Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 058 233 88 33

Telefax 058 215 39 49
E-mail gemeente@leeuwarden.nl

Gemeente Leeuwarden **Rekenkamer**

Aan de Raad van de gemeente Leeuwarden

Onderwerp	Informatiebeveiliging van de gemeente Leeuwarden
Uw kenmerk	
Ons kenmerk	
Sector	
Team	
Doorkiesnummer	(058) 233 4022 J.E. Rijpma
Bijlagen	
Datum	15-11-2016

Geachte gemeenteraad,

Het onderwerp van deze rekenkamerbrief is de informatiebeveiliging van de gemeente Leeuwarden. Het belang van dit onderwerp lijkt ons evident. Overheden automatiseren en digitaliseren in hoog tempo met als gevolg dat de betrouwbaarheid, beschikbaarheid en vertrouwelijkheid van gegevens voortdurend aandacht vragen[1]. Zeker gelet op de steeds uitbreidende taken van de lokale overheid - denk aan de drie grote decentralisaties – dient de informatiehuishouding hoog op de bestuurlijke en ambtelijke agenda te staan. Recente incidenten op dit gebied bij andere gemeenten bewijzen regelmatig hoe kwetsbaar gemeentelijke overheden op dit punt kunnen zijn. Zeer recent werden bijvoorbeeld de gemeenten Ede, Amersfoort en Almelo[2] slachtoffer van een zeer omvangrijke hack waarbij zo goed als zeker persoonsgegevens zijn gestolen.

In het afgelopen jaar heeft de Rekenkamer onderzoek gedaan naar de veiligheid van informatie in de gemeente Leeuwarden. Daartoe heeft de Rekenkamer een op dit gebied gespecialiseerd bureau[3] ingehuurd. In opdracht van de Rekenkamer heeft dit bureau een aantal werkzaamheden uitgevoerd en daarover gerapporteerd. Gelet op de aard van het onderwerp en het technische karakter van de uitgevoerde testen heeft de Rekenkamer er voor gekozen om de belangrijkste bevindingen en de daarop gebaseerde aanbevelingen niet als een onderzoeks*rapport* maar in de vorm van een rekenkamer*brief* aan te bieden.

[1] Duurzaam toegankelijke informatie Special (2016) Themanummer van *BinnenlandsBestuur* juni 2016
[2] Ede: http://www.gelderlander.nl/regio/de-vallei/ede/mogelijk-3-700-gedupeerden-door-hack-website-gemeente-ede-1.6254903,
Amersfoort: https://www.security.nl/posting/474710/Amersfoort+verzweeg+datalek+voor+Autoriteit+Persoonsgegevens,
Almelo: http://www.ad.nl/binnenland/enorme-hack-bij-gemeente-almelo-waarschijnlijk-persoonsgegevens~a5496f8c/
[3] Het veldwerk voor het onderzoek is uitgevoerd door dhr. Antoon Wuijster verbonden aan *Sincerus, informatiebeveiliging door professionals* te Zwolle.

1 Vraagstelling en onderzoeksonderwerp

Centraal in het onderzoek staat de vraag hoe veilig de informatiehuishouding – en daarmee de informatie – van de gemeente Leeuwarden is. Om deze vraag te kunnen beantwoorden is een aantal activiteiten ondernomen, te weten:

- Een beoordeling van het geldende beleid
- Een zogenoemde externe penetratietest
- Een zogenoemde interne penetratietest
- Een fysieke beveiligingstest

1.1 Beoordeling van het beleid

Hieronder verstaat de rekenkamer het geschreven en vastgestelde beleid van de gemeente Leeuwarden. Daartoe is een veelheid aan documenten opgevraagd en bestudeerd. Een belangrijke plaats neemt daarin de nota "*gesloten openheid 2012-2015"*, door het college van burgemeester en wethouders vastgesteld op 27 november 2012 en geactualiseerd (2015-2016) op 7 januari 2014. In deze nota wordt het richtinggevende beleid voor het management ten behoeve van informatiebeveiliging geformuleerd. Voor de overige geraadpleegde documenten verwijzen wij naar bijlage 1.

Bij de beleidsbeoordeling zal worden stil gestaan bij een aantal specifieke onderwerpen, zoals de actualiteit van beleid, toekomstbestendigheid, organisatorische randvoorwaarden, autorisatiebeleid en -beheer, risicomanagement en incidentafhandeling. Deze onderwerpen zullen worden beoordeeld vanuit de Baseline Informatiebeveiliging Gemeenten (BIG)[4]. De gemeente Leeuwarden heeft deze richtlijn als het gemeentelijke basisnormenkader voor informatieveiligheid overgenomen[5]. De beoordelingsnormen zijn dan ook [voornamelijk] afkomstig uit de BIG.

1.2 Externe penetratietest

Een penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt worden om in deze systemen in te breken. Een penetratietest vindt normaal gesproken om rechtmatige redenen plaats, met toestemming van de eigenaars van de systemen die getest worden, met als doel de systemen beter te beveiligen.

Met *externe* penetratietesten wordt nagegaan of de informatiehuishouding kwetsbaar is vanuit een externe omgeving. Met name is hierbij te denken aan ongeautoriseerde toegang tot het netwerk van de gemeente. Deze kwetsbaarheden kunnen ontstaan door fouten in hard- en software, door verkeerde implementaties en door standaardinstellingen van systemen. Bekende risico's zijn phishingmails[6], ransomware[7] en het hacken van e-mail

[4] De BIG is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD), in samenwerking met de Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). Hierbij is de Baseline Informatiebeveiliging Rijksdienst (BIR), een variant van de ISO 27001-norm, als basis genomen en is een vertaalslag gemaakt naar een richtlijn voor de gemeentelijke markt. De BIG bestaat uit drie onderdelen: een strategische en een tactische baseline voor verschillende afdelingen/functies binnen een gemeente en een groep operationele producten. Meer informatie is te vinden op www.ibdgemeenten.nl.

[5] Motie ChristenUnie 26-3-2014

[6] Hartholt, S. (2016) "Phishing ellende; kleine gemeenten digitaal veiliger" in: *Binnenlands Bestuur* 3 juni 2016, p. 4 (hoofdredactioneel).

[7] Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de gegevens weer leesbaar te maken.

van bestuurders en ambtenaren[8]. Voor de externe toegang tot het netwerk van de gemeente zijn met name het hardening-beleid[9], het patchbeleid[10] en de wijze waarop incidentmelding en incidentafhandeling zijn georganiseerd van belang.

1.3 Interne penetratietest

Met een *interne* penetratietest wordt nagegaan of personen die binnen het netwerk opereren toegang kunnen verkrijgen tot informatie waarvoor zij niet geautoriseerd zijn. Er is een aantal interne penetratietesten uitgevoerd om na te gaan of in de bestaande infrastructuur maatregelen zijn genomen om informatiestromen te scheiden.

Duidelijk mag zijn dat een gevonden interne kwetsbaarheid ernstiger wordt als ook externe kwetsbaarheden zijn aangetroffen. Voor zowel de externe als de interne penetratietesten heeft de rekenkamer vooraf toestemming gevraagd en verkregen. Van beide penetratietesten zijn separate rapportages gemaakt die de rekenkamer tegelijk met het ambtelijk wederhoor beschikbaar heeft gesteld aan de ambtelijke organisatie.

1.4 Fysieke beveiligingstest

De twee penetratietesten zijn technische instrumenten om de informatiehuishouding in beeld te krijgen. Bij de fysieke beveiliging gaat het om de meest kwetsbare schakel in het beveiligingsproces, te weten de mens. Nagegaan is of gemeentelijke informatie fysiek benaderbaar is. Hierbij is gebruik gemaakt van een mystery guest die een tweetal locaties van de gemeente Leeuwarden (Stadskantoor en Stadhuis) heeft bezocht. Een mystery guestbezoek geeft een goede indruk van het toegangsbeleid, het bewustzijn van personeel met betrekking tot informatieveiligheid en de mate van invoering van cleandesk- en clearscreenbeleid.

In de volgende paragraaf geven wij de voornaamste bevindingen van de vier verrichte onderzoeksactiviteiten. Enerzijds beschrijven wij de door ons aangetroffen situatie (empirische bevindingen), anderzijds geven wij daarover een eerste oordeel (normatieve bevindingen). Een overall oordeel is aan te treffen in paragraaf 3 waarin wij onze belangrijkste bevindingen samenvatten en aanbevelingen formuleren.

2 Bevindingen

De beoordeling van het gemeentelijk informatiebeveiligingsbeleid vindt voornamelijk plaats aan de hand van normen die te destilleren zijn uit de BIG (zie paragraaf 1.1).

---

[8] Hartholt, S. (2016) "Genant slechte beveiliging e-mail; drie van de vijftig gemeenten voldoen aan verplichte standaarden" in: *BinnenlandsBestuur* 3 juni 2016, pp. 16-18.

[9] Hardening-beleid is het beleid voor het aanbrengen van beschermingsmaatregelen die het systeem versterken en het wegnemen van onnodige, overbodige systeemfuncties en systeemprocessen.

[10] Patchbeleid is het beleid voor het aanbrengen van reparatiesoftware om kwetsbaarheden in programmatuur te herstellen.

2.1 Beleidskader

De BIG schrijft voor dat er een informatiebeveiligingsbeleid dient te zijn dat door het College is vastgesteld. In dit beleidskader dient aandacht te zijn voor risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

Empirische bevindingen: De gemeente Leeuwarden heeft een informatiebeveiligingsbeleid (zie 1.1). Daarin is aandacht voor achtergronden, uitgangspunten, status, opbouw en kwaliteitsnormen van informatiebeveiliging; voorts voor nieuwe ontwikkelingen, samenwerking, incidenten en uitzonderingen, en voor de benodigde financiële en personele middelen. Dit beleidskader is opgesteld voor de periode 2012-2015 en geactualiseerd tot 2016.

Normatieve bevindingen: Bij dit beleidskader plaatsen wij de volgende kanttekeningen:

1. Het beleidskader dient geactualiseerd te worden, te meer omdat het beleidsdocument gebaseerd is op een verouderd normenkader (namelijk de Code van Informatiebeveiliging); de BIG is niet expliciet in het geschreven beleid terug te vinden terwijl er wel conform gewerkt wordt. Sinds de vaststelling van het beleidskader hebben zich vele ingrijpende wijzigingen in wet- en regelgeving voorgedaan, zoals WBP[11], meldplicht datalekken en decentralisaties sociaal domein. Deze structurele veranderingen rechtvaardigen een aanpassing in beleid. In het beleidskader dient dan ook aandacht te zijn voor de wijze waarop op zulke ontwikkelingen ingespeeld wordt en hoe dat zijn weerslag krijgt in het officiële beleid. Juist aandacht voor de tijdelijkheid van beleid op dit snel wijzigende beleidsterrein, onderstreept de hoge prioriteit van dit beleidsterrein en de daarvoor noodzakelijke alertheid van managers.
2. In het beleidskader zijn de kritische bedrijfsprocessen niet beschreven of genoemd. Daardoor heeft het beleidskader een algemeen karakter en is niet aan de processen te relateren. Zo is bijvoorbeeld de afdeling die over de belastingen gaat verantwoordelijk voor de privacy van door hen gebruikte gegevens en daarmee ook voor een adequate risicoanalyse.

2.2 Cleandesk- en clearscreen beleid

De BIG schrijft een cleandeskbeleid voor waarin wordt bepaald dat de medewerkers geen vertrouwelijke informatie op hun werkplek mogen laten liggen. Deze informatie moet altijd in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer) worden opgeborgen.

Empirische bevinding: De gemeente Leeuwarden heeft een cleandeskbeleid, alsmede een clearscreenbeleid vastgesteld. Dit beleid is actueel en herleidbaar op de BIG. Geconstateerd is dat dit beleid niet altijd wordt nageleefd. Met name het verslag van de mystery guest geeft aan dat vrij gemakkelijk informatie kan worden verkregen van (langdurig) onbeheerde bureaus, van openstaande beeldschermen terwijl de betreffende medewerker

[11] Wet Bescherming Persoonsgegevens

was vertrokken en van ruimtes die vrij toegankelijk waren als men zich toegang had verschaft tot gemeentelijk gebouwen.

Normatieve bevinding: Het cleandesk- en clearscreenbeleid heeft tot doel om zorgvuldig en vertrouwelijk met informatie op de werkvloer om te gaan. Het beleid en de implementatie daarvan geven aanleiding tot de volgende opmerkingen:

1. Voor het cleandesk- en clearscreenbeleid is als wettelijk kader de BRP[12] gekozen. Dat is op zichzelf juist, maar te beperkt. Er zijn meer randvoorwaarden die voor een cleandesk- en clearscreenbeleid van belang zijn zoals SUWI[13], DigiD, PUN[14] en BIG.
2. De naleving – en het toezicht daarop – van het cleandesk- en clearscreenbeleid vertoont gebreken, waardoor de organisatie zowel intern (onbevoegde collega's) als extern (niet geautoriseerde buitenstaanders) kwetsbaar is met betrekking tot gevoelige informatie over personen en/of zaken.

2.3 Technische netwerkbeveiligingsmaatregelen

Het netwerk van de gemeente moet beschermd worden tegen ongeautoriseerd binnendringen en misbruik van buitenaf. De hiervoor te nemen maatregelen worden aangeduid als het 'hardeningsbeleid'. Een belangrijk onderdeel daarvan is *zonering*, daarmee wordt bedoeld dat het netwerk zodanig wordt ingericht met zones en voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke.

Empirische bevindingen: Het gemeentelijk hardeningsbeleid is van 2013 en kent zonering. De daarvoor geldende randvoorwaarden en de aansluiting van zones op elkaar zijn beschreven. Uit de bij de Rekenkamer aangeleverde documentatie blijkt niet welke maatregelen zijn getroffen om de zones van elkaar te scheiden. Het hardeningsbeleid voor Linux-systemen[15] is actueel.

Normatieve bevindingen: Het hardeningsbeleid van de gemeente Leeuwarden geeft aanleiding tot de volgende kanttekeningen:

1. Het hardeningsbeleid is deels niet meer actueel (2013) en heeft een beperkte scope omdat er geen specifieke eisen zijn aangetroffen voor de beheersing van de veiligheid van specifieke systemen binnen een zone.
2. De uitgevoerde externe penetratietesten hebben een beperkt aantal kwetsbaarheden met de kwalificatie 'hoog' opgeleverd. Hieruit mag geconcludeerd worden dat de hardening van buitenaf voldoende effectief is.
3. De hardening/zonering van binnenuit is zorgelijker. Uit de interne penetratietesten is gebleken dat er door de gekozen inrichting (geen tot beperkte zonering en hardening) op het interne netwerk,

---

[12] Basis Registratie Personen

[13] Structuur Uitvoeringsorganisatie Werk en Inkomen

[14] Paspoort Uitvoeringsregeling Nederland

[15] Linux is een besturingssysteem voor computers en is vrij beschikbaar voor iedereen en iedereen mag het uitbreiden - met als enige echte verplichting om - als men de software doorgeeft of verkoopt - de verbeteringen weer met iedereen te delen. Dit noemt men open-source software.

kwetsbaarheden zijn die mogelijk misbruikt kunnen worden. Dit creëert een groot aanvalsvlak bij mogelijk misbruik van binnenuit.

2.4 Organisatorische randvoorwaarden

Een goede organisatorische beschrijving van taken en verantwoordelijkheden is van groot belang voor de organisatie rondom functioneren en beheer van informatiesystemen. In ieder geval dienen de rollen van de CISO (Chief Information Security Officer) en het lijnmanagement te zijn beschreven. Zo dient de CISO rechtstreeks aan de gemeentesecretaris te rapporteren en dient in de taakomschrijving van de CISO te zijn opgenomen dat hij gevraagd en ongevraagd adviseert over de informatiebeveiliging. Hiertoe kan ook worden gerekend zijn onafhankelijke advisering over de door het lijnmanagement opgestelde plannen – en de uitvoering daarvan – m.b.t. informatiebeveiliging; kortom de planning&control van informatiebeveiliging.

Empirische bevindingen: De huidige rollen en functies binnen het werkveld van informatieveiligheid zijn beschreven. De verantwoordelijkheden overlappen elkaar deels waardoor het niet altijd duidelijk is wie bij een calamiteit waar voor verantwoordelijk is. De rollen en verantwoordelijkheden zijn tevens niet volledig conform de BIG richtlijnen beschreven.

Normatieve bevindingen: De beschreven organisatorische voorzieningen geven aanleiding tot de volgende opmerkingen:

1. Door de recente (2015) ontwikkeling in de ambtelijke organisatie zijn de beschreven functies, taken, verantwoordelijkheden en bevoegdheden niet meer actueel en voldoen niet aan de BIG richtlijn.
2. Uit aangeleverde documentatie[16] valt af te leiden dat in het verleden onderzoek is gedaan naar het bewustzijn van het lijnmanagement voor informatiebeveiliging. Hieraan heeft de Rekenkamer de indruk overgehouden dat vanuit het lijnmanagement meer initiatieven met betrekking tot de informatiebeveiliging van het primaire bedrijfsproces hadden mogen worden verwacht. Deze indruk wordt bevestigd door de bevindingen van de mystery guest.
3. Aanbevelingen en verbeterpunten van de CISO zijn niet gevolgd door vanuit het lijnmanagement opgestelde risicoanalyses en/of vastlegging van geaccepteerde risico's.
4. Rollen, verantwoordelijkheden en bevoegdheden van de CIO, de CISO, de adviseur Informatiebeveiliging en het lijnmanagement, hun positionering ten opzichte van elkaar en hun (on)afhankelijkheid ten opzichte van de organisatie zijn in onvoldoende mate duidelijk. Ook de verantwoordelijkheden van het lijnmanagement voor het informatiebeveiligingsbeleid zijn onvoldoende benadrukt.

2.5 Autorisatiebeleid en -beheer

In het autorisatiebeleid en –beheer gaat het om de vraag wie en onder welke voorwaarden toegang heeft tot de gebouwen, systemen en informatie. De WBP

[16] [9] 2015-347-cr-onderzoek-windows-accounts.pdf Bron: Gemeente Leeuwarden, [10] Opdrachtbrief Digid audit insite (pentest Sigmax en Exxellence).doc Bron: Gemeente Leeuwarden, [11] Adviesrapport Herinrichting O&I, versie extern.pdf Bron: Gemeente Leeuwarden, [14] volwassenheidsmeting 2014 STRICT.pdf Bron: Gemeente Leeuwarden, [24] Access Governance - v9.pdf Bron: Gemeente Leeuwarden, [25] IAM SRC module.doc Bron: Gemeente Leeuwarden

bepaalt dat passende technische en organisatorische maatregelen getroffen moeten worden om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Ongeautoriseerde toegang dient als datalek behandeld te worden.

Empirische bevinding: Het autorisatiemodel is beschreven in de documenten "access governance" en in "IAM SRC module". De hierin beschreven autorisaties zijn rolgebaseerd. Er zijn autorisaties voor GBA-v[17]. en BRP[18] Uit de aangeleverde documenten blijkt dat die periodiek worden gecontroleerd. Het aantal beheerdersaccounts is groot en het streven is om dat aantal terug te brengen. De autorisatierechten zijn opgeslagen in een centraal te beheren database (active directory).

Normatieve bevinding: Het autorisatiebeleid en –beheer geven aanleiding tot de volgende opmerkingen:

1. Het autorisatieproces is voor een aantal specifieke ICT-systemen uitgewerkt. Maar een overkoepelend gemeentelijk toegangsbeleid gebaseerd op een vertrouwensmodel met eenduidige inrichtingsprincipes ontbreekt. Met name voor de uitbreiding van de ICT-dienstverlening naar andere (keten)partners is zo'n overkoepelend beleid raadzaam.
2. De realisering van dit voornemen om het aantal beheerderaccounts terug te brengen is verstandig. Dit voornemen is echter niet terug te vinden in documentatie. Voorts wijst de Rekenkamer op de kwetsbaarheid van de enkelvoudige active directory (AD), ook in relatie met andere partners. Enerzijds omdat geen toegang tot de AD tot onbeschikbaarheid van alle systemen leidt; anderzijds omdat een hack van deze bron toegang geeft tot alle systemen die van deze dienst gebruik maken.

2.6 Risicomanagement en incidentafhandeling

Bij risicomanagement en incidentafhandeling gaat het respectievelijk om preventieve en repressieve aandacht voor informatiebeveiliging. De BIG schrijft voor dat er regelmatig aandacht is voor de beveiliging van informatie, met name als het gaat om persoonsgegevens. Voor de incidentafhandeling is van belang dat er procedures zijn voor het rapporteren van beveiligingsgebeurtenissen en voor reactie op en escalatie na een beveiligingsincident.

Empirische bevindingen: de gemeente Leeuwarden voert regelmatig risicoanalyses uit. Deze analyses vinden niet plaats op basis van de door de IBD[19] aangereikte methode. De incidentafhandeling is beschreven in de "procedure beveiligingsincidenten 2015". In het document "volwassenheidsmeting 2014" staan inrichtingsadviezen voor incidentafhandelingen. Er is structurele aandacht voor de afhandeling van beveiligingsincidenten.

[17] GBA-V: Gemeente Basisadministratie Verstrekkingen, centrale landelijke component in de basisadministratie
[18] BRP: Basisregistratie Personen, rijksoverheidsregistratie van persoonsgegevens
[19] Informatiebeveiligingsdienst voor gemeenten

Normatieve bevindingen: het risicomanagement en het incidentafhandelingsproces geven aanleiding tot de volgende opmerkingen:

1. Hoewel het uitvoeren van de op de BIG Baseline gebaseerde toets niet is voorgeschreven, is dat wel verstandig. Deze tactische baseline is namelijk zo gekozen dat als een gemeente daaraan voldoet, het niet nodig is om aanvullende diepergaande risico-analyses uit te voeren.
2. Zeker met betrekking tot de uitbreiding van de ICT-dienstverlening aan de (keten)partners – en de daarmee gepaard gaande bewerkersovereenkomsten – is zo'n gemodelleerde risicoanalyse aan te bevelen, mede omdat geconstateerd is dat de bewerkersovereenkomsten met ketenpartners onvolledig zijn[20]. Hierdoor heeft de gemeente niet goed zicht op welke risico's er bij de ketenpartners zijn. In dit verband wijzen wij er op dat de gemeente als bevoegd gezag verantwoordelijk is voor deze risico's en de gevolgen daarvan.
3. Het incidentenafhandelingsproces is op zichzelf adequaat. Opvallend is dat in de documentatie daarover geen verband is gelegd met het overkoepelende informatieveiligheidsbeleid.
4. De incidentafhandeling kent gradaties. Onduidelijk is wanneer het verantwoordelijk management of B&W op de hoogte moet worden gebracht van een incident.

2.7 De externe penetratietest

Op 1 maart 2016 heeft de Rekenkamer een externe penetratietest laten uitvoeren. Bij een penetratietest wordt vanaf het internet een doelsysteem onderzocht op kwetsbaarheden. Gevonden kwetsbaarheden worden geanalyseerd en geclassificeerd. In beginsel zijn er vijf classificaties mogelijk (kritiek, hoog, midden, laag, geen). Een classificatie wordt bepaald door de ernst van de kwetsbaarheid in combinatie met de kans dat die kwetsbaarheid zich voordoet. Dus een ernstige kwetsbaarheid met een grote kans van optreden krijgt de classificatie 'kritisch'.

Bij de penetratietesten voor de gemeente Leeuwarden zijn geen bevindingen met de classificatie 'kritisch' aangetroffen. Wel zijn twee kwetsbaarheden met de classificatie 'hoog'[21], zeven met de classificatie 'midden', en vijf met de classificatie 'laag' gevonden. Over alle kwetsbaarheden is separaat en vertrouwelijk gerapporteerd aan de ambtelijke organisatie[22]. Over de twee kwetsbaarheden met de classificatie 'hoog' het volgende. Eén daarvan had betrekking op verouderde versleutelingsmechanismes. In de test is niet vastgesteld dat er op dat moment persoonsgegevens over het koppelvlak werden uitgewisseld. De tweede hoge kwetsbaarheid had betrekking op het gebruik van standaardwachtwoorden van en op beelden van beveiligingscamera's. De apparatuur is aangesloten op de infrastructuur van de gemeente Leeuwarden, het eigendom en beheer van deze camera's ligt niet bij de gemeente.

2.8 De interne penetratietest

[20] Wij verwijzen in dit verband naar de artikelen 1, 2, 4, 5, 6, 6.2, 6.3, 6.4, 7.2-7.7, 8, 9 10.1, 11, 12, bijlage 1, 2 en 3

[21] De gevonden kwetsbaarheden met de classificatie 'hoog' zijn na de bevinding gemeld aan de CISO

[22] Rapportage penetratietest Leeuwarden v1 0(004); tegelijkertijd met ambtelijk wederhoor beschikbaar gesteld aan de ambtelijke organisatie

Naast de externe penetratietest zijn er ook interne kwetsbaarhedenscans uitgevoerd. Voor een goed begrip van de resultaten dient men zich hierbij twee dingen vooraf goed te realiseren. In de eerste plaats dat de externe Firewalls reeds zijn gepasseerd en in de tweede plaats levert een interne penetratietest altijd kwetsbaarheden op.

De interne test[23] heeft een groot aantal kwetsbaarheden blootgelegd. De gevonden kwetsbaarheden bij de gemeente Leeuwarden zijn qua aantal en aard vergelijkbaar met die in vergelijkbare organisaties. Daarnaast waren kwetsbaarheden terug te voeren op verouderde versies waarvoor nieuwe updates (patches) beschikbaar zijn. Hieruit is af te leiden dat patches voor interne systemen niet automatisch of snel genoeg uitgerold worden.

2.9 De mystery guest

Een mystery guest heeft op 26 april 2016 het stadskantoor en het stadhuis bezocht. In beide gevallen heeft de mystery guest gezegd dat hij op een collega wachtte. Door de situatie kort (minder dan 5 minuten) te observeren was het mogelijk binnen te komen door een (goederen)lift of door mee te lopen met een personeelslid door de personeelsingang. Eenmaal binnen vertelde de mystery guest dat hij een inventarisatie ten behoeve van een aanstaande verbouwing aan het voorbereiden was.

Aangetoond is dat fysieke toegang gemakkelijk is en dat het eenvoudig is (ICT)apparatuur te plaatsen en te koppelen aan het netwerk of mee te nemen zonder dat dit opgemerkt wordt. De mystery guest had toegang tot postvakken en kon documenten meenemen naar een onbemande ruimte waar hij ze ongestoord kon fotograferen of bestuderen. In vergaderruimtes trof de mystery guest flipovers met aantekeningen aan. Hoewel de mystery guest dat niet heeft gedaan, acht hij het zeer waarschijnlijk dat hij documenten ongezien buiten de gebouwen kon brengen. De mystery guest kon zich vrij door de gebouwen verplaatsen en had toegang tot werkplekken; het viel de mystery guest op dat de ICT-testruimte als zodanig werd aangegeven. Hij werd niet herkend als ‘bezoeker’.

3 Conclusies en aanbevelingen

Het onderzoek van de Rekenkamer was er op gericht om een beeld te verkrijgen van de beveiliging van informatie en gegevens binnen de gemeente Leeuwarden. Daartoe zijn een beleidsreview, een externe en interne penetratietest uitgevoerd, alsmede een mystery guest bezoek aan gemeentelijke gebouwen gebracht. In het algemeen kan gesteld worden dat op het moment dat de reviews plaatsvonden er geen ernstige datalekken of persoonsgegevens onbeheerd zijn aangetroffen. Bij deze relatief geruststellende bevinding passen twee relativeringen. Op de eerste plaats zijn de reviews momentopnames geweest. In de snel veranderende wereld van de ict is constante alertheid voor de veiligheid van opgeslagen informatie een voorwaarde; een relatief veilige omgeving kan in korte tijd omslaan in een extern doordringbare – en dus onveilige en kwetsbare – configuratie. In de tweede plaats is een 100% veilige informatiehuishouding in een moderne organisatie een illusie. Altijd zal er een balans gevonden moeten worden

[23] Nessus Analyse r.l.v0.1 (vertrouwelijk)); tegelijkertijd met ambtelijk wederhoor beschikbaar gesteld aan de ambtelijke organisatie

tussen technische en sociale maatregelen om de bedrijfsgegevens en -processen te beschermen enerzijds en de interne en externe efficiëntie van werken anderzijds.

Naast deze hoofdconclusie stellen wij het volgende vast:

1. De gemeente Leeuwarden heeft vastgesteld beleid m.b.t. informatiebeveiliging, maar de geanalyseerde (beleids)documenten zijn deels verouderd en onvoldoende aan elkaar gerelateerd;
2. De nieuwe BIG richtlijnen worden in de praktijk toegepast echter de benodigde functiescheiding van de CISO is niet conform deze richtlijn waardoor er bij calamiteiten en incidenten onduidelijkheid in de verantwoordelijkheden en sturing kan ontstaan.
3. In de afgelopen jaren is veel energie gestoken om de ict-infrastructuur af te schermen voor binnendringing vanaf het internet, maar van binnenuit blijkt deze infrastructuur kwetsbaar;
4. De ICT-omgeving van Leeuwarden is de afgelopen jaren enorm gegroeid en is mede dienstbaar (service provider) ten behoeve van andere partners. Dit stelt extra eisen vanuit beveiligingsperspectief. Met name de beheerderaccounts zijn door de inrichting van de ICT-infrastructuur een aantrekkelijk aanvalsvlak;
5. Op apparatuur van derden dat is aangesloten op de infrastructuur van de gemeente Leeuwarden is het gebruik van standaardwachtwoorden aangetroffen;
6. De bewerkersovereenkomsten met de ketenpartners (Amaryllis) zijn onvolledig waarbij het onduidelijk is hoe de informatiebeveiliging bij en voor de partners is geborgd. De gemeente loopt hier als bevoegd gezag risico's;
7. Bewerkersovereenkomsten met de op de ICT-dienstverlening aangesloten gemeenten zijn niet aangetroffen. Daarmee ontbreekt de formele basis voor de toegang tot gegevens van burgers van de aangesloten gemeenten en de bijbehorende autorisaties van medewerkers van de gemeente Leeuwarden;
8. Er worden regelmatig risicoanalyses uitgevoerd. Uit de aangeleverde informatie is gebleken dat deze risicoanalyses volgens een vastgestelde methode worden uitgevoerd. Voorts ligt de verantwoordelijkheid voor het uitvoeren van deze risicoanalyses in hoofdzaak bij de ICT-dienstverlening, en in minder mate bij het lijnmanagement waardoor hun verantwoordelijkheid in dezen onvoldoende uit de verf komt;
9. De gemeentelijke gebouwen zijn vrij gemakkelijk binnen te treden door onbevoegden. Ondanks fysiek toezicht, paslezers, dichtvallende deuren kunnen onbevoegden zich toegang verschaffen tot ruimtes waar vertrouwelijke informatie kan zijn opgeslagen.
10. Er is een cleandesk- en een clearscreen beleid, maar in de praktijk wordt dat onvoldoende toegepast.

Gelet op onze hoofdbevinding en deelconclusies komen wij tot de volgende aanbevelingen:

1. Op korte termijn dient er een nieuw (beleids)programma voor het informatieveiligheidsbeleid opgesteld te worden voor de periode 2016-2020. Dit beleid en de uitvoering dienen gebaseerd te zijn op de

strategische baseline van de IBD. Daarbij dient aandacht te zijn voor de rollen, verantwoordelijkheden en bevoegdheden van de CIO, de CISO, de adviseur informatiebeveiliging en het lijnmanagement;
2. Benadruk daarin het integrale karakter van het veiligheidsbeleid en de verantwoordelijkheden van het (hoogste) management bij de totstandkoming en feitelijke implementatie daarvan. Informatieveiligheidsbeleid is niet alleen het toepassen van wettelijke kaders, maar betreft het gehele bedrijfsproces, dus het geheel aan risico's, maatregelen, bewustzijn van management en medewerkers en organisatorische voorwaarden. ICT heeft daarbij een initiërende, ondersteunende en een controlrol;
3. Richt de ICT-infrastructuur zodanig in dat de organisaties (zoals de diverse gemeenten) die ICT-dienstverlening bij het SSL Leeuwarden afnemen meer hun eigen omgeving binnen deze infrastructuur hebben, zodat wordt voldaan aan de beveiligingseisen omtrent (privacy)informatie van deze organisaties. Leg dan expliciet vast welke diensten gezamenlijk dan wel separaat worden aangeboden c.q. gebruikt;
4. Partners die gebruik maken van de infrastructuur van de gemeente Leeuwarden en gebruik maken van standaardwachtwoorden, dienen daarop gewezen te worden;
5. Vernieuw de huidige bewerkersovereenkomsten (zoals met Amaryllis) en pas ze conform de IBD-richtlijnen aan, zodat de gemeente als bevoegd gezag haar controlerende rol richting haar ketenpartners volledig vastlegt en navolgbaar uitvoert.
6. Sluit tevens bewerkersovereenkomsten af met die gemeenten die van de ICT-dienstverlening van het SSL Leeuwarden gebruik maken, waardoor autorisaties van medewerkers hiermee geformaliseerd worden. Maak tevens gebruik van rolgebaseerde autorisaties en leg tevens de afspraken over identificatie, authenticatie en autorisatie vast.
7. Herzie de huidige toelatingspraktijk m.b.t. gemeentelijke gebouwen en ontwikkel concrete acties om het veiligheidsbewustzijn van medewerkers en management te vergoten. Hierbij kan gebruik worden gemaakt van de ervaringen die uit ons mystery guest onderzoek naar voren komen. Met name de naleving van het cleandesk- en clearscreenbeleid dient geïntensiveerd te worden.

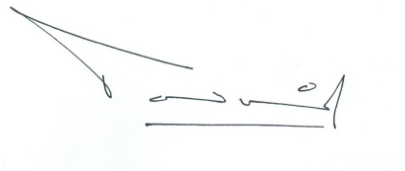
4 Advies

Omdat onze rapportage de vorm van een rekenkamerbrief heeft gekregen, hebben wij – anders dan gebruikelijk – onze bevindingen met conclusies en aanbevelingen aangeboden voor een ambtelijk wederhoor. Vervolgens is een bestuurlijke reactie van het College van B&W ingewonnen. Deze reactie is als bijlage bij deze brief gevoegd. Deze reactie geeft de Rekenkamer wel/niet aanleiding tot de volgende opmerkingen.

Wij adviseren de gemeenteraad om kennis te nemen van onze bevindingen en om middels besluitvorming onze aanbevelingen onder de aandacht van het College te brengen.

Hoogachtend,

Rekenkamer gemeente Leeuwarden,



dr. P.L. Polhuis, voorzitter

J.E. Rijpma-Veninga, secretaris