

Wachtwoordenbeleid

Het wachtwoordenbeleid (zomer '21 vastgesteld) biedt praktische handvatten en bevat een goede basis voor een veilig wachtwoordbeleid. Er zijn verschillende eisen aan de opbouw van wachtwoorden. Uit de technische test blijkt dat deze eisen echter nog niet volledig door het systeem worden afgedwongen.

Inkoopbeleid

De Inkoopvoorwaarden hanteren onder meer open data principes naast eisen als de Algemene Verordening Gegevensbescherming (AVG). Bij aanschaf van nieuwe diensten en producten zijn niet altijd de Information Security Officers (ISO) en Privacy Officers (PO) betrokken. Het risico is dat deze gebruikt worden zonder dat ze voldoen aan de eisen.
Sinds november '21 is een programma van eisen voor sectorhoofden bij aanschaf van IT diensten of producten beschikbaar.

Na aanschaf is de controle of het product of dienst voldoet aan de eisen beperkt. De leverancier levert een zelf beschreven reactie op de eisen. Extra documentatie of bewijs wordt niet gevraagd. Mogelijk leveren bepaalde leveranciers wel jaarlijks een ISAE verklaring (International Standard for Assurance Engagements) aan, maar beoordeling vindt niet plaats. Het ligt niet vast wie dit zou moeten doen.

Het informatiebeveiligingsbeleid stelt dat "bij uitbesteding van diensten de gemeente eindverantwoordelijk blijft voor de betrouwbaarheid. Het toezien op naleving van dit beleid bij leveranciers is een verantwoordelijkheid van de bureau Chief Information Security Officer (CISO)". Uit interviews blijkt dat het niet duidelijk is wie hier verantwoordelijk voor is.

Dat afdelingen IT toepassingen gebruiken (Shadow IT), die niet bekend zijn bij de Chief Information Officer (CIO) en CISO en niet voldoen aan de veiligheidseisen, is een reëel risico blijkt uit interviews.

Calamiteiten

Er is een calamiteitenplan (2021). Uit interviews blijkt dat in de praktijk veel ad hoc en via het informele netwerk gehandeld wordt. Tot nu toe werkt dit goed, maar het is afhankelijk van (de beschikbaarheid van) personen en dus kwetsbaar.
Er is een meldpunt voor datalekken en beveiligingsincidenten. In het calamiteitenplan staat dat in geval van informatiebeveiligingsmeldingen de CISO hierbij adviseert. De rol Functionaris Gegevensbescherming (FG) is hierbij niet opgenomen.

Een Business Continuity Plan ontbreekt. Het huidige calamiteitenplan is te abstract en richt zich met name op de bestuurlijke kant. Er is een overzicht van de meest kritische bedrijfsapplicaties, echter de business recovery plannen zijn hier nog niet voor opgesteld.

Gijzelsoftware / ransomeware maakt gebruik van kwetsbaarheden in systemen om het netwerk binnen te dringen. Daarom wil de gemeente concreet dat een software versie niet meer dan één update achter loopt. Om hieraan te voldoen is men nu bezig met een inhaalslag, systemen lopen (ver) achter met wijzigingen.

Smartcity toepassingen en de AVG

Eindhoven heeft smartcity toepassingen als auto handhaving parkeerbelasting, bodycams, druktemeter binnenstad, en cameratoezicht openbare orde en veiligheid. Eindhoven werkt hierbij veel samen met externe partijen voor de ontwikkeling en de hosting van nieuwe toepassingen. Hierbij is onvoldoende oog voor de bescherming van persoonsgegevens.

Bij risicovolle verwerkingen zijn de sectoren verplicht om Data Protection Impact Assessments (DPIA's) uit te voeren. Bureau FG investeert in 2018 en 2019 veel in gesprekken, bewustwording, ontsluiten van informatie en het opstellen van gedetailleerde handreikingen.

Bureau FG toetst of een ingediende verwerking voldoet aan de AVG eisen. Er is een achterstand in DPIA's. Daarnaast is een toename van risicovolle verwerkingen zonder dat een DPIA is gestart dan wel afgerond. Met de komst van een centrale privacy officer start sinds 2021 bureau FG met de uitbouw van de toezichthoudende taken.

De gemeentelijke organisatie bevindt zich nog volop in de fase van bewustwording. Er ontbreekt nog veel kennis en capaciteit binnen de sectoren over de AVG verantwoordelijkheden en de rollen. De verdere digitalisering binnen de samenleving en ook de gemeente maken dit een reëel risico.

Organisatie

Er is onvoldoende wisselwerking tussen het bestuur en de organisatie over informatiebeveiliging en privacy. Het managen van de risico's op gebied van informatiebeveiliging is voor een groot deel "bottom up". Het bestuur ziet een top-down agendering van deze onderwerpen. De communicatie is incident gedreven. Verantwoordelijke functionarissen werken hard aan het verbeteren van de veiligheid en beveiliging van de informatie binnen de gemeente, echter ervaren beperkte steun vanuit de organisatie. Tevens komt naar voren dat taken en verantwoordelijkheden niet helder operationeel zijn afgebakend en medewerkers hebben te weinig mandaat. Een helder onderscheid tussen strategische, tactische en operationele verantwoordelijkheden is van belang.
Het bestuur is onvoldoende betrokken en stuurt te weinig op de thema's informatiebeveiliging en privacy blijkt uit interviews. Het budget is te beperkt en er lijkt geen ruimte om meer budget te verkrijgen.

Er blijkt nog steeds te weinig eigenaarschap over de opvolging van bevindingen uit een (interne) audit of openstaande punten.

Sectorhoofden zijn verantwoordelijk voor het risicomanagement. Het is de vraag of deze ook gericht zijn op bredere (toekomstige) dreigingen en risico's.

PENETRATIETESTEN

Na aanpassing van de spamfilter reageert op een phishing mail (met Eindhovense opmaak) zo'n 20% van de medewerkers. Penetratietesten wijzen uit dat de informatiebeveiliging op ict gebied op een aantal vlakken kwetsbaar is. Uit de test blijkt de bescherming van buitenaf tegen onbevoegden relatief het beste.

TOEKOMSTIGE OPGAVEN EN RISICO'S

- Smart city toepassingen dienen te voldoen aan geldende en toekomstige wet- en regelgeving, zie ook het laatste rapport van de AP;
- Met de ambitie om de ITorganisatie te verbeteren naar een serviceorganisatie is (de inrichting van) het proces het eerste belangrijke onderwerp;
- Investeren in voldoende middelen, kennis en kunde om bij te blijven in het snel veranderende landschap van informatiebeveiliging.

4. AANPAK

Het onderzoek vindt plaats vanaf half juni tot november 2021.
De rekenkamercommissie selecteert Hoffmann voor het veldonderzoek. Het onderzoek is verricht door documentanalyse en interviews met de betrokken ambtenaren en de portefeuillehouder. Daarnaast zijn penetratietesten verricht en zijn reacties van medewerkers getoetst op phishing. Het feitenrelaas is gecontroleerd op onjuistheden, de bestuurlijke reactie volgt separaat. De rekenkamer bedankt de ambtelijke organisatie en het college voor de medewerking.

BIJLAGE
RAPPORTAGE HOFFMANN

Rekenkamerrapport

Informatiebeveiliging Gemeente Eindhoven

november 2021

Hoffmann
Luidsprekerstraat 10
1322 AX Almere

T 088 - 298 66 00
E info@hoffmann.nl
W www.hoffmann.nl

IBAN NL87ABNA0861616820
KvK 33170622
BTW NL006275199B01

INHOUDSOPGAVE

Management samenvatting

In opdracht van de Rekenkamercommissie Eindhoven is de informatiebeveiliging onderzocht bij de Gemeente Eindhoven. Om een gedegen beeld te krijgen van de aanwezige kwetsbaarheden, is tijdens het onderzoek het beveiligingsniveau van zowel de organisatie, mens als techniek (ICT) onderzocht. Op basis van de bevindingen zijn de daarmee samenhangende risico's en de concreet uitvoerbare verbetermogelijkheden in kaart gebracht.

Het onderzoek naar de organisatie van de informatiebeveiliging had tot doel na te gaan of de gemeente de belangrijkste risico's in beeld heeft, hoe het vigerende informatiebeveiligingsbeleid binnen de organisatie wordt toegepast en of de beveiligingsmaatregelen door de organisatie worden nageleefd.

Tijdens het technische onderzoek is getoetst of de informatiesystemen van de gemeente voldoende beveiligd zijn tegen het risico van hacken. Onderzoekers hebben de informatiebeveiliging zowel getest vanaf het internet (externe penetratietest), als vanuit het gemeentehuis (interne penetratietest).

Het bewustzijn van de medewerkers is getest door middel van mail phishing, waarbij er een e-mail is verstuurd die uitnodigde op een link te klikken en de gebruiker te verleiden om persoonlijke inloggegevens af te geven.

Organisatie

Onderzoek naar de organisatie en het beleid op het gebied van informatiebeveiliging bestond uit interviews en documentanalyse. Centraal hierbij stond het informatiebeveiligingsbeleid uit 2019. Het beleid blijkt in de praktijk niet volledig geïmplementeerd te zijn. Het is onvoldoende in lijn met de BIO en sluit in mindere mate aan bij de praktijk van de gemeente. Momenteel is er een nieuw beleid in de maak, deze is echter niet beoordeeld. Informatiebeveiliging lijkt binnen de gemeente "ad hoc" georganiseerd. Er worden goede initiatieven genomen en op onderdelen ook getracht de risico's beheersbaar te maken. De verantwoordelijke informatiebeveiligingsfunctionarissen hebben goed in beeld wat er dient te gebeuren, echter lijken dit vooral zelfstandig op te nemen. Op verschillende onderdelen, waaronder patch-management en DPIA analyses is nog een achterstand. Zorgen zijn ook het inkoopproces en het risico van "Shadow IT". Dit risico houdt in dat er software wordt gebruikt binnen de organisatie die niet is goedgekeurd, of waarvan de risico's onvoldoende in beeld zijn bij de Informatiebeveiligingsorganisatie. Een business continuity plan (BCM) ontbreekt. Het huidige calamiteitenplan is te abstract en richt zich met name op de bestuurlijke kant. Er is een overzicht

gemaakt van de meest kritische bedrijfsapplicaties, echter de business recovery plannen zijn hier nog niet voor opgesteld.

Mens (social engineering)

Met het versturen van een phishing mail is het bewustzijn van de medewerkers ten aanzien van het herkennen van een nep-e-mail getoetst. Na het aanpassen van de spamfilter is een e-mail verstuurd met Eindhovense opmaak. Bij de 2955 verstuurde phishing e-mails hebben 686 gebruikers (23%) de unieke link in de e-mail geopend. In totaal zijn er 613 inlogpogingen van unieke gebruikers met geldige e-mailadressen geregistreerd (21%). Met een enkele geldige gebruikersnaam en wachtwoord kan een kwaadwillende verbinding maken met het draadloze netwerk en zo de multi-factor authenticatie omzeilen.

Deze percentages zijn relatief hoog in vergelijking met andere gemeenten waar dit scenario is toegepast, en laat zien dat een significant deel van medewerkers gevoelig is voor dergelijke aanvallen. Wij adviseren om medewerkers via een gedragsprogramma te ‘leren’ hoe zij phishing e-mails kunnen herkennen en ervoor te zorgen dat medewerkers weten hoe te handelen in geval van twijfel.

Techniek (Penetratietesten)

Tijdens het onderzoek zijn kritieke kwetsbaarheden geconstateerd. De specifieke bevindingen, impact en aanbevolen aanbevelingen naar aanleiding van zowel de externe als de interne penetratietest zijn vanwege de diepgang en vertrouwelijkheid gedeeld met de ambtelijke organisatie.

1. Inleiding

In opdracht van de rekenkamer is een informatiebeveiligingsonderzoek uitgevoerd bij de gemeente Eindhoven in de periode van half juni tot november 2021.

1.1 Doelstelling

De centrale vraag van het onderzoek luidt: Hoe doelmatig en doeltreffend is de gemeente Eindhoven om de informatieveiligheid te waarborgen?

De deelvragen hierbij zijn:

- Wat zijn beleidsdoelen, -kaders en middelen?
- Hoe is de stand van zaken?
- Wat is (verder) mogelijk om de informatieveiligheid te optimaliseren?
- Hoe is de privacy van burgers geborgd binnen de gemeente?
- Wat zijn toekomstige opgaven, benodigde middelen, risico's?

De doelstelling van het onderzoek is om inzicht te verkrijgen in de mate waarin de gemeente Eindhoven de informatieveiligheid waarborgt. Het onderzoek moet een gedegen beeld geven van aanwezige kwetsbaarheden en de daarmee samenhangende risico's. Tevens worden er aanbevelingen gedaan over condities en concreet uitvoerbare verbetermogelijkheden. Dit conceptrapport bespreekt de bevindingen van het onderzoek op het onderdeel "organisatie".
Leeswijzer:
In Hoofdstuk 2 zijn de bevindingen opgenomen en uitgewerkt. Het gedetailleerde overzicht en uitwerking van de bevindingen omtrent het onderzoek naar de organisatie rondom informatiebeveiliging en privacy is terug te vinden in hoofdstuk 3. In hoofdstuk 4 volgt de techniek. In de bijlagen zijn constateringen opgenomen met aanbevelingen.

2. Organisatie

In het onderzoek naar de organisatie van informatiebeveiliging is gekeken naar de bovenstaande deelvragen. Deze deelvragen zijn niet apart beantwoord, maar zijn meegenomen in de analyse en de uitwerking van de bevindingen. Hierbij is voor het onderzoek een analyse uitgevoerd op de door de gemeente Eindhoven beschikbaar gestelde documentatie, rapporten en verklaringen en daarnaast door het uitvoeren van verschillende interviews met medewerkers van de gemeente voor toelichting op het gevraagde materiaal. Het kwalitatieve onderzoek is een momentopname van de situatie zoals deze nu wordt gezien en ervaren. In de bijlage is een opgave van de geïnterviewden opgenomen en een overzicht van de documenten die zijn meegenomen in de beoordeling.

2.1 Overzicht van bevindingen

Op basis van de ontvangen documentatie en verschillende interviews zijn onderstaande bevindingen geformuleerd.

2.1.1 Beleid

Het beleidsdocument 'Informatiebeveiligingsbeleid Gemeente Eindhoven 2019' vormt de basis voor informatiebeveiliging van de gemeente Eindhoven. Het beschrijft uitgangspunten, op basis waarvan de sectoren invulling kunnen geven aan de uitvoering van het informatiebeveiligingsbeleid. Daarnaast bevat het beleid de beveiligingseisen en maatregelen die voor alle gemeentelijke processen en systemen gelden. Geconstateerd wordt dat:

Op 31 januari 2019 is het Informatiebeveiligingsbeleid 2019 opgesteld door een externe partij namens de CISO Office. In de RIB van juli 2019 staat het volgende genoemd: "*Het college heeft onlangs een geactualiseerd informatiebeveiligingsbeleid vastgesteld als basis voor de te implementeren maatregelen zoals die genoemd zijn in de Baseline Informatiebeveiliging Gemeenten (BIG).*" Hierbij wordt echter niet benoemd welke versie van het beleid het betreft.

Het ontvangen beleidsdocument dateert van 28 januari 2019 en beschrijft geen frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. Het risico is dat het beleid veroudert en geen actuele kaders en richtlijnen geeft voor de organisatie om naar te handelen. Zo wordt bijvoorbeeld nog verwezen naar verouderde normenkader; de Baseline Informatiebeveiliging Gemeenten (BIG). Gemeenten dienen per 2020 te voldoen aan de nieuwe overheid brede Baseline Informatiebeveiliging Overheid (BIO). Het is conform BIO vereist om het beleid periodiek (voorkeur jaarlijks) te evalueren en waar nodig te actualiseren[1]. In Turap1-2021 is terug te lezen dat een update van het informatiebeveiligingsbeleid is uitgesteld naar zomer 2021 in verband met toenemende werkzaamheden voor de CISO naar aanleiding van Corona[2]. Uit interviews kwam naar voren, dat een nieuw informatiebeveiligingsbeleid is opgesteld, volledig in lijn met de BIO. De onderzoekers hebben deze echter niet ontvangen en derhalve ook niet kunnen beoordelen. De planning is dat dit beleid in Q1 2022 in de directieraad besproken wordt. De onderstaande analyse op het oude beleidsstuk blijft ook van belang bij het beoordelen en implementeren van het nieuwe beleidsstuk.

Inhoudelijk kijkende naar het IB-beleid merken wij op dat het compleet is omschreven en concrete en praktische handvaten biedt, zoals je zou verwachten in een beleidsstuk. Zo zijn conform de BIO[3]; strategische uitgangspunten en randvoorwaarden, de organisatie van de informatiebeveiligingsfunctie, de toewijzing van de verantwoordelijkheden, gemeenschappelijke betrouwbaarheidseisen en normen en de bevordering van het beveiligingsbewustzijn omschreven. Wat het beleid mist is een omschrijving van de frequentie waarmee het beleid dient te worden geëvalueerd, zoals hierboven reeds omschreven. Het lijkt het erop dat de 'ist' en 'soll' situatie vaak door elkaar heen wordt beschreven. Het is de vraag of de ontwikkeling van het beleid met voldoende afstemming binnen de organisatie heeft plaatsgevonden, zodat er commitment heeft kunnen ontstaan. Tijdens de interviews wordt bijvoorbeeld duidelijk dat het beleid minder goed aansluit bij de praktijk. Deze punten maken dat

[1] Zie BIO; Informatiebeveiligingsbeleid 5.1.2.
[2] Zie Turap 1 2021
[3] Zie BIO: Informatiebeveiligingsbeleid 5.1.1.1.

opvolging en naleving in de praktijk wordt bemoeilijkt. Een IB-beleid (en elk ander beleid) werkt het best als het voor en door de organisatie zelf wordt opgesteld en aansluit bij de cultuur een uitgangspunten van de organisatie. Het huidige beleid is voornamelijk opgesteld door een externe partij. Wij adviseren het nieuwe beleid zelf of minimaal in co-creatie op te maken en verder te laten aansluiten op het BIO normenkader[4]. Gedurende de interviews werd duidelijk dat er momenteel wel een beweging gaande is, waarbij specifieke eisen uit de BIO in de praktijk geconcretiseerd worden op tactisch niveau ("bottom up"). Dit zou de gemeente kunnen gebruiken als opstap naar het nieuwe en aangepaste beleid en lijkt een mooie volgende stap naar commitment vanuit de organisatie. Hierbij hoort ook een duidelijker rol van de CIO en CISO, inclusief een afgestemd mandaat.

2.1.2 Wachtwoordbeleid

Voor het wachtwoordbeleid wordt in het informatiebeveiligingsbeleid verwezen naar het wachtwoord beleidsdocument van de gemeente. De onderzoekers hebben het 'Toegangsbeveiliging beleid gemeente Eindhoven' ontvangen ter analyse. In de zomer '21 is het nieuwe toegangsbeleid vastgesteld. Het biedt handvatten voor de praktijk en bevat een goede basis voor een veilig wachtwoordbeleid. Er worden verschillende eisen gesteld aan de opbouw van wachtwoorden. Uit de technische test blijkt dat deze eisen echter niet volledig door het systeem worden afgedwongen. Ook wordt de voorgeschreven omgang met wachtwoorden (zoals opslaan en versturen) niet altijd nageleefd. Wij adviseren de gemeente om nader te bekijken hoe het beleid en praktijk beter op elkaar kunnen worden afgestemd.

2.1.3 Inkoop- en leveranciersmanagement

Idealiter worden eisen m.b.t. informatiebeveiliging en privacy aan producten, diensten en leveranciers gesteld in de selectiefase vóór de aanschaf. Deze eisen zijn opgesteld op basis van het beleid en geïdentificeerde risico's van het product en worden adequaat getoetst, zodat men enige zekerheid heeft dat de aan te schaffen diensten en producten en de leverancier die deze levert voldoet aan de eisen die de gemeente stelt. Om te borgen dat tijdens de looptijd van een contract de leverancier blijft voldoen aan de eisen, worden deze vastgelegd in een overeenkomst of contract en worden deze periodiek getoetst. Onderstaand een aantal bevindingen met betrekking tot dit proces bij de gemeente:

Eisen met betrekking tot informatiebeveiliging en privacy worden door ISO's en PO's (ad hoc) geformuleerd wanneer zij betrokken worden bij inkooptrajecten en leveranciersselecties. Het komt echter ook voor dat zij niet, of laat in het proces betrokken worden. Het risico wat de gemeente hier loopt is dat informatiebeveiligings- en privacy eisen niet (volledig) worden meegenomen bij de aanschaf van diensten en producten, waardoor deze in gebruik worden genomen zonder aan de eisen te voldoen. Momenteel zijn deze eisen onvoldoende vastgelegd of opgenomen in de interne processen van de gemeente, waardoor het afhankelijk is van de ISO of PO of de gestelde informatiebeveiligings- en privacy eisen worden opgevolgd[5].

[4] Zie BIO: "deel 2 Kader BIO"

[5] Ambtelijke reactie: Voor informatiebeveiliging is begin november '21 een Programma van Eisen opgesteld dat gebruikt wordt bij inkoop van producten en diensten. Voor privacy is een standaard dat gebruikt dient te worden. Dit wordt echter bij inkoop- en contractmanagement niet altijd gebruikt.

Ten tijde van dit onderzoek was de organisatie bezig met het opstellen en implementeren van een leidraad die sectorhoofden kunnen/moeten hanteren wanneer zij (IT)producten aanschaffen of diensten inkopen. In deze leidraad worden verschillende eisen op o.a. het gebied van informatiebeveiliging, privacy, beheer, architectuur opgenomen. Onderzoeker heeft nog geen kennis kunnen nemen van een (concept) versie van deze leidraad. Het gebruik van software binnen de gemeente, die niet bekend is bij de CIO/CISO en die mogelijk niet voldoen aan de veiligheidseisen (Shadow IT), werd gedurende de interviews als reëel risico benoemd.

Wanneer er wel eisen geformuleerd worden, is de toetsing van het product of dienst hieraan beperkt. De beoordeling van deze eisen vindt uitsluitend op papier plaats, middels een door de leverancier zelf beschreven reactie op de eisen. Er wordt geen ondersteunende documentatie of ander bewijs van leveranciers opgevraagd om daadwerkelijk te toetsen of er voldoende aan de eisen wordt voldaan. Uit interviews kwam naar voren dat er mogelijk wel jaarlijkse ISAE verklaring (International Standard for Assurance Engagements) worden aangeleverd door bepaalde leveranciers, echter dat de beoordeling daarvan niet plaatsvindt, omdat niet is vastgelegd of bepaald wie en hoe de controle hierop moet plaatsvinden.

Volgens het IB beleid gelden in beginsel altijd de Algemene Inkoop Voorwaarden (AIV)[6], waarin onder meer geheimhouding en aansprakelijkheid is geregeld. Afwijkingen op de AIV dienen te worden getoetst aan informatiebeveiligingsbeleid. Vereiste beveiligingsmaatregelen worden aanvullend vastgelegd in contracten en/of verwerkersovereenkomsten. Daarin is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de gemeente het recht heeft afspraken te (laten) controleren. In de praktijk blijkt dat hetgeen beschreven is niet altijd wordt nageleefd. Er mag in de praktijk meer aandacht zijn voor het opnemen van eisen m.b.t. informatiebeveiliging in contracten en overeenkomsten met leveranciers. Wij raden aan de verantwoordelijkheid hiervoor te beleggen en te formaliseren.

Het is van belang dat er ook tijdens de looptijd van het contract wordt getoetst of er door de leverancier (nog steeds) wordt voldaan aan de gestelde eisen. Dit is opgenomen in het IB beleid, waarin wordt beschreven dat dit een verantwoordelijkheid is voor de CISO Office[7]: *Bij externe hosting van data en/of services (uitbesteding, Cloud computing) blijft de gemeente eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop. Het toezien op naleving van dit beleid bij leveranciers is een verantwoordelijkheid van het CISO office.*
De onderzoekers hebben tijdens de interviews gemerkt dat er onduidelijkheid bestaat over wie hier binnen verantwoordelijkheid voor is. Wij raden de organisatie aan om hier duidelijkheid te scheppen, deze verantwoordelijkheid te beleggen en dit te formaliseren.

[6] Zie hoofdstuk 3.7 van het Informatiebeveiligingsbeleid Gemeente Eindhoven 2019
[7] Zie hoofdstuk 7.3 van het Informatiebeveiligingsbeleid Gemeente Eindhoven 2019

2.1.4 Calamiteitenplan

De gemeente beschikt over een calamiteitenplan[8], waarin er een crisisteam formeel is vastgesteld. Het document richt zich echter voornamelijk op het bestuurlijk proces van het managen van een calamiteit. Er wordt niet gesproken over calamiteiten-scenario's en de daarbij behorende plannen. Uit de interviews blijkt dat in de praktijk nog veel ad hoc wordt geacteerd gedurende calamiteiten, en dat functionarissen betrokken worden via het informele netwerk dat men met elkaar heeft. Dat heeft tot nu toe goed gewerkt, echter is dit informele proces sterk afhankelijk van specifieke personen en de beschikbaarheid daarvan. Het risico wat men loopt is dat tijdens een calamiteit niet de juiste medewerkers worden geïnformeerd en/of er niet voldoende mandaat om beslissingen te nemen, zoals dit is afgestemd in het calamiteitenplan. Het calamiteitenplan mag meer als leidraad voor de praktijk gebruikt worden en kan nog worden uitgebreid met de beschrijving van welke beslissingsbevoegdheden de verschillende actoren hebben. Daarnaast is het raadzaam om periodiek het calamiteitenplan in de praktijk te oefenen.

Uit nader onderzoek blijkt dat er geen verdere documenten beschikbaar zijn over Business Continuity Management (BCM) of crisismanagement aangaande informatieveiligheid. Wel is een start gemaakt met BCM in de vorm van een Business Impact Analyse (BIA) als één van de onderdelen van de Business Continuity Lifecycle. Het streven is om vanaf begin 2022 het BIA instrument, daar waar nuttig, onderdeel te maken van de werkwijze van ICT advisering en dienstverlening. Voor wat betreft de bedrijf kritische applicaties is het raadzaam om het calamiteitenplan uit te breiden met een concreet business recovery plan. De gemeente heeft wel per domein in kaart gebracht welke applicaties gebruikt worden en deze geregistreerd in Bluedolphin. Hierin is ook vastgelegd in welke mate de specifieke applicatie een kritisch proces ondersteunt.

Datalekken en beveiligingsincidenten dienen door de medewerker te worden gemeld aan meldpuntdatalekken@eindhoven.nl. Volgens het IB beleid verloopt de afhandeling van beveiligingsincidenten via een vastgesteld proces t.w. het Proces Calamiteit[9]. Bij dit proces wordt de CISO in geval van security incident meldingen betrokken bij het calamiteiten managementteam. Conform de RACI matrix in dit document is de rol van de CISO voornamelijk adviserend. Opmerkelijk genoeg wordt de rol van de Functionaris Gegevensbescherming (FG) niet specifiek in het proces opgenomen. De reden hiervan ligt in het feit dat het document zich met name richt op de continuïteit van de (IT) dienstverlening.
Het advies is om een concreter en completer Informatiebeveiligingscontinuïteit plannen op te stellen. Deze plannen dienen de crisis- en incidentmanagement teams met hun taken en bevoegdheden te omschrijven, inclusief duidelijke crisis scenario's met bijbehorende plannen. Ultiem dienen deze plannen en het managen van een crisis ook periodiek te worden getraind.

[8] Document: Proces Calamiteit, versie 1.7, januari 2021
[9] Document: Proces Calamiteit, versie 1.7, januari 2021

2.1.5 Patch- en Releasemanagement proces

Wanneer een organisatie niet tijdig (security) patches installeert is een organisatie kwetsbaar voor security breaches. Ransomeware maakt gebruik van kwetsbaarheden in systemen om het netwerk binnen te dringen. De gemeente heeft daarom de ambitie gesteld om bij te zijn met patches van systemen (n -1). Concreet betekent dit, dat een software versie niet meer dan 1 update achter mag lopen. Om hieraan te voldoen is men nu bezig met een inhaalslag, systemen lopen (ver) achter met patches.

Volgens het IB beleid worden *technische kwetsbaarheden regulier met een minimum van vier keer per jaar gerepareerd door het 'patchen' van software, of 'ad hoc' bij acute dreiging of na een incident.* Hetgeen beschreven in het IB beleid is echter geen afspiegeling van de praktijk, het beleid is (nog) niet juist en volledig geïmplementeerd. Het is in eerste instantie zaak om alle hard- en software op het gewenste patch niveau te krijgen. Daarnaast dient er een degelijk proces ingericht te worden om in de toekomst op ambitieniveau n -1 te blijven. Dit proces dient te worden vastgelegd en te voldoen aan de kaders gesteld in het IB-beleid.

Voordat nieuwe software uitgebracht wordt, wordt dit getest o.b.v. landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicaties. Volgens het IB beleid dient ten minste getest te worden op bekende kwetsbaarheden zoals vastgelegd in de OWASP[10] Top 10. Mede gelet op de bevindingen vanuit het onderwerp betreffende "Inkoop- en leveranciersmanagement", is het onduidelijk of dit voor alle software binnen de gemeente ook gebeurt. De gemeente Eindhoven heeft echter recent een Life Cycle Manager aangesteld die zich o.a. bezig gaat houden met (het opstellen van regels en procedures voor) het releasen van software en het onderhoud hiervan, wat aangeeft dat het onderwerp op de agenda staat.

Het advies is om de inhaalslag die inmiddels in gang is gezet te continueren. Hierbij kan afhankelijk van de kwetsbaarheid van de applicatie, rekening worden gehouden met prioritering op kritische applicaties. Tevens dienen de eisen met betrekking tot het patchen van software worden meegenomen in de verdere uitwerking van het inkoop- en leveranciersmanagement beleid en proces. Tot slot is het van belang om periodiek de technische kwetsbaarheden van de systemen te testen door middel van een pentest.

2.1.6 Innovaties en Living Labs (smart city toepassingen)

Innovaties en smart city toepassingen worden geïnitieerd door het Ruimtelijk Domein, Veiligheid Juridische Zaken en Bestuur (zoals auto controle parkeerbelasting, camera's bij stoplichten, bodycams, digitale deurbel). Hierbij wordt samengewerkt met externe partijen voor zowel de ontwikkeling, als de hosting van nieuwe toepassingen. Het nadeel hiervan is dat de eigen organisatie,

[10] Het Open Web Application Security Project (OWASP) is een stichting zonder winstoogmerk die zich inzet voor het verbeteren van de beveiliging van software.

met name I&B, CIOoffice en de privacy officers niet, nauwelijks of te laat in het proces betrokken worden. Het is voor deze afdelingen zaak om zo snel mogelijk op de hoogte te zijn en blijven van nieuwe toepassingen om tijdig aan te kunnen haken en de persoonsgegevens te beschermen.

De sectoren zijn verplicht om Data Protection Impact Assessments (DPIA's) uit te voeren bij de risicovolle verwerkingen. Om dit van de grond te krijgen heeft bureau FG in 2018 en 2019 veel geïnvesteerd in gesprekken, bewustwording, ontsluiten van informatie en het opstellen van gedetailleerde handreikingen. Voor het privacy framework was in 2018 een applicatie door de gemeente aangekocht (SmartPia van USoft), die in 2019 verder is uitgerold. In dit framework zijn ook de NOREA[11] vragenlijsten voor de risico inventarisatie t.b.v. de DPIA's opgenomen. Hiermee verloopt het bijhouden van de registers vrijwel geheel digitaal door inzet van de diverse privacy officers binnen de sectoren. Vanuit bureau FG wordt getoetst of een ingediende verwerking voldoet aan de eisen die de AVG stelt. Een centrale privacy officer werkt sinds augustus 2020 aan bewustwording en biedt tweedelijns ondersteuning aan de privacy officers. Sinds 2021 is er binnen de gemeente een start gemaakt met de uitbouw van de toezichthoudende taken van bureau FG.

Ter bevordering van de bewustwording op intranet is een infographic beschikbaar genaamd "het ABC van de AVG" waarin stappen zijn opgenomen dienen te worden gezet bij het opstarten van nieuwe, innovatie projecten (zoals het uitvoeren van een DPIA). Het is de onderzoeker niet duidelijk geworden of deze infograhic makkelijk vindbaar is voor medewerkers die betrokken zijn met het opstarten van projecten of dat de privacy organisatie meer moet doen om dit onder de aandacht te brengen.

Uit de interviews blijkt dat de gemeentelijke organisatie zich nog volop bevindt in de fase van bewustwording en dat nog veel kennis en capaciteit ontbreekt binnen de sectoren betreffende de verantwoordelijkheden en de rol van de sectoren en/of medewerkers betreffende de AVG. De verdere digitalisering binnen de samenleving en ook de gemeente maken dit een reëel risico. Het organiseren en uitvoeren van een gedegen DPIA (die op tijd wordt uitgevoerd) is van cruciaal belang zodat risico's op tijd worden onderkend en er ook maatregelen tegenover kunnen worden geplaatst. Het advies is de ingezette koers van de rol van bureau FG verder te blijven professionaliseren, maar vooral het belang om te voldoen aan de AVG binnen de gehele organisatie te blijven omarmen en uit te dragen.

2.2 Optimalisatie

2.2.1 Tone at the Top

In de interviews kwam sterk naar voren dat er onvoldoende wisselwerking is tussen het bestuur en organisatie m.b.t. informatiebeveiliging en privacy. Het bestuur ziet een top-down agendering van deze onderwerpen. Het managen van de risico's op gebied van informatiebeveiliging gebeurt voor een groot deel "bottom up". Verantwoordelijke functionarissen werken hard aan het verbeteren van de

[11] Methodische handreiking Privacy Impact Assessment (PIA) die is uitgegeven door NOREA; de beroepsorganisatie van ITauditors in Nederland

veiligheid en beveiliging van de informatie binnen de gemeente, echter ervaren beperkte steun vanuit de organisatie. Op het gebied van privacy is wel meer aandacht binnen het bestuur, blijkt ook de aanstelling van een tijdelijke (inhuur) privacy jurist (bij sector Veiligheid, Juridische Zaken en Bestuur) en een centrale privacy officer (bij CIO-office). Echter, ook op dit onderwerp dient het bewustzijn van de risico's binnen de sectoren nog te verbeteren en is behoefte aan meer aansturing voor het inbedden van de privacy binnen de processen. Uit interviews bleek dat er weinig eigenaarschap is in de opvolging van bevindingen uit een (interne) audit of openstaande punten.
De algemene afdronk is dat het bestuur onvoldoende betrokken is en te weinig stuurt op de thema's informatiebeveiliging en privacy, de communicatie is incident gedreven. Juist deze betrokkenheid en een duidelijk "tone at the top", zal helpen om beide onderwerpen binnen de organisatie verder te verbeteren. Bewustzijn kan gemeten worden door de vragen die de raad stelt, maar ook door de bereidheid om budget beschikbaar te stellen voor de organisatie. De algehele indruk uit interviews was dat dit budget te beperkt is en dat er geen ruimte lijkt om meer budget/middelen te verkrijgen.

2.2.2 Taken en verantwoordelijkheden formaliseren

In het informatiebeveiligingsbeleid, staat helder omschreven hoe de verschillende taken en verantwoordelijkheden binnen de organisatie zijn belegd. Het lijkt er echter op dat het beleid nooit formeel is uitgerold, waardoor voor bepaalde functies geldt dat hun taken en verantwoordelijkheden niet operationeel helder zijn afgebakend. Wanneer taken en verantwoordelijkheden niet helder zijn afgebakend kan het voorkomen dat medewerkers elkaar overlappen in verantwoordelijkheden wat tot spanningen kan leiden of dat zaken juist niet worden opgepakt, omdat uiteindelijk niemand verantwoordelijk is. Het advies is om taken en verantwoordelijkheden (m.b.t. informatiebeveiliging en privacy) formeel door te voeren en te mandateren.

2.2.3 Rolzuiverheid

Bepaalde toezichthoudend of toetsende functies vervullen adviserende taken, hierbij valt te denken aan de FG en de IT-auditor (interne concerncontrol). Zo is de FG, met haar team vanwege het beperkte bewustzijn binnen de organisatie veel betrokken bij het advies over hoe de privacy binnen de organisatie geborgd dient te worden. De IT-auditor is bijvoorbeeld ook betrokken bij de advisering over nieuwe applicaties, die deze functionaris later zelf ook dient te auditen. An sich zeer begrijpelijk dat deze taken zo ontstaan binnen de organisatie, echter de gemeente dient zich ervan bewust te zijn dat vermenging van adviserende en toetsende/toezichthoudende taken binnen een functie, ten koste gaat van de rolzuiverheid. Het risico is, dat mogelijk de toetsing of het toezicht niet voldoende onafhankelijk plaats kan vinden. Deels worden door de gemeente stappen gemaakt, die zich met name richten op het bewustzijn binnen de organisatie en de lijnverantwoordelijkheid die daarbij hoort[12]. Zoals hierboven aangegeven zal de "tone at the top" een belangrijke volgende stap zijn ter verbetering, zodat onafhankelijk toetsende en toezichthoudende functies en rollen gecreëerd kunnen worden.

[12] Ambtelijke reactie: De CIO office investeert hierin door de aanstelling van een centrale AVG privacy coördinator en het IT Governance team. Taken worden gesplitst, dit is per 1-1-2022 operationeel.

2.2.4 Mandaat

Bepaalde functies hebben niet voldoende mandaat om zaken af te dwingen of te escaleren. Tijdens het onderzoek werden voorbeelden genoemd dat de CISO geen mandaat heeft om bepaalde beveiligingsmaatregelen af te kondigen die dwingend worden opgevolgd. Er hebben zich situaties voorgedaan dat er op een advies/beveiligingsmaatregel van de CISO geëscaleerd werd en dat zijn besluiten werd overruled door leidinggevenden/sectorhoofden, zonder dat hier een goede risicoanalyse en besluitvorming aan ten grondslag lag. Hierdoor kan de gemeente risico's lopen. Het is voor bepaalde functies, waaronder de CISO functie essentieel om mandaat en bevoegdheden te hebben om bepaalde maatregelen, op basis van een gedegen risicoafweging en in goed overleg met het bestuur, op te kunnen leggen. Dit zou idealiter formeel vastgelegd dienen te zijn.

2.2.5 Vak volwassenheid

Voor bepaalde functies geldt dat de uitvoerende medewerkers nog niet voldoende onderlegd zijn qua kennis en opleiding. In interviews is genoemd dat dit geldt voor functies op praktisch niveau op het vlak van informatieveiligheid en privacy. Functies bekleed door medewerkers die onvoldoende kennis of competenties hebben worden niet adequaat en met voldoende kwaliteit uitgevoerd. Daarnaast leidt het af van de rol van de toezichthouder (CISO en FG), doordat deze automatisch in een advies en kennisdelingsrol (bewustzijn sessies) worden geduwd. Ons advies is om in kaart te brengen waar deze kennistekorten zitten binnen de organisatie en deze medewerkers verder op te leiden tot het niveau waarop zij voldoende vakkennis bezitten.

2.2.6 Afbakening verantwoordelijkheden strategisch, tactisch, operationeel niveau

Medewerkers op strategische functies acteren op operationeel niveau. Uit interviews is gebleken dat bijvoorbeeld hoger management zich bezig houdt met wachtwoord instellingen en andere operationele zaken. Teveel capaciteit en aansturing op operationeel niveau kan ten koste gaan van aandacht voor strategische thema's en het uitwerken van een visie op structurele verbeteringen en vernieuwingen. Het is raadzaam om een heldere verdeling en afbakening van taken en verantwoordelijkheden op strategisch, tactisch en operationeel niveau te formaliseren.

2.2.7 Centralisatie Privacy Officer en Decentrale Information Security Officer

Per 1 augustus 2020 is de nieuwe rol van een Centrale Privacy Officer ingericht die werkt aan thema's als awareness en 2^{e} lijns ondersteuning aan Privacy Officers. De overige PO's en DISO's zijn per sector aangesteld. De inhoudelijke en functionele aansturing en coördinatie is centraal georganiseerd. Elke ISO is zelfstandig en alleen werkzaam binnen een sector. Dit kan leiden tot een problematische functionele aansturing voor uitvoering van het strategische beleid in de sector. De CISO heeft geen mandaat om de ISO's functioneel aan te sturen zodat het beleid eenduidig wordt geïmplementeerd binnen de sectoren. Ons advies is om het mandaat van de CISO te versterken.

2.2.8 Eigenaarschap

Eigenaarschap is niet voldoende ingericht. Dit blijkt bijvoorbeeld bij audit bevindingen, vastgelegd in Lias die niet tijdig en volledig worden opgepakt omdat men zich geen eigenaar voelt. Er wordt tussen verschillende actoren heen en weer “gepingpongd” over wie wat zou moeten doen, terwijl ondertussen de bevinding (met bijbehorende risico’s) niet wordt opgepakt. Dit geldt ook voor structurele verbeteringen en dagelijkse werkzaamheden waarbij het onduidelijk is wie de eigenaar is en zou moeten zorgen dat zaken geregeld worden.

Ons advies is om een RACI tabel op te stellen voor alle applicaties en processen waarin duidelijk het eigenaarschap wordt geformaliseerd. Vervolgens dient dit geïmplementeerd te worden. Eigenaren dienen te worden opgeleid in wat er van ze verwacht wordt, zodat ze zich hiernaar kunnen gaan gedragen.

2.2.9 Vertrouwen interne medewerkers

Vanuit de interviews kwam naar voren, dat wordt ervaren dat het bestuur zich voornamelijk laat leiden door de aanbevelingen van de accountant, zonder dit te reflecteren met de interne organisatie. Het gevoel dat bij de interne organisatie ontstaat, is dat er onvoldoende wordt vertrouwd op de eigen expertise in de organisatie. Het gevolg is dat informatiebeveiliging te algemeen en niet organisatie specifiek worden opgepakt en uitgewerkt door externen (zie opmerking over IB-beleid). Eigen medewerkers kennen de organisatie het beste en dienen nauw betrokken te worden, zodat beleid en praktijk integraal onderdeel van elkaar worden.

2.3 Privacy

2.3.1 Beleid

In juni 2021 is het Privacy beleid Gemeente Eindhoven 2020-2023 geactualiseerd en vastgesteld in juli 2021[13]. Doel van het beleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy en rechten van personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken).

Rechten van betrokkenen worden beschreven in het beleid. Daarnaast worden deze rechten aan betrokkenen kenbaar gemaakt via de website van de gemeente. Daar zijn voor verschillende specifieke onderwerpen privacy verklaringen opgesteld:

- Belasting en heffingen;
- Bestuur en organisatie;
- Burgerzaken, contact en dienstverlening;
- Klachten, bezwaar en beroep;
- Kunst en cultuur;

[13] Raadsinformatiebrief_Evaluatie_en_actualisatie_Privacy_beleid.pdf (parlaeus.nl)

- Ondernemen;
- Onderwijs en jeugd;
- Enquetes, onderzoek en statistiek;
- Parkeren, verkeer en bouwprojecten;
- Veiligheid en handhaving;
- Vrije tijd, sport en evenementen;
- Website en (social) media;
- Werk en inkomen;
- Wonen en leefomgeving;
- Zorg en ondersteuning.

2.3.2 Rol FG

Jaarlijks stelt de FG een jaarrapportage op met betrekking tot de bescherming van persoonsgegevens (AVG). Enkele bevindingen uit de rapportage van 2019 zijn in 2020 opgepakt, zoals aandacht vragen binnen de organisatie voor het melden van datalekken en het inrichten van een proces voor het invullen van een DPIA en het aanstellen van een centrale privacy officer. Deze laatste is verantwoordelijk voor awareness, 2de lijns ondersteuning aan privacy officers, kaders en richtlijnen, etc.. Zaken waar voorheen de FG voor verantwoordelijk was. Met de komst van de centrale privacy officer heeft de FG sinds 2021 een start kunnen maken met de uitbouw van de toezichthoudende taken van bureau FG.

In de jaarrapportage van 2020 is een opvallende bevinding genoteerd dat betrekking heeft op het (te) laat invulling geven aan privacy verplichtingen. Dit is risicovol, omdat het belangrijk is om in een zo vroeg mogelijk stadium bij de ontwikkeling of wijziging van producten en diensten aandacht te geven aan privacy (privacy by design). Los daarvan vergt het doen van aanpassingen achteraf vaak meer kosten en inspanning dan wanneer privacy vriendelijke maatregelen al tijdens de ontwikkelfase zijn geïmplementeerd en toegepast. Het advies is en blijft daarom om in een zo vroeg mogelijk stadium invulling te geven aan de AVG verplichtingen.

Het sectorhoofd is verantwoordelijk voor het uitvoeren van een DPIA aan de start van een traject. Hiervoor wordt gebruik gemaakt van een tool (SmartPia van USoft). De sector stelt een DPIA team samen. Dit team stelt de DPIA op. De Privacy Officer (PO) stuurt de DPIA naar de centrale privacy officer voor een eerste kwaliteitscheck. Na eventuele aanpassingen door het team wordt de DPIA naar de FG gestuurd door de PO. De FG stelt na ontvangst van de DPIA een zwaarwegend, formeel advies[14] op en stuurt deze naar het sectorhoofd. Het advies bevat verschillende uit te voeren acties alsmede een advies voor een herhaal DPIA. De PO toetst bij de proceseigenaar de voortgang van de uit te voeren acties. De toetsing van de opvolging van de acties door de PO gebeurt door navragen bij

[14] Dit advies is wettelijk verplicht (artikel 35 lid 2 AVG). Er kan van worden afgeweken mits dit beargumenteerd wordt vastgelegd. Dit conform de richtlijnen van de Autoriteit Persoonsgegevens en het Eindhovens privacybeleid.

betreffende medewerkers. De PO controleert niet of de implementatie daadwerkelijk heeft plaatsgevonden.

Bureau FG werkt zeer zorgvuldig en zet zaken uitgebreid uiteen. Uit de interviews blijkt dat de organisatie moeite heeft om de volledigheid en zorgvuldigheid van de gekozen werkwijze over te nemen. Gekeken naar de inhoudelijke AVG en AP vereisten blijkt dat de organisatie nog altijd niet zelfstandig over de nodige kennis en capaciteiten beschikt om op de voorgeschreven manier een DPIA in te vullen. Ook wordt te laat met dit traject gestart, wanneer een project of proceswijziging soms al gestart is. Uit de interviews blijkt tevens dat, mede vanwege de hoge standaard en strakke naleving van de gestelde AVG normen, in de praktijk weerstand merkbaar is in de richting van bureau FG. Vanwege de achterstand adviseren we de gemeente om te verkennen of een efficiëntere uitwerking van DPIA's mogelijk is. Een betere samenwerking zal er ons inziens tevens voor zorgen dat bureau FG eerder wordt betrokken bij nieuwe projecten.

2.3.3 DPIA's

Voor verwerkingen die gestart waren voor mei 2018 is de deadline voor het invullen van DPIA's van de AP inmiddels verstreken (mei 2021).[15] Voor nieuwe verwerkingen is een achterstand met het invullen van DPIA's. Dit jaar zijn risicovolle verwerkingen toegenomen zonder dat een DPIA is gestart dan wel is afgerond.
Het is van groot belang om tijdig een juiste en volledige DPIA uit te voeren, omdat hiermee wordt gecontroleerd of de (te starten/wijzigen) verwerking voldoet aan de AVG en/of welke maatregelen of aanpassingen gedaan moeten worden binnen de verwerking. De DPIA is een waarborg voor een goede gegevensbescherming vanuit perspectief van de inwoners (beschermen van de inwoners), een kwaliteitsinstrument voor de organisatie en een waarborgdocument waarin de gemeente verantwoording aflegt.

2.3.4 Bewustzijn

Bureau FG brengt twee rapportages uit om de raad te informeren: een rapportage voor de verwerkingen van persoonsgegevens, die onder verantwoordelijkheid van de gemeenteraad worden uitgevoerd. Deze worden aan de gemeenteraad aangeboden met een memo van burgemeester (voorzitter van de raad) en de griffier. Voor de verwerkingen die onder verantwoordelijkheid van het college van B&W worden uitgevoerd, wordt de jaarrapportage door B&W voorzien van een raadsinformatiebrief. In de raadsinformatiebrief geeft B&W aan wat zij met de adviezen en aanbevelingen van bureau FG gaan doen. I
Uit de interviews blijkt dat er echter weinig tot geen vragen vanuit de raad worden gesteld over het borgen van gegevensbescherming bij bijvoorbeeld diverse raadsvoorstellen en raadinformatiebrieven.

[15] Voor verwerkingen die gestart waren vóór mei 2018 had de AP een zachte deadline voor het invullen van DPIA's (mei 2021). Hiervoor zijn reële planningen per sector opgesteld die gevolgd worden, zodat de DPIA's op zorgvuldige wijze ingevuld kunnen worden. Van belang voor betrokkenen is namelijk dat naar de bedoeling van de AVG wordt gehandeld op zorgvuldige wijze (in plaats van DPIA's "af te vinken" zodat een zachte deadline gehaald werd).

Recent is er aandacht geweest om medewerkers meer bewust te maken en uitleg te geven over het melden van datalekken. Dit heeft geresulteerd in een stijging in het aantal datalekken dat gemeld is. Medewerkers kunnen datalekken melden bij de FG. De sector zorgt voor registratie van de melding in het datalekkenregister. Dit verloopt in de praktijk via de privacy officer. De FG beoordeelt of melding gemaakt moet worden bij de AP en hoe de melding kan worden opgepakt. Per januari 2022 worden deze werkzaamheden belegd bij de PO, om de rolzuiverheid van de FG meer te waarborgen.

2.3.5 Algemene constatering classificatie

Alhoewel Hoffmann geen specifiek onderzoek heeft gedaan naar de werkwijze in de classificatie van informatie is het opgevallen, dat de ontvangen en gereviewde documenten niet voorzien zijn van een classificatie vermelding. Het informatie beveiligingsbeleid[16] stelt dat er vier niveaus van classificatie gelden: Openbaar, Bedrijfsvertrouwelijk, Vertrouwelijk en Geheim. Nu is het in het IB beleid niet helder omschreven op welke wijze deze classificatie dient te worden ingevoerd, echter een van de maatregelen kan een vermelding op het document zijn. Advies is te overwegen om de classificatie actief te vermelden op de documenten.

2.4 Toekomst

Aangezien binnen de gemeentelijk organisatie de sectorhoofden verantwoordelijk zijn voor het risicomanagement is het de vraag of deze ook gericht zijn op bredere (toekomstige) dreigingen en risico's. Het is aannemelijk dat binnen de sectoren voornamelijk oog is voor de operationele risico's binnen de bestaande processen waardoor mogelijk sector overschrijdende risico's worden gemist. Een voorbeeld hiervan is het risico van ransomware en dan met name de ontwikkeling hiervan. De bestudeerde risicoanalyses zijn voornamelijk incident gedreven en in retroperspectief opgemaakt. Het niet tijdig in kunnen spelen op dit soort dreigingen maakt de organisatie kwetsbaar, juist ook omdat de aanpak voor het managen of voorkomen van dit soort risico's aanvullende beveiligingsmaatregelen vraagt binnen de sectoren (bv bewustzijn, actief bijdragen aan cyberveilig gedrag, etc.). Het advies is om naast de sectorale risicoanalyses en risicomanagement via de CIO en CISO, periodiek (jaarlijks) een Risicoanalyse Informatiebeveiliging uit te voeren die helpt bij de verder inrichting een Informatie Security Management Systeem (ISMS) en beheersing van de risico's.

Andere bevindingen en toekomstige uitdagingen die uit het onderzoek naar voren zijn gekomen zijn:

- Inzet van smart city toepassing dient te voldoen aan geldende en toekomstige wet- en regelgeving > rapport AP;
- Transitieplan n.a.v. onderzoek Gartner. Uit dit onderzoek kwam naar voren dat de IT organisatie qua maturity level op het laagste niveau scoort, te weten middelen organisatie (licht schurend tegen proces organisatie). De ambitie is uitgesproken om te veranderen naar een service organisatie (licht schurend tegen een waardeketen). Proces en procesinrichting wordt hierbij het eerste belangrijke onderwerp;

[16] Zie hoofdstuk 4.4 van het Informatiebeveiligingsbeleid Gemeente Eindhoven 2019

- Vaststellen nieuw informatiebeveiligingsbeleid welke actief wordt uitgedragen door directie/ bestuur;
- Investeren in voldoende kennis en kunde bij personeel om bij te blijven in het snel veranderende landschap van informatiebeveiliging.

3. Mens (social engineering)

In dit hoofdstuk worden de bevindingen in detail beschreven en zijn schermafdrukken opgenomen ter illustratie.
Het cyber(on)veilige gedrag van de medewerkers is getest door middel van de volgende manier:

1. Mail-phishing, waarbij er een e-mail is verstuurd die uitnodigde op een link te klikken en de gebruiker te verleiden om persoonlijke inloggegevens af te geven;

3.1 Mail phishing-aanval

De onderzoekers waren in eerste instantie niet in staat om met de phishingmail direct door de beveiliging (spamfilter) van de gemeente te komen.
De gemeente heeft hierop de beveiliging specifiek en alleen voor deze actie aangepast zodat de phishing test uitgevoerd kon worden. De onderzoeker ontving 2955 e-mailadressen van de gemeente. Naar al deze-mailadressen is op dinsdag 19 oktober 2021 vanaf 14:18 uur tot ongeveer 17:00 een phishing e-mail verstuurd. De onderzoeker heeft het domein ‘gemeente-eindhoven.com’ geregistreerd. Via dit domein zijn vanaf het e-mailadres ‘servicedesk@gemeente-eindhoven.com’ de e-mails met Eindhovense opmaak verstuurd.

Autorisatie netwerk apparatuur

Servicedesk <servicedesk@gemeente-eindhoven.com>
Aan

Deze afzender servicedesk@gemeente-eindhoven.com is afkomstig van buiten uw organisatie.

Lees deze mail goed door om problemen met je Wi-FI te voorkomen

Beste Collega,

De Wi-Fi toegang gaat verlopen over 2 dagen. In deze mail staat beschreven hoe je dit kan wijzigen.
Om het draadloze netwerk te beschermen tegen ongeautoriseerde apparaten dienen alle apparaten waarop je draadloos Wi-Fi gebruikt eenmalig geregistreerd te worden.
Door in te loggen met je laptop, smartphone of iPad wordt je account toegevoegd aan de database van geautoriseerde systemen.

Instructie apparaat koppelen
Om toegang tot het draadloos Wi-Fi netwerk te behouden klik je thuis of op kantoor op de onderstaande link naar het Wi-Fi portaal van de Gemeente Eindhoven en log je in om het apparaat te registreren.

https://wifi.gemeente-eindhoven.com

Waarom?
- Een niet veilig Wi-Fi bedrijfsnetwerk kan tot gevolg hebben dat anderen toegang krijgen tot het gemeentenetwerk.
- De Gemeente Eindhoven loopt dan het risico dat de bedrijfsinformatie en persoonsgegevens in handen van anderen kunnen komen.

Actie vereist!
Indien je geen actie onderneemt, zal de toegang tot het draadloos netwerk verlopen binnen enkele dagen.

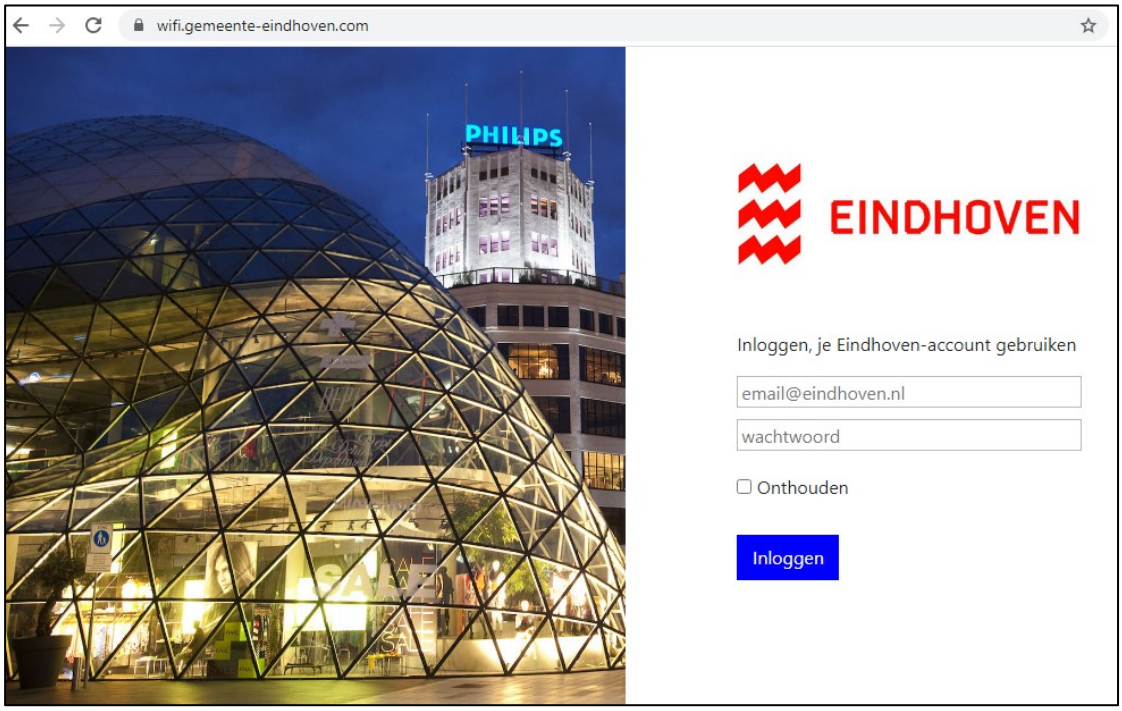
Loop je hierna toch tegen problemen aan? Neem dan contact op met de Servicedesk ICT, via de Self Service Portal, of telefonisch via (040 238) 2222.

Met vriendelijke groet,

ICT Servicedesk,
ICT Servicedesk| noreply@eindhoven.nl |
(040 238) 2222

EINDHOVEN

Figuur 1: Phishing e-mail 'gemeente-eindhoven.com', met als onderwerp 'Autorisatie netwerkapparatuur'. Gebruikers die op de knop 'Inloggen' klikten kregen de website in figuur 2 te zien. Een oplettende gebruiker herkende dit e-mail bericht als phishing en heeft bovenstaande afbeelding inclusief rode markeringen op het intranet van de gemeente geplaatst.



Figuur 2: Phishing website gemeente 'wifi.gemeente-eindhoven.com'.

Doordat de link naar de website een uniek ID bevat, kon worden geregistreerd hoeveel unieke gebruikers de website bezochten en/of hun gebruikersnaam en wachtwoord invulden. De wachtwoorden van gebruikers zijn niet geregistreerd tijdens de mail phishing.
Op de eerste dag zijn er tot 18:00 uur 487 gebruikers geregistreerd die hun gebruikersnaam en wachtwoord hebben ingevuld. Omstreeks 18:01 uur heeft de gemeente een e-mail gestuurd over de gesimuleerde phishing-aanval. Na die tijd zijn er nog 126 gebruikers geweest die hun gebruikersnaam en wachtwoord hebben ingevuld.

Figuur 3: Melding over de phishing mail van de servicedesk gepost op het intraweb.

Er zijn in totaal 686 unieke bezoekers geregistreerd (23%) waarvan 613 gebruikers (21%) hun gebruikersnaam en wachtwoord hebben ingevuld. Het wachtwoord is niet opgeslagen, ook zijn de credentials niet getest op geldigheid. Het aantal geldige credentials is waarschijnlijk lager dan 613. De mail-phishing campagne is gestopt op donderdag 21 oktober 2021 omstreeks 18:00.

De onderzoekers identificeren dit als een risico in de categorie ‘hoog’ omdat het percentage medewerkers die credentials hebben ingevoerd op de phishing site vrij hoog ligt. Deze medewerkers hebben ook de waarschuwing dat de e-mail afkomstig was van buiten de organisatie (zie figuur 1) over het hoofd gezien. Het risico van remote inloggen door middel van credentials verkregen door de phishing wordt grotendeels gemitigeerd door multi-factor authenticatie. Met deze credentials kan wel ingelogd worden op het draadloze netwerk. Wij adviseren gemeente hier de nodige stappen te nemen, waaronder medewerkers bewust te maken van mail-phishing-technieken door bewustwording en gedragsveranderingsprogramma’s; en te zorgen dat medewerkers weten welke domeinnamen van de gemeente zijn en dat ze geen gebruik moeten maken van andere domeinen.

4. Techniek (penetratietesten)

De (werking van) de informatiebeveiliging is onderzocht met behulp van externe, interne penetratietesten en penetratietest van het WiFi-netwerk.

4.1 Rapportage penetratietesten

Techniek (penetratietesten)
Tijdens het onderzoek zijn kritieke kwetsbaarheden geconstateerd. De specifieke bevindingen, impact en aanbevolen aanbevelingen naar aanleiding van zowel de externe als de interne penetratietest zijn vanwege de diepgang en vertrouwelijkheid gedeeld met de ambtelijke organisatie.

5. Conclusies en aanbevelingen

5.1 Conclusies

5.1.1 Organisatie

Informatiebeveiliging is binnen de gemeente Eindhoven momenteel teveel een “bottom up” proces. Een aantal verantwoordelijke functionarissen werken hard aan het verbeteren van de veiligheid en beveiliging van de informatie binnen de gemeente, echter ervaren beperkte steun vanuit de organisatie. Binnen de organisatie zijn de risico’s onvoldoende breed bekend en is er (nog) geen aansturing vanuit beleid. Mogelijk dat het nieuw opgestelde beleid (niet beoordeeld) meer draagvlak en bijbehorende aansturing vanuit de directie krijgt. Het algehele beeld dat is dat informatiebeveiliging onvoldoende op de agenda staan van het College en de Raad en dit de uitwerking in praktijk bemoeilijkt.

5.1.2 Mens (social engineering)

Naar aanleiding van 2.955 verstuurde phishing e-mails hebben 686 gebruikers (23%) de unieke link in de e-mail geopend. In totaal zijn er 613 inlogpogingen van unieke gebruikers met geldige e-mailadressen geregistreerd (21%). Dit laat zien dat het merendeel van de medewerkers zich bewust was dat de e-mail een phishing mail betrof of op tijd de waarschuwingen van collega’s over deze e-mail meekreeg. Echter gezien de hoeveelheid inlogpogingen is er zeker nog ruimte voor verbetering.

5.1.3 Techniek

Tijdens het onderzoek zijn kritieke kwetsbaarheden geconstateerd die onmiddellijk met het team ICT-beleid en -beheer zijn gedeeld. Vanwege de diepgang en vertrouwelijkheid zijn de technische uitkomsten en aanbevelingen van de pentesten gedeeld met de ambtelijke organisatie.

5.2 Aanbevelingen

Uit het onderzoek zijn meerdere bevindingen naar voren gekomen die een risico vormen voor de informatiebeveiliging van de gemeente. In bijlage 1 is een top 5 van bevindingen gemarkeerd waar volgens de onderzoekers prioriteit aan gegeven dient te worden met impact en aanbevelingen. In de tabel wordt voor de specifieke bevinding ook verwezen naar de paragraaf, waar deze bevinding verder is omschreven.

Disclaimer

Ondanks het feit dat de onderzoekers zeer zorgvuldig onderzoek verrichten, bestaat de mogelijkheid dat zij niet iedere kwetsbaarheid detecteren in de IT-infrastructuur van onze opdrachtgever. Dit komt mede doordat onze medewerkers gebonden zijn aan een budget- en tijdslimiet (een penetratietest is altijd een momentopname).
Dit rapport is geschreven voor de opdrachtgever, zodat hij of zij staat wordt gesteld om maatregelen te nemen teneinde de cyberweerbaarheid van zijn/haar organisatie te verhogen. Wij kunnen geen aansprakelijkheid aanvaarden voor acties of maatregelen die door opdrachtgever of diens vertegenwoordigers op basis van het rapport worden ondernomen. Tenslotte verwijzen wij naar de van toepassing zijnde dienstverleningsvoorwaarden.

Bijlagen

Bijlage 1 Overzicht bevindingen en aanbevelingen[17]

Paragraaf	Bevinding	Impact	Aanbeveling
2.1.1	Vaststelling en versie van het IB-beleid zijn niet terug te vinden in het beleidsdocument zelf.	Voor de lezer is het onduidelijk wat de status van het document is en of dit door de organisatie is vastgesteld.	Het is raadzaam om de vaststelling van een beleid door het College en de directieraad in het document zelf op te nemen. Zo is voor de lezer duidelijk wat de status van het document is.
2.1.1	In het IB-beleid wordt geen frequentie en proces beschreven hoe en wanneer het IB-beleid geactualiseerd wordt. Dit document verwijst nog naar verouderde wetgeving (BIG).	Het beleid veroudert en geeft geen actuele kaders en richtlijnen voor de organisatie om naar te handelen.	Het is raadzaam om dit periodiek (jaarlijks) te evalueren en waar nodig te actualiseren. Zorg dat het nieuwe beleid verwijst naar het huidige normenkader (BIO).
2.1.1	Het IB-beleid sluit niet (voldoende) aan bij de praktijk van de organisatie. De 'ist' en 'soll' situatie wordt vaak door elkaar beschreven.	Het IB-beleid is opgesteld door een externe partij en lijkt afstemming te missen met de organisatie. Omdat het beleid onvoldoende aansluit met de praktijk blijft de opvolging en naleving van het beleid in de praktijk uit.	Een IB-beleid (en elk ander beleid) werkt het best als het voor en door de organisatie zelf wordt opgesteld en aansluit bij de actuele praktijk, cultuur en uitgangspunten van de organisatie. Aangepast beleid mag nog meer aansluiten op het normenkader van de BIO.
2.1.2	Bij de aanschaf van (IT) producten en diensten en innovatieve ontwikkelingen (living labs) worden Security en Privacy Officers niet, of (te) laat betrokken, waardoor eisen m.b.t. informatiebeveiliging niet voldoende worden gewaarborgd.	Er worden (IT) producten en diensten aangeschaft of ontwikkeld en in gebruik genomen die niet voldoen aan het IB-beleid en de gestelde beveiligingseisen.	Bij elke aanschaf moet worden voldaan aan de eisen m.b.t. informatiebeveiliging[18]. De eisen dienen voor het sectorhoofd/de inkoper helder en vindbaar te zijn.

[17] Rood gearceerd zijn top 5 aanbevelingen en conclusies
[18] Zie hiervoor BIO "Leveranciersrelaties". Hoofdstuk 15.1

2.1.2	Tijdens de looptijd van een contract wordt niet (voldoende) gecontroleerd of het product/de leverancier voldoet aan de door de gemeente gestelde (in het contract opgenomen) eisen m.b.t. informatiebeveiliging.	De aangeschafte (IT) producten en diensten en/of de leverancier die het levert voldoen niet aan het IB-beleid en de gestelde beveiligingseisen.	Periodiek (minimaal jaarlijks) dient er een controle uitgevoerd te worden op de naleving van eisen m.b.t. informatiebeveiliging[19].
2.1.3	Tijdens calamiteiten wordt er ad hoc geacteerd en worden functionarissen betrokken via het informele netwerk dat men met elkaar heeft. Er is geen crisisteam formeel vastgesteld.	Tijdens een calamiteit worden niet de juiste medewerkers geïnformeerd en/of is er niet voldoende mandaat om beslissingen te nemen.	Stel een calamiteitenplan op waarin duidelijke processen, rollen en beslissingsbevoegdheden van actoren beschreven staan. Plan een periodieke oefening (inclusief evaluatie) om te waarborgen dat het plan in praktijk functioneert.
2.1.3	Beschikbaarheidseisen van kritische applicaties zijn zeer algemeen vastgesteld in het document “Proces Calamiteit, Bijlage 1 Prioriteitenmatrix”. De aangegeven oplostijd is <1 uur, er is echter geen plan geformuleerd hoe dit gerealiseerd kan worden.	Kritische applicaties kunnen mogelijk niet binnen de gestelde tijd hersteld zijn. geformuleerd hoe dit . in de praktijk gerealiseerd dient te worden.	Breid document bedrijfsapplicaties per domein uit met een concreet business recovery plan voor de bedrijf kritische applicaties.
2.1.4	De gemeente loopt achter met het patchen van hard- en software. Er wordt een inhaalslag gemaakt om aan de ambitie n -1 te voldoen.	Wanneer een organisatie niet tijdig (security) patches installeert is een organisatie kwetsbaar voor security breaches. Ransomeware maakt gebruik van kwetsbaarheden in systemen om het netwerk binnen te dringen.	Het is in eerste instantie zaak om alle hard- en software op het gewenste patch niveau te krijgen. Daarnaast dient er een degelijk proces ingericht te worden om op ambitie niveau n -1 te blijven.

[19] Zie hiervoor BIO “Beheer van dienstverlening van leveranciers”. Hoofdstuk 15.2

2.1.4	De gemeente heeft drie opties om kwetsbaarheden in de IT omgeving te detecteren - Vulnarability scan - Intern test - Externe test Er is geen concrete planning geconstateerd om deze periodiek uit te voeren.	Onvoldoende inzage in de kwetsbaarheden van het systeem.	Periodiek testen van IT omgeving, waarbij onafhankelijkheid van testen geborgd is door een combinatie van intern en extern testen.
2.2.2	Voor bepaalde functies geldt dat hun taken en verantwoordelijkheden niet helder zijn afgebakend in de uitvoering.	Wanneer taken en verantwoordelijkheden niet helder zijn afgebakend kan het voorkomen dat medewerkers elkaar overlappen in verantwoordelijkheden wat tot spanningen kan leiden of dat zaken juist niet worden opgepakt, omdat niemand verantwoordelijk is.	Taken en verantwoordelijkheden (m.b.t. informatiebeveiliging en privacy) ook beleggen en mandateren.
2.2.3	Bepaalde toezichthoudende of toetsende functies vervullen adviserende taken.	Vermenging van adviserende en toetsende/toezichthoudende taken binnen een functie gaat ten koste van de rolzuiverheid en maakt dat de toetsing of het toezicht niet voldoende onafhankelijk plaats vindt.	Ga verder met het creëren van een duidelijke scheiding in adviserende en onafhankelijk toetsende en toezichthoudende functies. “Tone at the top” en commitment vanuit de directie is hierbij van groot belang.
2.2.4	De CISO heeft niet voldoende mandaat om zaken af te dwingen bij DISO’s en de organisatie.	Besluiten m.b.t. onveilige situaties worden overruled waardoor gemeente risico loopt.	Leg mandaat en bevoegdheden van functies formeel vast. Zorg dat implementatie van maatregelen via de lijn worden geaccordeerd.
2.2.5	Binnen de IB functies zijn nog niet alle verantwoordelijke medewerkers voldoende opgeleid.	Functies bekleed door medewerkers die verantwoordelijk zijn voor informatiebeveiliging ontberen specifieke kennis om hun werk adequaat en met voldoende kwaliteit uit te voeren.	Breng het kennistekort in kaart en leid medewerkers op tot het niveau waarop zij voldoende vakkennis bezitten. Indien gewenst overweeg inhuur van expertise.

2.2.6	Te weinig afbakening tussen strategisch, tactisch en praktisch niveau. Medewerkers op strategische functies acteren op operationeel niveau en passeren daarmee de verantwoordelijke functionarissen.	Teveel capaciteit en aansturing op operationeel niveau, te weinig aandacht voor strategische thema's en uitwerken van een visie op structurele verbeteringen en vernieuwingen, en mogelijke demotivatie van verantwoordelijke medewerkers.	Heldere verdeling en afbakening van taken en verantwoordelijkheden op strategisch, tactisch en operationeel niveau en een formele vastlegging hiervan.
2.2.7	PO's en DISO's zijn per sector aangesteld en niet centraal georganiseerd.	Een decentrale inrichting van de PO en ISO functies leidt tot een verlies aan slagkracht gemeentebreed. Daarnaast leidt dit tot een problematische functionele aansturing voor uitvoering strategische beleid in de sector.	Functies DISO en PO centraal in organisatie beleggen i.p.v. per sector.
2.2.8	Eigenaarschap niet voldoende ingericht.	Audit bevindingen en andere werkzaamheden worden niet tijdig en volledig opgepakt omdat men zich geen eigenaar voelt.	RACI opstellen en implementeren voor alle applicaties en processen.
2.2.9	Teveel "blind" vertrouwen op inzet externe adviseurs en accountant, waarbij advies zonder interne review en betrokkenheid wordt overgenomen.	Externe adviezen worden overgenomen zonder hierbij de interne organisatie te betrekken. Risico hierbij is tweeledig: - Externe adviezen zijn niet altijd sluitend voor wat betreft de praktijk van Gemeente Eindhoven. - Interne organisatie leert te beperkt van de bevindingen, of wordt niet meegenomen in de oplossingen en raakt gedemotiveerd.	Advies van externe adviseurs blijven toetsen aan de interne expertise en eigen praktijk en de interne organisatie nauwer betrekken bij de oplossingen.
2.1.1 2.3.1	Onvoldoende wisselwerking tussen bestuur en organisatie m.b.t. informatiebeveiliging en privacy.	Het bestuur is onvoldoende op de hoogte wat er speelt m.b.t. informatiebeveiliging en privacy. Lage bewustwording van medewerkers en de naleving van beleid, wegens gebrek aan bewustwording bij bestuur ("tone at the top").	Vanuit de organisatie investeren op het bestuur meer te betrekken, door bijvoorbeeld rapportages en informatievoorziening.

2.3.3	Gemeente loopt achter met het uitvoeren van DPIA's.	Verwerkingen zijn gestart zonder dat er een DPIA is opgesteld en zijn mogelijk onrechtmatig en voldoen niet aan eisen m.b.t. informatiebeveiliging en privacy.	Inhaalslag blijven maken met DPIA's en monitoren van reeds gestarte verwerkingen. Tijdig opstellen van DPIA's in processen formaliseren.
3.3.2	Uitgebreide en zorgvuldige manier van werken van Bureau FG stelt een hoge norm voor de uitvoering in de praktijk.	Achterstand DPIA's en weerstand in samenwerking met bureau FG.	Onderzoek of een efficiëntere werkwijze voor bijvoorbeeld het uitwerken van DPIA's mogelijk is
2.3.5	Er is geen duidelijk classificatie proces, waarbij het op documenten van de gemeente helder is welke vertrouwelijkheid het document heeft.	Het risico hiervan, is dat vertrouwelijke documenten die beschikbaar zijn bij medewerkers, niet als zodanig worden (h)erkent en ze mogelijk onbedoeld, maar onrechtmatig worden gedeeld.	Voer een helder beleid op gebied van classificatie van documenten in en zorg dat zichtbaar wordt op de documenten welke rubricering van toepassing is.
2.4	Onvoldoende inzicht in en sturing op risico's en (toekomstige) dreigingen. Risicoanalyses zijn incident gedreven.	Het niet tijdig in kunnen spelen op (toekomstige) dreigingen maakt de organisatie kwetsbaar.	Implementatie van risicomanagement en uitvoeren van dreigingsanalyses en deze periodiek actualiseren.
2.4	Er is geen ISMS geconstateerd bij de gemeente Eindhoven, waarmee er structureel een PDCA aanpak op informatiebeveiliging (IB) wordt geborgd	Door het missen van een ISMS, ontstaat het risico dat IB op ad-hoc basis wordt georganiseerd en dat (nieuwe) dreigingen en risico's onvoldoende adequaat worden (h)erkent en beheerst	Een ISMS dient aan te sluiten op het beleid en de strategie van de organisatie en dient geïntegreerd te worden in de bestaande processen. Het doel van een ISMS is (vertrouwelijke) informatie beter te beveiligen.
2.1.2	Wachtwoordenbeleid schrijf voor dat wachtwoorden minimaal één speciaal teken moet bevatten, Uit technisch onderzoek blijkt dat dit niet wordt afgedwongen door het systeem.	Minder complexe wachtwoorden vormen een grotere kwetsbaarheid voor hacks (bijvoorbeeld password spraying/brute force attacks)	Zorg ervoor dat het systeem de eisen waar een wachtwoord aan dient te voldoen technisch afdwingt. Neem medewerkers mee in het hoe en waarom; waarom is een complex wachtwoord belangrijk en hoe is deze het beste vorm te geven?

2.1.2	Het beveiliging beleid schrijft voor dat wachtwoorden versleuteld en niet in originele vorm (plain text) opgeslagen of verstuurd mogen worden. Dit wordt in praktijk niet nageleefd. Wachtwoorden in leesbare tekst verstuurd via e-mail en opgeslagen in word bestanden.	De beschikbaarheid/leesbaarheid van wachtwoorden in bestanden of mail maakt dat kwaadwillenden deze relatief gemakkelijk kan onderscheppen en hiermee de veiligheid van andere systemen/bestanden niet meer te garanderen is.	Verhoog het bewustzijn onder medewerkers over wat het beveiliging beleid voorschrijft op het gebied van wachtwoorden. Schenk tevens aandacht aan het hoe en waarom.
3.1	Van de 2.955 gebruikers heeft 23% de unieke link in de e-mail geopend. In totaal zijn er 613 inlogpogingen van unieke gebruikers met geldige e-mailadressen geregistreerd (21%).	**Hoog** Een significant aantal medewerkers is kwetsbaar voor phishing-aanvallen waarbij getracht wordt inloggegevens te achterhalen. Wanneer een kwaadwillende over deze gegevens beschikt kan hij zich daar toegang mee verschaffen tot de systemen van de gemeente.	Leer medewerkers hoe zij phishing e-mails kunnen herkennen. Zorg dat medewerkers weten hoe te handelen in geval van twijfel.

Bijlage 2 Overzicht geïnterviewden

Functie
CIO
CISO
FG
Sectorhoofd I&B
Concerncontroller
Controller Interne IT auditor
Coördinerend Privacy Officer
Directeur bedrijfsvoering en dienstverlening
Wethouder van Financiën en bedrijfsvoering
Wethouder van Financiën en bedrijfsvoering a.i.

Bijlage 3 Overzicht bestudeerde documenten

Onderstaande tabel bevat de documenten die zijn ontvangen vanuit de gemeente Eindhoven en bestudeerd ten behoeve van het onderzoek naar de organisatie van informatiebeveiliging.

Document	Versie	Datum
Informatiebeveiligingsbeleid Gemeente Eindhoven 2019, De basis voor een betrouwbare gemeentelijke dienstverlening	1.0	31-01-2019
Privacy Beleid Gemeente Eindhoven 2020-2023	-	Juni 2021
Proces Calamiteit	1.7	Januari 2021
Jaarrapportage 2019, bescherming van persoonsgegevens (AVG)	-	Januari 2020
Jaarrapportage 2020, Bescherming van persoonsgegevens (AVG)	-	Maart 2021
Onderzoek Smart Cities, Autoriteit Persoonsgegevens	-	Augustus 2020
Raadsinformatiebrief Onderwerp: Pilot Bodycam	21.27.202	6-07-2021
Bedrijfsapplicaties Per Domein (PPT)	PDF 1.7	27-08-2021
Raadsinformatiebrief Onderwerp: Privacy beleid	21.26.202	29-06-2021
Raadsvragen: Data Belastingdienst in strijd met de privacywetgeving?	21.28.103	13-07-2021
TURAP-1	-	2021
Raadsinformatiebrief: Informatieveiligheid en ENSIA audit DigiD, Suwinet, BAG, BGT en BRO	9.26.202	25-06-2019
Deloitte: Managementletter 2020, Bestuurlijk relevante bevindingen en aanbevelingen interim-controle	-	26-11-2020
Overzicht gemeentelijke verwerkingen van belastingdienst data (op basis van antwoorden februari 2021)	-	15-04-2021
Raadsinformatiebrief Formatie ontwikkeling	20.15.202	07-04-2021
Raadsvragen: ‘Impact Corona-crisis ambtelijke organisatie’ (vervolg')	21.21.103	25-05-2021
Raadsinformatiebrief: Onderzoek naar het gebruik van persoonsgegevens, die de Belastingdienst heeft verstrekt aan de gemeente Eindhoven.	21.15.104	13-04-2021
Jaarstukken 2019	-	04-06-2019
Beheersmaatregelen gemeente Eindhoven RAET HR Systeem	-	6-12-2019
Memo: Betreft: Advies ex artikel 35 AVG van de Functionaris Gegevensbescherming (FG) bij de Data Protection Impact Assessment (DPIA) pilot bodycam voor boa’s van sector Ruimtelijke Uitvoering.	-	3 juni 2021
Rapport Data Protection Impact Assessment – AVG: Risico’s en maatregelen bij Toezicht en handhaven in de stad ANPR-auto	2.4 definitief	14 april 2021

Document	Versie	Datum
Memo: Betreft: Advies ex artikel 35 AVG van de Functionaris Gegevensbescherming (FG) bij de Data Protection Impact Assessment (DPIA) Inzet ANPR auto bij handhaven parkeren van sector Ruimtelijke Uitvoering.	-	9 april 2021
Rapport Data Protection Impact Assessment – AVG: Risico's en maatregelen bij Tijdelijke overbruggingsregeling zelfstandig ondernemers (Tozo)	2.0	Maart 2021
Memo: Betreft: Advies ex artikel 35 AVG van de Functionaris Gegevensbescherming (FG) bij de Data Protection Impact Assessment (DPIA) Tozo van Sociaal Domein.	-	25 maart 2021
Rapport Data Protection Impact Assessment – AVG: Risico's en maatregelen bij Beheer KCC Contactformulieren	1.0 definitief	Juli 2020
Memo: Betreft: Advies ex artikel 35 AVG van de Functionaris Gegevensbescherming (FG) bij de Data Protection Impact Assessment (DPIA) Beheer KCC Contactformulieren van sector Publiekscontacten.	-	4 mei 2021
Rapport Data Protection Impact Assessment – AVG: Risico's en maatregelen bij Beheer ICT-Projecten	0.2	Juli 2021
Memo: Betreft: Advies van de Functionaris Gegevensbescherming (FG) bij de Data Protection Impact Assessment (DPIA) Beheer ICT projecten van de sector Informatisering en Beheer (IenB).	-	Juli 2021
002.1 covid-19 CISO als onderdeel van het Crisis Management Team	-	-
Beheersmaatregelen gemeente Eindhoven RAET HR Systeem P&O	-	6-12-2019
008.1 Privacy en Security advies inzake Huis van Werk	-	-
008.2 Privacy en Security advies inzake projecten _ applicaties	-	-

Bijlage 4 Begrippenlijst

BCM: (*Business Continuity Management)* bedrijfscontinuïteitsbeheer.

BIA: (*Business Impact Analysis*) analyse van bedrijfsprocessen om onderscheid te kunnen maken tussen kritieke en niet kritieke bedrijfsprocessen.

DPIA: een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

ISMS: (*Information security management system*) managementsysteem voor informatiebeveiliging.

RACI: matrix die gehanteerd wordt om de rollen en verantwoordelijkheden van de personen die bij een project of werkzaamheden betrokken zijn weer te geven. RACI staat voor Responsible, Accountable, Consulted, Informed.