

Aan de leden van de gemeenteraad

12 december 2024

Geachte leden van de gemeenteraad,

Belang van informatieveiligheid

Een betrouwbare en veilige informatievoorziening is essentieel voor gemeenten. Door de toegenomen digitalisering wordt het steeds belangrijker om zorgvuldig om te gaan met de gegevens van burgers en organisaties. Het noodzaakt gemeenten extra aandacht te hebben voor de bescherming van persoonsgegevens en de privacy van inwoners.

Onderzoek Informatieveiligheid 2020

In 2020 heeft de rekenkamercommissie in 2020 een onderzoek verricht naar de effectiviteit en doelmatigheid van de informatieveiligheid in Oss. Gelet op het technische karakter van het onderzoek is er voor gekozen om dit onderzoek uit te besteden aan een extern bureau.

Destijds werd door ons geconcludeerd dat de veiligheid van de systemen waarvan de gemeente Oss gebruik maakt onvoldoende is. Onderzoekers konden op afstand toegang krijgen tot e-mail, wachtwoorden, fileshares, desktops en diverse programma's. Tevens hebben de onderzoekers twee dagen vanuit het gemeentehuis kunnen werken door het bemachtigen van onderhoudspassen. Overigens geldt daarbij de opmerking dat de onderzoekers wel zijn gesignaleerd door de bode en dat de CISO (Chief Information Security Officer) hierna is ingeschakeld.

De onderzoekers hebben binnen de beschikbare tijd geen beheerrechten kunnen verkrijgen op het netwerk. Vanwege het aantal en de ernst van de aangetroffen kwetsbaarheden, de grote hoeveelheid informatie en het aantal nog nader te onderzoeken systemen, was het volgens de externe onderzoeker echter zeer waarschijnlijk dat dit wel was gelukt met meer tijd.

De resultaten zijn besproken met de organisatie en de geconstateerde onvolkomenheden zijn hersteld voordat wij de resultaten van dit onderzoek hebben gepresenteerd. Overigens zijn de onderliggende onderzoeksresultaten, met het oog op de veiligheid, niet openbaar gemaakt.

Op basis van het onderzoek heeft de rekenkamercommissie de volgende aanbevelingen aan de raad gedaan:

1. Het herstel van de aangetoonde kwetsbaarheden te (laten) beoordelen door middel van een vervolgonderzoek.
2. De analyse van de overige vermoede kwetsbaarheden en het herstel daarvan in te zetten.

3. De informatiebeveiliging op een dusdanige wijze te laten organiseren dat de organisatie op korte termijn 'in control' komt op dit onderwerp, waarmee de koppeling wordt hersteld tussen gedrag, beleid en uitvoering. De aanpassingen in organisatie en processen moeten ervoor zorgen dat nieuwe risico's in de toekomst voorkomen worden;
4. Jaarlijks een 'stresstest' te plannen en uit te voeren om er zeker van te zijn dat er geen nieuwe kwetsbaarheden zijn ontstaan (door wijzigingen in het systeem of technologische ontwikkelingen);
5. De gemeenteraad van Oss binnen drie maanden te informeren over de aanpak en uitkomsten van bovenstaande aanbevelingen.

Onderzoek informatieveiligheid 2024

Inmiddels zijn we vier jaar verder. De afgelopen jaren hebben wij gemerkt dat er diverse maatregelen zijn doorgevoerd om de toegang tot systemen aan te scherpen. Naar aanleiding daarvan hebben wij besloten om de situatie rondom de informatieveiligheid opnieuw te bezien en uw raad te rapporteren over de voortgang en resultaten van de acties die na het uitbrengen van de eerste rapportage in gang zijn gezet.

Op basis van eerste gesprekken in de ambtelijke organisatie ontstaat een positief beeld. Wij constateren dat de aanbevelingen van de rekenkamercommissie zijn opgepakt. De technische omgeving wordt, onder andere met ondersteuning van een externe partij, regelmatig beoordeeld om te beoordelen of er kwetsbaarheden aanwezig zijn. Daar waar nodig worden verbeteringen aangebracht. Ook wordt aandacht besteed aan het vergroten van de bewustzijn van alle gebruikers van de systemen om alert te zijn op veiligheidsrisico's.

Onderzoeksvraag

Om te kunnen beoordelen of de genomen technische en organisatorische maatregelen voldoende zijn om de informatieveiligheid van de gemeente Oss te garanderen hebben wij een externe partij (LBVD) gevraagd om nader onderzoek te verrichten.

Centrale onderzoeksvraag: "Zijn de persoonsgegevens en andere gevoelige informatie bij de gemeente Oss in goede handen?"

De beantwoording van deze onderzoeksvragen is op de volgende drie aspecten gericht: Organisatie, Mens en Techniek.

We hebben ervoor gekozen het onderzoek via een viertal deelonderzoeken uit te voeren:

1. Voice phishing. Dit betreft een onderzoek met een telefonische mystery-guest. Bij dit onderzoek gebruikt de onderzoeker de telefoon om potentiële slachtoffers te misleiden om gevoelige informatie te verkrijgen, zoals inloggegevens, financiële gegevens en/of andere vertrouwelijke gegevens. Men kan zich voordoen als betrouwbare entiteit zoals: bankmedewerker, overheidsfunctionarissen, technische ondersteuning of vertegenwoordigers van bekende bedrijven. Een enkel telefoontje kan voor een cybercrimineel genoeg zijn om een groot incident te veroorzaken.
2. Fysieke mystery-guest.
Een fysieke mystery guest is een onderzoek, waarbij een onderzoeker een organisatie probeert te infiltreren. De onderzoeker doet zich bijvoorbeeld voor als monteur, serviceprovider, schoonmaker of nieuwe medewerker. Op deze manier kan inzicht verkregen worden in kwetsbaarheden op het gebied van (informatie)beveiliging en security awareness.

Voorbeelden van kwetsbaarheden zijn:

- Ongeautoriseerde toegang tot het kantoorpand, (beveiligde) werkruimtes en systemen.
- Het achterhalen van inloggegevens en andere vertrouwelijke gegevens
- Onzorgvuldig omgaan met apparatuur, informatie en dossiers op bureaus, bij printers en in kasten.

3. Phishing-simulatie

Een phishing simulatie geeft inzicht in hoeverre medewerkers phishingmails openen, of zij doorklikken op links of bijlagen en of er gevoelige gegevens worden achtergelaten.

4. Penetratietest

Met een penetratietest test de onderzoeker op realistische wijze de systemen. Hiermee wordt een helder inzicht verkregen in de risico's en kwetsbaarheden in de IT omgeving van de organisatie. De onderzoekers nemen de systemen net zoals echte cybercriminelen onder handen. Creativiteit en kennis spelen een essentiële rol in het vinden van risico's die anders onopgemerkt bleven.

Bij de genoemde vier deelonderzoeken zijn de volgende *deelvragen* geformuleerd:

Ad 1. Telefonische mystery-guest:

- a. Zijn medewerkers bewust van mogelijke risico's, en kennen ze de eigen rol in het voorkomen van incidenten op het gebied van informatiebeveiliging?
- b. Wat zijn de dreigingen voor het verkrijgen van (vertrouwelijke) informatie middels het medium 'telefoon'?

Ad 2. Fysieke mystery-guest:

- a. Zijn de huidige beveiligingsprocedures en -maatregelen toereikend om onbevoegden uit/bij het doelobject te weren?
- b. Reageren medewerkers en/of beveiligingsfunctionarissen op een ongenode gast op het terrein en/of in het gebouw?
- c. In welke mate kan een ongenode/onbevoegde gevoelige informatie bemachtigen?

Ad 3. Phishing-simulatie:

- a. Hoe is het gesteld met het huidige bewustzijn betreffende phishing e-mails binnen gemeente Oss?

Ad 4. Penetratietest:

- a. Welke kwetsbaarheden in het doelobject zijn via internet door een onbevoegde c.q. kwaadwillend persoon (een 'hacker') te vinden en mogelijk uit te buiten en vormen daarmee een bedreiging c.q. risico voor de organisatie?
- b. Kan een interne, maar kwaadwillende gebruiker zonder toegangsrechten zichzelf (extra) privileges verschaffen waardoor hij informatie kan bemachtigen of functionaliteiten kan aanspreken die niet voor hem/haar zijn bestemd?

Aanpak onderzoek

Voor dit onderzoek is gebruik gemaakt van zogenaamde ethische hackers en social engineers: onderzoekers die nagaan of de medewerkers kwetsbaar zijn voor misleiding en de systemen van de gemeente Oss extern of intern kwetsbaar zijn voor misbruik. Dit is met de ambtelijke organisatie afgestemd.

Resultaten

Algemene conclusie: In algemene zin kan gesteld worden dat persoonsgegevens en andere gevoelige informatie bij de gemeente Oss grotendeels in goede en veilige handen is. Dat neemt niet weg dat een aantal zaken kan worden verbeterd.

De risico's en kwetsbaarheden die tijdens het onderzoek naar voren zijn gekomen, zijn aan de verantwoordelijke medewerkers binnen de gemeente gemeld en door hen opgepakt. De mens blijkt de zwakke schakel te zijn als het gaat om risico's. Het spreekt voor zich dat in verband met de mogelijke veiligheidsrisico's hierover niet in openbaarheid gerapporteerd kan worden. Daarom zijn de onderliggende rapporten, opgesteld door het externe bureau LBVD, ter inzage gelegd bij de griffie. Het betreft een overzicht van de vier deelrapportages en een managementsamenvatting. Wij wijzen u erop dat dit technische onderzoeksinformatie betreft. De belangrijkste bevindingen en conclusies zijn samengevat zodat u in één oogopslag een beeld krijgt van de mogelijkheden tot verbetering op de diverse onderdelen.

Nadere toelichting op onderzoeksresultaten

Gelet op het technische karakter van dit onderzoek hebben wij met de onderzoekers van LBVD gesproken over een toelichting op de onderzoeksactiviteiten en de uitkomsten. Hiervoor is op 3 oktober een vertrouwelijke bijeenkomst georganiseerd.

Namens de rekenkamer gemeente Oss,

5.1.2e

gemeente Oss

Resultaten onderzoek informatieveiligheid

Algemeen

Persoonsgegevens en andere gevoelige informatie zijn bij de gemeente Oss grotendeels in goede/veilige handen. Er is veel goed geregeld. Dat neemt niet weg dat nog een aantal zaken beter of anders geregeld moet worden:

1. Het bleek mogelijk om door middel van 'ethisch' hacken oneigenlijk toegang te krijgen tot inloggegevens. Toegang werd verkregen door middel van twee accounts die gebruik maakten van zwakke wachtwoorden. Nadat men was binnengekomen in het systeem bleken de mogelijkheden om verder te infiltreren in de systemen beperkt. De onderzochte informatiesystemen van Gemeente Oss zijn goed beschermd tegen misbruik door zowel interne als externe kwaadwillenden.
2. Er komt een divers beeld naar voren als het gaat om het bewustzijn van informatieveiligheid binnen de organisatie. De mens blijkt de zwakke schakel te zijn:
 - men maakt gebruik van zwakke wachtwoorden ondanks de duidelijke aanwijzingen van de Chief Information Security Officer (CISO)
 - 14% van de medewerkers klikt op een phishing e-mail en 72% van degenen die hebben geklikt laten ook inloggegevens achter
 - mystery-guest konden zonder veel weerstand het pand en verschillende afdelingen betreden, de sociale controle nabij de kamers van B&W is hoog
 - de telefonische benadering heeft geen enkele poging geresulteerd in een gesprek waarbij (persoons)gegevens zijn bemachtigd of door de medewerker gewijzigd.
3. Er ontbreekt beleid, beleid kan worden aangescherpt of beleid wordt niet goed uitgevoerd omtrent:
 - verloren / gestolen toegangspassen
 - procedures met betrekking tot melden verdachte situaties en/of ongewone aanwezigheid
 - toepassen clean desk en clear screen

Resultaten deelonderzoeken

1. Telefonische mystery-guest

In algehele zin toonden de medewerkers van de gemeente Oss een hoge mate van bewustzijn en naleving van de regels voor informatiebeveiliging, wat resulteerde in een veilige en vertrouwelijke omgang met persoonsgegevens en verzoeken van bellers:

1. De medewerkers van de gemeente Oss stelden consistent adequate verificatievragen aan de MysteryGuests (MG's) gedurende alle gesprekken. Dit gold zowel aan het begin van elk gesprek als bij eventuele aanvragen van documenten;
2. Tijdens de gesprekken tussen de medewerkers en de MG's werden geen gevoelige (persoons)gegevens, zoals NAW-gegevens, namen of financiële informatie, onthuld of besproken. De medewerkers hielden zich aan de richtlijnen voor het beschermen van persoonsgegevens;
3. In alle gesprekken werd correct omgegaan met verzoeken om adreswijzigingen. Adreswijzigingen werden niet doorgevoerd zonder adequate verificatie en er werden geen documenten verstuurd naar nieuw doorgegeven adressen zonder eerst de juiste procedures te volgen.

2. Fysieke mystery-guest

Uit het onderzoek is gebleken dat het onderzochte doelobject van gemeente Oss matig beschermd is tegen misbruik door kwaadwillenden:

- Naleving van protocollen: Er is een gebrek aan strikte naleving van het clean-desk en clear-screen protocol, wat leidt tot potentiële informatielekken. Een gebrek aan (tijdig) uitvoeren van het blokkeren van een verloren/gestolen pas kan ertoe leiden dat er (langdurig) misbruik gemaakt kan worden van de verkregen toegang;
- Reactie op ongewone aanwezigheid: De MG's konden gemakkelijk de dekmantel van brandveiligheidsinspecteurs gebruiken om toegang te krijgen en werden zelden uitgedaagd of gecontroleerd door het personeel. Hoewel de MG's uiteindelijk werden gestopt, toont het incident aan dat de reactie op ongewone aanwezigheden verbeterd kan worden;
- Fysieke beveiliging: De toegangscontrole en interne zonering binnen het gebouw zijn onvoldoende om onbevoegde toegang te voorkomen;
- Toegangspassen en sleutels: Het gemak waarmee de MG's toegangspassen en sleutels konden verkrijgen, wijst op een risico in de beveiliging van deze persoonlijke c.q. essentiële items;

Positieve bevindingen:

- Transparantie en zichtbaarheid: De open en transparante inrichting van de kantoorruimtes werkte als een afschrikmiddel voor het plaatsen van keyloggers of het onopgemerkt doorzoeken van documenten;
- Eindcontrole en ontmaskering: De uiteindelijke ontmaskering van de MG's door enkele medewerkers toont aan dat er een zekere mate van alertheid en beveiligingsbewustzijn aanwezig is, maar dat deze niet consistent wordt toegepast bij alle medewerkers.

3. Phishing simulatie

Uit deze simulatie is gebleken dat de medewerkers nog gematigd op de hoogte zijn van de herkenningpunten van phishing e-mails. Voor een organisatie van deze omvang is 14.18% een hoog klikpercentage. Van de medewerkers die op de link hebben geklikt, heeft ook 72.15% zijn/haar inloggegevens ingevuld. Uit deze cijfers wordt een direct risico gezien voor gemeente Oss.

4. Penetratietest

Uit het onderzoek is gebleken dat de onderzochte informatiesystemen van Gemeente Oss goed beschermd zijn tegen misbruik door zowel interne als externe kwaadwillenden. De geïmplementeerde beveiligingsmaatregelen beschermen de Gemeente Oss goed tegen misbruik voor kwaadwillende met fysieke toegang tot een netwerkaansluiting. Het is voor een kwaadwillende zeer lastig om toegang te krijgen tot het netwerk zonder dat dit wordt opgemerkt en maatregelen direct actief zijn om misbruik te beperken of zelfs voorkomen.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 4