Volwassenheidsonderzoek informatiebeveiliging gemeente Overbetuwe

Rekenkamercommissie Overbetuwe 2021

Overbetuwe, 2 maart 2021

gemeente Overbetuwe

Voorwoord

Overheden beschikken over grote hoeveelheden vertrouwelijke en gevoelige informatie. Informatie die nodig is om een groot aantal taken goed te kunnen uitvoeren. Zo beschikt de gemeente Overbetuwe niet alleen over alle persoons-, woon- en verblijfsgegevens van haar inwoners, maar bijvoorbeeld ook informatie die te maken heeft met zorg- en ondersteuningsvragen, uitkeringen, overeenkomsten, in ontwikkeling zijnde (ruimtelijke, project- en beleids-)plannen of de persoonsgegevens van het ambtelijk personeel. Allemaal zaken waarvan het ongewenst is dat deze in handen komen van de verkeerde personen of organisaties.

Verschillende gemeenten, zoals Lochem, Bergen op Zoom, Ede, Zutphen en Hof van Twente werden het afgelopen jaar slachtoffer van hack-aanvallen. Heel recent was de hack-aanval op de Nederlandse Organisatie voor Wetenschappelijk onderzoek (NWO), maar het meest in het oog sprong toch wel de hack in december 2019 van de systemen van de Universiteit Maastricht, waardoor duizenden studenten werden gedupeerd en onderzoek enige tijd kwam stil te liggen. Een dergelijk scenario, waarbij wordt ingebroken in systemen en processen ernstig worden verstoord, is ook in Overbetuwe zeker niet ondenkbaar.

Vandaar dat de wetgever een normenkader voor de beveiliging van deze informatie heeft vastgesteld, de Baseline Informatiebeveiliging Overheid. Afgekort, de BIO. Na een overgangsjaar (2019) heeft dit normenkader met ingang van 1 januari 2020 het vorige normenkader, de Baseline Informatiebeveiliging Gemeenten (BIG), vervangen. Daarmee hanteren alle overheidsorganen één gezamenlijk normenkader. (Wettelijk) verplichte kost dus voor iedere overheidsorganisatie, maar hoe doet het Overbetuwe het (aantoonbaar) op dit gebied?

Eerst het goede nieuws. De gemeente Overbetuwe is er zich ervan bewust dat het noodzakelijk is om het beveiligingsbewustzijn te stimuleren. Daar begint iedere verandering mee, bewustzijn. Er is flink geïnvesteerd om ervoor te zorgen dat alle medewerkers beschikken over de juiste kennis, houding en gedrag ten aanzien van informatiebeveiliging.

Dat is mooi. Maar we hebben ook moeten vaststellen dat de gemeente Overbetuwe nog onvoldoende inzicht heeft in de mate waarin zij momenteel (aantoonbaar) voldoet aan de eisen van de BIO. Technische kwetsbaarheden worden nog onvoldoende inzichtelijk gemaakt en basisprocessen zijn niet aantoonbaar op orde. Waarmee wij niet anders kunnen concluderen dat aan het overgrote deel van de normen die de BIO hanteert aantoonbaar (nog) niet wordt voldaan. Er is dus nog veel te doen. Dat is in essentie de conclusie en daarmee ook de waarschuwing die uit ons onderzoek komt.

In ons rapport treft u een aantal concrete aanbevelingen welke door ons op zeer korte termijn zouden moeten worden opgepakt. En hoewel, of misschien zelfs juist, het onderwerp voor veel gemeenteraadsleden ver van hun dagelijks werk of van hun interesses staat zou u het college kunnen verzoeken u jaarlijks te rapporteren over de stand van zaken met betrekking tot de BIO. De organisatie is op dit punt kwetsbaar, de gegevens van uw inwoners en van het gemeentebestuur dus ook.

Wij hebben ook meegekeken naar uw vergadering op 28 oktober jl. Uw organisatie was op onderdelen verrassend transparant over een aantal beveiligingsvraagstukken, met name over een aantal kwetsbaarheden. Zo transparant dat wij ons afvroegen of u in het openbaar hierover niet wat terughoudender zou moeten zijn. Ook wij hebben op een belangrijk deel van de informatie waarop wij onze bevindingen, conclusies en aanbevelingen hebben gebaseerd geheimhouding opgelegd. Weliswaar is deze informatie voor u als leden van de gemeenteraad -onder geheimhouding- in te zien, uw rekenkamercommissie heeft niet de ambitie om kwaadwillenden op ideeën te brengen.

Omdat wij als commissie onvoldoende kennis in huis hadden om dit onderzoek zelf uit te voeren hebben wij voor dit specifieke onderwerp een extern onderzoeker ingeschakeld. In het rapport treft u zijn bevindingen aan over zaken die beter zouden kunnen en zouden moeten. Het geeft u als gemeenteraad, als lekenbestuur een goede inkijk in de wondere wereld van de informatietechnologie en de normen die worden gehanteerd. Maar net zo belangrijk als die inkijk, hopen en verwachten wij dat de organisatie met deze bevindingen zijn voordeel kan doen.

Wij wensen u veel leesplezier toe.

Volwassenheidsonderzoek informatiebeveiliging gemeente Overbetuwe

Datum	: 01 maart 2021
Opdrachtgever	: Rekenkamercommissie Overbetuwe
Auteur	: Mick Deben BSc. CISSP
Versie	: 2.0
Status	: Definitief
Pagina's	: 24
Classificatie	: **OPENBAAR**

Documentclassificatie

Dit document is geclassificeerd als **OPENBAAR**. Dit betekent dat het document vrij gepubliceerd en gedeeld mag worden zonder restricties.

DMC GROUP
SECURITY MANAGEMENT

Managementsamenvatting

In opdracht van de rekenkamercommissie heeft DMC Group onderzocht in hoeverre de gemeente Overbetuwe (verder 'Overbetuwe') aantoonbaar de eisen van de Baseline Informatiebeveiliging Overheid (BIO) heeft geïmplementeerd. De BIO is een normenkader op het gebied van informatiebeveiliging en is verplicht voor alle Nederlandse overheden. Informatiebeveiliging onderscheidt vier hoofd aandachtsgebieden: mensen, processen, techniek en fysieke veiligheid. Het op orde hebben van informatiebeveiliging is van essentieel belang om diensten en producten te kunnen (blijven) leveren aan burgers en bedrijven en het voorkomen en/of beperken van reputatie-, operationele- of financiële schade door bijvoorbeeld een boete van de privacy toezichthouder (Autoriteit Persoonsgegevens).

Mens

Overbetuwe heeft zicht op de beveiligingsrisico's die gepaard gaan met menselijk gedrag en heeft hier ook aantoonbaar in geïnvesteerd om dit in positieve zin te beïnvloeden. De verantwoordelijkheden, taken en bevoegdheden ten aanzien van informatiebeveiliging zijn nog niet volledig vertaald naar de dagelijkse praktijk waardoor het lijnmanagement in de praktijk nog in onvoldoende mate informatiebeveiligingsactiviteiten uitvoert, hierop stuurt of controleert.

Proces

Overbetuwe heeft in onvoldoende mate zicht op naleving van de eisen van de BIO en de effectiviteit en doeltreffendheid van reeds getroffen beveiligingsmaatregelen. Ook heeft zij beveiligingsrisico's nog onvoldoende in kaart gebracht en wordt hier nauwelijks op gestuurd. De doelstellingen zijn niet SMART geformuleerd en er wordt niet gerapporteerd over de mate waarin de doelstellingen worden bereikt. Voor een groot deel van de BIO ontbreekt het aan tactische en operationele regels en richtlijnen, waardoor informatiebeveiliging nog niet op eenduidige wijze aantoonbaar wordt toegepast.

Techniek

Overbetuwe heeft nog onvoldoende inzicht in de mate waarin ICT voldoet aan de beheersmaatregelen van de BIO en stuurt / monitort hier niet actief op. Daarnaast vinden er geen controles plaats om vast te stellen of processen correct worden uitgevoerd of dat beveiligingsrisico's adequaat beheerst worden. De CISO en ISO hebben inhoudelijk overleg met ICT, maar vanuit het (senior) management is hier nog te weinig aandacht voor. Monitoren op technische kwetsbaarheden kan verder worden verbeterd en basisprocessen zijn niet aantoonbaar op orde.

Fysieke beveiliging

Er is geen toegangsbeleid vastgesteld waaruit blijkt op welke wijze bedrijfsmiddelen beschermd (moeten) worden in gebouwen, specifieke zones of ruimten en welk gedrag daarbinnen (on)wenselijk is. De mate waarin beveiliging wordt toegepast binnen de gebouwen van de gemeente berust momenteel primair bij Buitenruimten en Vastgoed. Het is onduidelijk of alle aspecten van informatiebeveiliging hierbij in acht worden genomen.

Onderzoeksvragen

In dit onderzoek is de onderstaande onderzoeksvraag beantwoord:

In hoeverre heeft de gemeente Overbetuwe de BIO (aantoonbaar) geïmplementeerd?

Overbetuwe heeft geen overzicht van de mate waarin zij momenteel (aantoonbaar) voldoet aan de eisen van de BIO. De laatste gap-analyse stamt uit 2017 en was nog gericht op de BIG. Uit de geanalyseerde documentatie en gesprekken is gebleken dat er in zeer beperkte mate informatie beschikbaar is waaruit blijkt hoe zij informatiebeveiliging in de bedrijfsprocessen heeft geborgd. In bijlage D is, voor zover dat mogelijk was, op maatregel niveau toegelicht welke bevindingen er zijn. Geconcludeerd kan worden dat aan het merendeel van de BIO **niet** aantoonbaar wordt voldaan. Dit wil niet zeggen dat zaken ook niet geregeld zijn, maar wel dat dit in ieder geval nog onvoldoende kan worden aangetoond. Overbetuwe heeft software aangeschaft om controlewerkzaamheden en bewijslast ('evidence') in te registreren en te onderhouden, maar maakt hier tot op heden nog nauwelijks gebruik van.

Naast de hoofdvraag zijn er nog twee deelvragen opgesteld:

1. *Hoe realistisch zijn de BIO-eisen vergeleken met de bestaande infrastructuur van Overbetuwe?*
2. *Naast de technische beveiliging is de gebruiker cruciaal. Wat is het bewustzijn van de gebruiker als het gaat om informatiebeveiliging (met name nu vanwege de Corona-crisis waar veelal vanuit huis gewerkt wordt)?*

Deelvragen

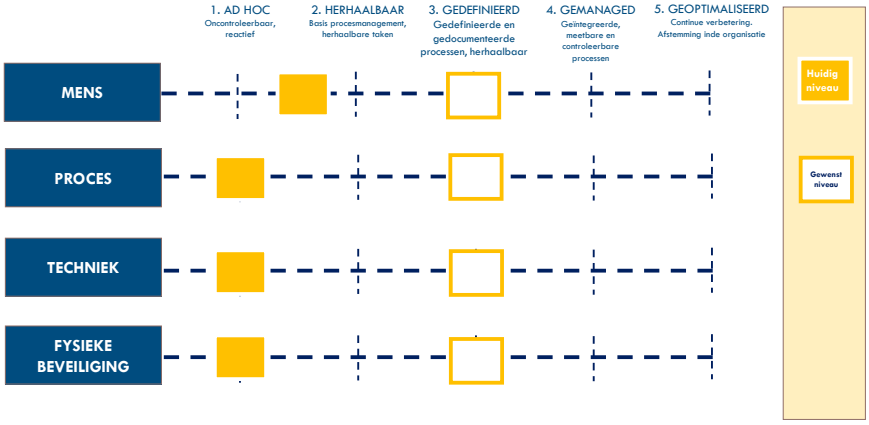
Ad 1. De 114 beheersmaatregelen van de BIO zijn verplicht voor alle Nederlandse overheden, dus ook voor Overbetuwe. Het feit dat zij haar ICT volledig heeft uitbesteed zorgt ervoor dat het zorgdragen voor het aantoonbaar voldoen aan de BIO primair bij de gemeente Lingewaard ligt. Ongeveer 60% van de BIO-beheersmaatregelen heeft direct betrekking op ICT. Dit is echter **niet** de verantwoordelijkheid van Lingewaard, maar van Overbetuwe ('je kunt alles uitbesteden, behalve je verantwoordelijkheid').

Ad 2. Het beveiligingsbewustzijn is over alle medewerkers gezien nog onder de maat. Dit blijkt uit verschillende onderzoeken en metingen die zij heeft gedaan, maar Overbetuwe heeft flink geïnvesteerd om dit te structureel te verbeteren. In 2021 zal gemeten worden of de investeringen de gewenste resultaten hebben behaald.

Conclusie

De gemeten volwassenheid van Overbetuwe is geplot op het volwassenheidsmodel voor informatiebeveiliging en weergeven in onderstaande figuur. Voor de aanbevelingen ter verdere verbetering wordt verwezen naar paragraaf 7.2.

Volwassenheidsmodel informatiebeveiliging gemeente Overbetuwe (status oktober 2020)



Noot: Omdat de fysieke (toegangs)beveiliging niet geobserveerd kon worden en er geen functionarissen zijn geïnterviewd die hier verantwoordelijk voor zijn, kan het daadwerkelijke volwassenheidsniveau hoger liggen. Aangezien er geen documentatie is aangeleverd is op dit moment het laagste volwassenheidsniveau (ad-hoc) toegekend. Het gewenste niveau is op volwassenheidsniveau drie (Gedefinieerd) geplaatst omdat dit het niveau is waar Overbetuwe minimaal zou moeten willen staan. Als dit niveau behaald is verricht zij structureel diverse activiteiten waardoor opzet, bestaan en effectieve werking van beheersmaatregelen aantoonbaar gemaakt kunnen worden en worden beveiligingsrisico's adequaat beheerst. De BIO zorgt ervoor dat de gemeente haar processen met betrekking tot informatiebeveiliging heeft gedocumenteerd, structureel uitvoert en aantoonbaar maakt.

DMC GROUP
SECURITY MANAGEMENT

Inhoudsopgave

1. Inleiding

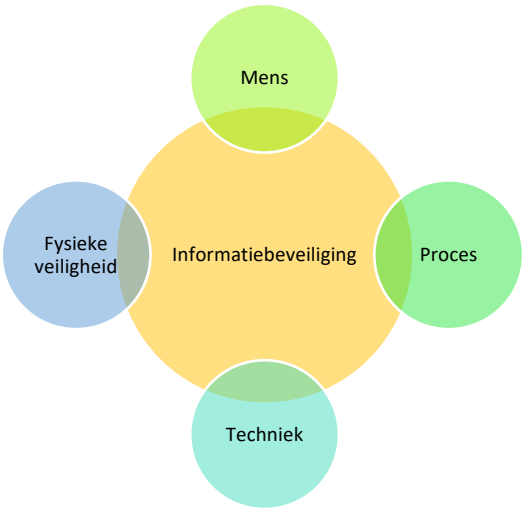
Dit rapport bevat de bevindingen van het volwassenheidsonderzoek met betrekking tot Informatiebeveiliging van de gemeente Overbetuwe (verder Overbetuwe). Met volwassenheid wordt hier bedoeld ten opzichte van het vigerend normenkader voor alle Nederlandse overheden, de Baseline Informatiebeveiliging Overheid (BIO). Het onderzoek is uitgevoerd in opdracht van de rekenkamercommissie Overbetuwe en heeft plaatsgevonden in de periode september-oktober 2020.

1.1 Achtergrond

De rekenkamercommissie is een orgaan dat onafhankelijk onderzoeken verricht in afstemming met de gemeenteraad. Informatieveiligheid ('informatiebeveiliging' wordt ook wel 'cybersecurity' genoemd) is een steeds belangrijkere randvoorwaarde voor gemeenten door de sterk toenemende digitalisering in de samenleving. De afhankelijkheid van informatie & communicatie technologie (ICT) en data wordt steeds groter. Goed huisvaderschap ten aanzien van informatiebeveiliging is noodzakelijk om de dagelijkse gang van zaken draaiende te kunnen houden en gegevens van burgers en bedrijven adequaat te beschermen. Het toenemende belang van informatiebeveiliging onder andere ook merkbaar aan de komst van nieuwe wet- en regelgeving voor privacy (Algemene Verordening Gegevensbescherming - AVG) en informatiebeveiliging (Baseline Informatiebeveiliging Overheid - BIO).

Informatiebeveiliging

Informatiebeveiliging focust op drie aspecten: beschikbaarheid, integriteit en vertrouwelijkheid. Dit betekent in de praktijk dat alleen geautoriseerde gebruikers toegang hebben tot juiste en volledige informatie waar en wanneer dit nodig is op basis van de vastgestelde betrouwbaarheidseisen. Informatiebeveiliging onderscheidt vier hoofd aandachtsgebieden: mensen, processen, techniek en fysieke veiligheid. Adequate informatiebeveiliging is opgebouwd uit een gelaagde beveiliging die uit verschillende soorten beheersmaatregelen bestaat. Een organisatie kan verschillende technische beheersmaatregelen implementeren om ongeautoriseerde toegang voorkomen, maar als de fysieke toegangsbeveiliging niet ook op orde is dan kan een aanvaller alsnog ongeautoriseerde toegang krijgen tot informatie(systemen). Het is daarom van essentieel belang dat informatiebeveiliging in alle vier hoofd aandachtsgebieden voldoende wordt vertegenwoordigd om ongewenste situaties te voorkomen. De BIO is het verplichte normenkader voor informatiebeveiliging binnen de overheid en helpt gemeenten om dit doel te bereiken.



Baseline Informatiebeveiliging Overheid (BIO)

De BIO heeft met ingang van 1 januari 2020 de Baseline Informatiebeveiliging Gemeenten (BIG) formeel vervangen als vigerend normenkader voor informatiebeveiliging binnen gemeenten. Hierbij

gold 2019 als overgangsjaar om van BIG naar BIO te migreren. De BIO is gebaseerd op de ISO 27002 standaard (2013 versie) en is verplicht gesteld voor de hele overheid en onderscheidt drie basisbeveiligingsniveaus (BBN). In de regel is voor gemeenten BBN-2 van toepassing. Risicomanagement vormt het uitgangspunt bij de BIO waarop de plan-do-check-act cyclus (PDCA-cyclus) conform de ISO 27001 toegepast dient te worden. De PDCA-cyclus is bedoeld om continue verbetering te kunnen realiseren ten aanzien van informatiebeveiliging. De ISO 27001 beschrijft hoe de PDCA-cyclus ingericht dient te worden en beschrijft 114 beheersmaatregelen waarmee generieke beveiligingsrisico's gemitigeerd kunnen worden (het 'wat'). De ISO 27002 bevat een nadere uitwerking van deze 114 beheersmaatregelen die zijn opgenomen in de ISO 27001 en beschrijft op welke manier deze geïmplementeerd kunnen worden (het 'hoe'). Dit laatste is precies hetgeen dat in de BIO is opgenomen maar dan nader toegespitst op alle Nederlandse overheden. De 114 beheersmaatregelen van de BIO zijn verplicht.

1.2 Doelstelling opdrachtgever

Het doel van het onderzoek is vaststellen in hoeverre de BIO door Overbetuwe aantoonbaar is geïmplementeerd. Hierbij dienen de volgende deelvragen beantwoord te worden:

1. *Hoe realistisch zijn de BIO-eisen vergeleken met de bestaande infrastructuur van Overbetuwe?*
2. *Naast de technische beveiliging is de gebruiker cruciaal. Wat is het bewustzijn van de gebruiker als het gaat om informatiebeveiliging (met name nu vanwege de Corona-crisis waar veelal vanuit huis gewerkt wordt)?*

1.3 Onderzoeksaanpak

Om een goed beeld te kunnen vormen van de mate waarin Overbetuwe aantoonbaar voldoet aan de eisen van de Baseline Informatiebeveiliging Overheid (BIO) is de onderstaande werkwijze toegepast.

1. Overbetuwe is voorafgaand aan de interviews gevraagd documentatie aan te leveren waarmee zij aantoont dat aan de BIO wordt voldaan ('show it'). Denk hierbij aan beleidsstukken, audit resultaten, ENSIA-rapportages, overige rapportages en interne documentatie zoals procedures of artikelen. Daarnaast is via openbare bronnen gezocht naar relevante informatie. In Bijlage A is een overzicht opgenomen van de ontvangen documentatie. In Bijlage C zijn enkele bevindingen van het open bronnen onderzoek[1] beschreven.

[1] Met open bronnen onderzoek wordt bedoeld dat er via openbare bronnen zoals het internet is gezocht naar relevante informatie voor dit onderzoek over de gemeente Overbetuwe. Cybercriminelen doen dit ook om zoveel mogelijk bruikbare informatie te vergaren die gebruikt kan worden tijdens een latere fase van de cyberaanval).

2. Om een goed beeld te kunnen vormen van de mate waarin informatiebeveiliging geïntegreerd is in de dagelijkse werkzaamheden van Overbetuwe zijn meerdere functionarissen van de gemeente op strategisch, tactisch en operationeel niveau geïnterviewd. Om de privacy van de betrokken medewerkers te beschermen worden er geen namen genoemd in dit rapport of wordt verwezen naar gedane uitspraken. Van elk interview is een verslag opgesteld dat is afgestemd is met de betrokken functionaris (*'hoor en wederhoor'*) en met hun instemming is gebruikt in dit onderzoek.

3. Tot slot is een analyse uitgevoerd op de bevindingen op basis waarvan conclusies zijn getrokken en aanbevelingen zijn gedaan met betrekking tot de informatiebeveiliging van Overbetuwe.

1.4 Beperkingen

Voor dit onderzoek is een beperkt aantal uren beschikbaar gesteld waardoor niet voor alle aspecten van informatiebeveiliging de volledige diepte in gedoken kan worden. Daarnaast is er in beperkte mate bewijslast ('evidence') aangeleverd door de gemeente Overbetuwe, waardoor veel bevindingen gebaseerd zijn op de informatie die in de interviews is aangereikt zonder dat hier een uitputtende controle op heeft kunnen plaatsvinden. Tot slot is het in verband met de Corona-crisis niet mogelijk geweest om op locatie de dagelijkse praktijk te observeren, bijvoorbeeld met betrekking tot de fysieke toegangsbeveiliging.

1.5 Leeswijzer

Hoofdstuk twee beschrijft in generieke zin het dreigingslandschap van Nederlandse gemeenten. Hoofdstuk drie beschrijft op hoofdlijnen de bevindingen die betrekking hebben op het aandachtsgebied mens. Hoofdstuk vier beschrijft op hoofdlijnen de bevindingen met betrekking tot het aandachtsgebied proces. Het vijfde hoofdstuk beschrijft de bevindingen met betrekking tot het aandachtsgebied Techniek. Hoofdstuk zes beschrijft de bevindingen met betrekking tot het aandachtsgebied fysieke beveiliging en hoofdstuk zeven bevat de conclusies en aanbevelingen.

Bijlage A bevat een overzicht van onderzochte documentatie. Bijlage B bevat een overzicht van geïnterviewde functionarissen. Bijlage C bevat enkele bevindingen die via openbare bronnen zijn vergaard en bijlage D bevat een toelichting op maatregelniveau van de ISO 27001 en Baseline Informatiebeveiliging Overheid.

2. Dreigingslandschap gemeenten

Afhankelijk van de sector waarin een organisatie opereert kan het dreigingslandschap er anders uit zien. De Informatiebeveiligingsdienst (IBD) is het sectorale Computer Emergency Response Team (CERT) en informeert Nederlandse gemeenten proactief over bedreigingen en (technische) kwetsbaarheden. De IBD voorziet gemeenten in passende beveiligingsadviezen, biedt hulpmiddelen aan om de algehele informatiebeveiliging te bevorderen, biedt ondersteuning bij (majeure) beveiligingsincidenten en vormt tot slot het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

Hoewel dit onderzoek primair gericht is op de mate van naleving van de eisen van de BIO door Overbetuwe zijn de relevante bedreigingen voor Nederlandse gemeenten meegewogen in het onderzoek. De voornaamste reden hiervoor is dat de BIO stelt dat gemeenten op basis van risicomanagement dienen te handelen. Zicht hebben op relevante beveiligingsrisico's en daar adequaat op reageren is daar een essentieel onderdeel van. De IBD heeft op 24 september 2020 het dreigingsbeeld (2021 – 2022) voor Nederlandse gemeenten gepubliceerd en gecommuniceerd naar alle gemeenten. Hierin worden actuele bedreigingen genoemd die een risico vormen voor verschillende doelgroepen. Omdat dit dreigingsbeeld pas zeer recent is uitgebracht is voor dit onderzoek nog rekening gehouden met het dreigingsbeeld 2019-2020. De risico's en prioriteiten van het dreigingsbeeld zijn gebruikt om gericht vragen te stellen aan de verschillende functionarissen. In bijlage B is een overzicht opgenomen van de geïnterviewde functionarissen.

Figuur 1 Overzicht risico's en prioriteiten 2019-2020 volgens de Informatiebeveiligingsdient

3. Mens

Het beveiligingsbewustzijn van de medewerkers is van essentieel belang bij het voorkomen, het (tijdig) identificeren van en het adequaat reageren op beveiligingsincidenten. Fysieke beveiliging vormt de eerste beveiligingslaag en de medewerkers vormen de laatste beveiligingslaag. Daartussen worden administratieve, procedurele en technische maatregelen getroffen. Om informatiebeveiliging adequaat in te richten is het van essentieel belang dat alle medewerkers hun verantwoordelijkheid ten aanzien van informatiebeveiliging kennen, bekend zijn met het informatiebeveiligingsbeleid en relevante wet- en regelgeving, dat zij de bedreigingen voor gemeenten in het algemeen op hoofdlijnen kennen en dat zij specifieke beveiligingsrisico's voor Overbetuwe kennen en weten hoe zij moeten handelen wanneer zich een beveiligingsincident voordoet. Het is ook van groot belang dat Overbetuwe zorgdraagt voor een organisatiecultuur waarin fouten gemaakt mogen worden en waar geleerd wordt van gemaakte fouten zonder dat de medewerkers daar de dupe van worden (*'no-blame cultuur'*).

Overbetuwe is zich ervan bewust dat het noodzakelijk is om het beveiligingsbewustzijn te stimuleren. In de afgelopen periode is flink geïnvesteerd om ervoor te zorgen dat alle medewerkers beschikken over de juiste kennis, houding en gedrag ten aanzien van informatiebeveiliging. Zo heeft er een nulmeting plaatsgevonden om het huidige niveau van beveiligingsbewustzijn te bepalen. De uitkomsten daarvan hebben geleid tot een gerichte bewustwordingscampagne die nog loopt tot en met februari 2021. Ook heeft er een phishing[2] simulatie plaatsgevonden en is Zivver[3] geïmplementeerd om menselijke fouten en datalekken[4] via e-mail te beperken en te voorkomen. De gekozen onderwerpen in de bewustwordingscampagne zijn generiek van aard, maar wel toegespitst op een aantal bekende beveiligingsrisico's van Overbetuwe. Zo bleek bijvoorbeeld dat het merendeel van de medewerkers niet wist waar en op welke manier beveiligingsincidenten gemeld moesten worden. Dit is essentieel omdat het niet of (veel) te laat melden van een beveiligingsincident de impact daarvan enorm kan verhogen. Wanneer de bewustwordingscampagne is afgerond zal een 1-meting plaatsvinden waarmee de delta wordt vastgesteld zodat bepaald kan worden of de huidige campagne de gewenste resultaten heeft opgeleverd.

Naast de activiteiten van het bewustwordingsprogramma is het ook van belang dat het lijn- en teammanagement het onderwerp informatiebeveiliging periodiek op de agenda plaatst om de voor hen relevante aspecten met de medewerkers te bespreken. Hierbij kan gedacht worden aan het bespreken van recente beveiligingsincidenten die zich hebben voorgedaan, geïdentificeerde beveiligingsrisico's of bijvoorbeeld ontwikkelingen die van invloed kunnen zijn op de dagelijkse gang van zaken. Ook heeft het management een cruciale rol in het waarborgen van informatiebeveiliging binnen hun verantwoordingsgebied. Denk hierbij onder andere aan het toepassen van risicomanagement, het uitvoeren van controles, het implementeren van beheersmaatregelen en het periodiek rapporteren over informatiebeveiliging aan de directie.

Ondanks de vele inspanningen en middelen die zijn gestoken in het meten en verhogen van het beveiligingsbewustzijn zijn er nog diverse aandachtspunten voor Overbetuwe om dit naar een hoger niveau te tillen:

- Gebleken is dat medewerkers bij indiensttreding nog niet 'secure-by-design' worden inge-werkt. Hiermee wordt bedoeld dat zij nog in onvoldoende mate worden voorzien van essenti-

[2] Phishing is een social engineering techniek waarbij geprobeerd wordt om mensen te verleiden om informatie te verstrekken, logingegevens af te staan, op een link te klikken of om een bijlage te openen.
[3] Zivver is een technische oplossing welke volledig geïntegreerd is in Outlook (Office365) en het mogelijk maakt voor medewerkers om veilig gevoelige informatie uit te wisselen via e-mail. Daarnaast draagt Zivver bij aan het verhogen van het beveiligingsbewustzijn door het geven van meldingen en het voorkomen van datalekken door content-monitoring.
[4] Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Of zonder dat dit wettelijk is toegestaan.

ele informatie, opleiding en training ten aanzien van informatiebeveiliging. Door het ontbreken hiervan beschikken zij niet direct vanaf indiensttreding over de noodzakelijke basiskennis (briefing);

- Gebleken is dat bij uitdiensttreding geen gesprekken plaatsvinden waarbij bijvoorbeeld de aspecten van geheimhouding worden besproken (debriefing);
- Deelname aan de activiteiten van de bewustwordingscampagne zijn vrijblijvend waardoor de dekkingsgraad onder alle medewerkers (hoogstwaarschijnlijk) lager zal zijn dan gewenst;
- Informatiebeveiliging is nog te veel 'het feestje van de CISO en de ISO'. Hiermee wordt bedoeld dat er nog onvoldoende eigenaarschap wordt getoond en dat de verantwoordelijkheden ten aanzien informatiebeveiliging nog onvoldoende worden behartigd op de juiste niveaus;
- Gebleken is dat de mate waarin informatiebeveiliging besproken wordt in team- of afdelingsverband sterk afhankelijk is van de verantwoordelijke lijnmanager;
- Er vindt geen registratie plaats van medewerkers die hebben deelgenomen aan bewustwordingsactiviteiten. Hierdoor kan niet aangetoond worden welke medewerkers hebben deelgenomen;
- Op het intranet is een speciale groep 'informatiebeveiliging' aangemaakt waarin de Chief Information Security Officer (CISO) en Information Security Officer (ISO) berichten plaatsen die van belang zijn voor alle medewerkers. Deelname aan deze groep is vrijblijvend waardoor deze belangrijke informatie hoogstwaarschijnlijk niet alle medewerkers bereikt.

4. Proces

Met 'proces' wordt hier bedoeld alle beleidsstukken, processen en procedures met betrekking tot informatiebeveiliging. Deze kunnen uiteenlopen van de onderwerpen van de BIO zoals bijvoorbeeld kwetsbaarhedenmanagement of het veilig inrichten van een nieuw gebouw, maar ook overige onderwerpen die niet expliciet in de BIO voorkomen zoals bijvoorbeeld kunstmatige intelligentie.

Gemeenten zijn complexe organisaties met veel verschillende werkprocessen. Om de werkprocessen goed te kunnen verrichten is Overbetuwe afhankelijk van verschillende bedrijfsmiddelen zoals mensen, hardware, software, netwerken en fysieke ruimten. Niet alle processen van Overbetuwe zijn even belangrijk voor het leveren van diensten en producten aan burgers en bedrijven of het verwerken van gevoelige informatie zoals bijzondere persoons- of financiële gegevens. Vanuit informatiebeveiligingsperspectief is het van essentieel belang dat Overbetuwe de voor haar meest belangrijke bedrijfsmiddelen ('kroonjuwelen'), identificeert, classificeert en koppelt aan een eigenaar (lees: verantwoordelijke). Onder classificeren wordt verstaan dat de betrouwbaarheidseisen (beschikbaarheid, integriteit en vertrouwelijkheid) worden toegekend aan bedrijfsmiddelen.

Naast het identificeren van de belangrijkste bedrijfsmiddelen is het van belang dat alle bedrijfsmiddelen zijn geïnventariseerd en zijn vastgelegd in een register.[5] Wanneer niet alle bedrijfsmiddelen in beeld zijn kunnen deze ook niet adequaat beveiligd worden. Denk bijvoorbeeld aan het doorvoeren van een update van een besturingssysteem waarmee kritieke kwetsbaarheden worden verholpen. Als niet alle apparatuur in beeld is bestaat de mogelijkheid dat de update niet overal wordt toegepast, waardoor de gemiste apparatuur per definitie vatbaar is voor de openbaar bekende kwetsbaarheden.

Als bedrijfsmiddelen inzichtelijk zijn gemaakt dient Overbetuwe te bepalen op welke manier zij minimaal beschermd moeten worden tegen ongeautoriseerde toegang, manipulatie en vernietiging. Dit kan door de doelstellingen en uitgangspunten van het informatiebeveiligingsbeleid verder te concretiseren op specifieke onderwerpen. Hierbij kan onder andere gedacht worden aan tactisch beleid, processen en werkinstructies voor IT-servicemanagement, kwetsbaarhedenmanagement, encryptie en fysieke beveiliging.

Afhankelijk van de context van deze processen, bedrijfsmiddelen en fysieke locaties en de onderlinge afhankelijkheden daartussen kunnen er verschillende beveiligingsrisico's zijn die een negatieve impact kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Het is daarom van belang dat Overbetuwe risicomanagement incorporeert in haar processen zodat beveiligingsrisico's (tijdig) geïdentificeerd, geclassificeerd en behandeld worden in lijn met de risico-acceptatiegrens. Wanneer beveiligingsrisico's niet of te laat worden gedetecteerd kunnen er ook geen passende maatregelen getroffen worden om de risico's te mitigeren tot een acceptabel niveau.

Als beveiligingsmaatregelen getroffen worden, bijvoorbeeld omdat dit een eis is vanuit wet- en regelgeving of omdat deze geïdentificeerde beveiligingsrisico's verkleinen, dient ook te worden vastgesteld of deze maatregelen de gewenste resultaten opleveren en voldoen aan interne en externe wet- en regelgeving ('compliance'). Overbetuwe kan dit doen door het (laten) uitvoeren van interne audits of door het inhuren van externe expertise om zekerheid te verschaffen over de mate waarin informatiebeveiliging voor een specifiek proces of informatiesysteem is geborgd.

Het college van burgemeester en wethouders (verder 'het college') heeft in juli 2020 het strategische informatiebeveiligingsbeleid vastgesteld. Hierin zijn de strategische doelstellingen, de visie, rollen en verantwoordelijkheden en belangrijkste uitgangspunten voor informatiebeveiliging vastgesteld. Het is de verantwoordelijkheid van de directie om vast te stellen of de vastgestelde doelstellingen worden

[5] Configuration Management DataBase (CMDB)

bereikt of dat moet worden bijgestuurd. Door de strategische doelstellingen SMART[6] te formuleren en te eisen dat zij periodiek geïnformeerd wordt over de status daarvan kan de directie hier beter grip op krijgen. Het 'systeem' waarmee een organisatie activiteiten met betrekking tot informatiebeveiliging aanstuurt en controleert wordt ook wel governance genoemd.

Ondanks dat Overbetuwe het afgelopen jaar de nodige inspanningen heeft geleverd en aantoonbaar goede stappen heeft gezet om haar volwassenheidsniveau ten aanzien van informatiebeveiliging te verhogen zijn er nog voldoende aandachtspunten, te weten:

- Overbetuwe heeft haar kritische bedrijfsmiddelen ('kroonjuwelen') nog niet geïdentificeerd, geclassificeerd en gekoppeld aan eigenaren. Hierdoor wordt er nog onvoldoende gefocust op de belangrijkste bedrijfsmiddelen, de mate van beveiliging die daarvoor benodigd is en het minimaliseren van beveiligingsrisico's. Gebleken is dat het voor sommige lijnmanagers niet duidelijk is voor welke bedrijfsmiddelen zij verantwoordelijk zijn;
- Gebleken is dat er geen zekerheid kan worden verschaft over de juistheid en volledigheid van het CMDB[7]. Hierdoor is er een verhoogde kans op het niet (tijdig) verhelpen van technische kwetsbaarheden;
- Er zijn nauwelijks tactische beleidsstukken, procedures en werkinstructies opgesteld voor specifieke onderwerpen van informatiebeveiliging. Hierbij kan gedacht worden aan onderwerpen zoals kwetsbaarhedenmanagement, IT-servicemanagement, encryptie of fysieke beveiliging. Hierdoor kan slechts in beperkte mate aangetoond worden op welke manier informatiebeveiliging in de praktijk moet worden toegepast en kan hier geen adequate controle op plaatsvinden;
- Er is nog geen methodiek voor integraal risicomanagement (Enterprise Risk Management - ERM) of specifiek voor informatiebeveiliging geïncorporeerd in de bedrijfsprocessen. Hierdoor worden beveiligingsrisico's nog niet op een gestructureerde wijze geïdentificeerd, geclassificeerd en opgevolgd. Er zijn tot op heden nog geen formele risicoanalyses uitgevoerd, ook niet in het kader van privacy (zogenaamde 'gegevenseffectenbeoordeling'). Kanttekening hierbij is dat er gewerkt wordt aan de opzet voor integraal risicomanagement onder leiding van concern control.
- Gebleken is dat reeds geïdentificeerde beveiligingsrisico's onvoldoende zijn opgepakt. Zo zijn eind 2019 al diverse (grote) beveiligingsrisico's aangekaart bij de directie, maar tot op heden niet opgepakt);[8]
- Gebleken is dat er geen plan is opgesteld waaruit blijkt welke beveiligingsmaatregelen op welke wijze, door wie en met welke frequentie moeten worden getoetst op doeltreffendheid, effectiviteit en compliance;
- Gebleken is dat de governance op informatiebeveiliging nog onvoldoende is ingericht zodat de gemeenteraad, college en directie kunnen controleren en gericht sturen op activiteiten met betrekking tot informatiebeveiliging. Zo sluit bijvoorbeeld de CISO regelmatig aan bij het directie-overleg, maar zijn de doelstellingen niet SMART geformuleerd of wordt er nog onvoldoende door het lijnmanagement gerapporteerd over de status en voortgang ten aanzien van

[6] SMART staat voor Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden
[7] De Configuration Management Database (CMDB) is een register waarin alle bedrijfsmiddelen inclusief hun belangrijkste kenmerken worden vastgelegd en bijgehouden. Als onbekend is welke assets een organisatie heeft kan ook niet bepaald worden of deze voldoende beveiligd zijn.
8 Zie ook hoofdstuk 5.

informatiebeveiliging. Informatiebeveiliging is ook geen vast agendapunt van de gemeenteraad en het college. Op geaggregeerd niveau vindt er rapportage aan de raad plaats over informatiebeveiliging. Hierdoor zijn zowel gemeenteraad als college onvoldoende in staat om vast te stellen of de 'juiste dingen worden gedaan' om beveiligingsrisico's adequaat te beheersen;

- Gebleken is dat er de afgelopen jaren geen gap-analyse meer is uitgevoerd om de mate van compliance ten opzichte van de Baseline Informatiebeveiliging Overheid (BIO) vast te stellen (tot eind 2019 was dit de BIG). Wel is software aangeschaft waarin controlewerkzaamheden en bewijslast kunnen worden geregistreerd en bijgehouden, maar dit wordt in de praktijk nauwelijks gebruikt. Hierdoor kan Overbetuwe niet aantonen wat de actuele status is ten opzichte van de BIO.

5. Techniek

Vanwege de sterk toenemende digitalisering in de samenleving neemt de afhankelijkheid van Informatie en Communicatie Technologie (ICT) en digitale informatie alleen maar toe. Het is daarom van groot belang dat beveiligingsrisico's in relatie tot ICT adequaat worden beheerst. Zo werd de gemeente Lochem afgelopen jaar nog op geavanceerde wijze aangevallen met als doel het ontoegankelijk maken van informatie(systemen) via ransomware zodat er losgeld geëist kon worden.[9] Overbetuwe heeft haar ICT volledig uitbesteed aan de gemeente Lingewaard (verder 'Lingewaard'). Hierdoor heeft zij het zorgdragen voor het aantoonbaar implementeren van een groot deel van de BIO-beheersmaatregelen uitbesteed. Echter Overbetuwe is en blijft zelf eindverantwoordelijk voor haar informatiebeveiliging (*'je kunt alles uitbesteden, behalve je verantwoordelijkheid!'*)

Voor het adequaat beveiligen van ICT-componenten zoals hard- en software is het van belang dat de basisprocessen op orde zijn. De basisprocessen zijn:

- Configuratiemanagement (*'weten wat je in huis hebt'*);
- Patchmanagement (*'dat wat je in huis hebt actueel houden'*);
- Wijzigingsbeheer (*'met de juiste aanpassingen hou je het veilig'*);
- Incidentmanagement (*'hoe reageer ik als het toch misgaat?'*).

Gebleken is dat organisaties vaak succesvol worden aangevallen omdat de basisprocessen niet op orde zijn. Ondanks dat Overbetuwe haar ICT-dienstverlening heeft uitbesteed blijft zij verantwoordelijk voor het aantoonbaar voldoen aan de eisen van de BIO die betrekking hebben op ICT. Het is daarom voor Overbetuwe van belang dat er strikte eisen worden gesteld aan de ICT-dienstverlening van Lingewaard en dat er wordt gecontroleerd op de effectiviteit en doeltreffendheid daarvan. Dit kan bijvoorbeeld bewerkstelligd worden door zelf controlewerkzaamheden uit te (laten) voeren of door te vragen om zekerheidsverklaringen ('assurance'). Lingewaard kan door het afgeven van zekerheidsverklaringen aantonen dat zij in voldoende mate beveiligingsmaatregelen heeft toegepast om beveiligingsrisico's te beheersen of dat processen correct worden uitgevoerd. Voorbeelden hiervan zijn ISO 27001 certificering, TPM-verklaringen[10] of Service Organisation Control (SOC) rapportages. Daarnaast kan Overbetuwe maatregelen zoals bijvoorbeeld een Service Level Agreement (SLA) overeenkomen met Lingewaard om haar eisen ten aanzien van de beschikbaarheid van de dienstverlening op te leggen en voor onderwerpen zoals incidentmanagement, geheimhouding en toegang tot informatie(systemen) van Overbetuwe.

Overbetuwe is aangehaakt op het GGI-veilig traject waarmee gemeenten hun weerbaarheid ten aanzien van informatiebeveiliging kunnen verhogen door het collectief verwerven van producten en diensten. Dit bespaart ook kosten waardoor ook kleinere gemeenten kunnen profiteren van geavanceerde oplossingen. Gebleken is dat Overbetuwe al voorbereidingen aan het treffen is voor de implementatie van een Security Information & Event Monitoring (SIEM) systeem en een Security Operations Center (SOC). Een SIEM verzamelt informatie uit logbestanden van informatiesystemen en monitort deze op opvallende of verdachte activiteiten. Een SOC monitort het netwerk 24x7 op indicatoren van reeds bekende cyberaanvallen ('Indicators of Compromise'). Beide oplossingen geven het volwassenheidsniveau van Overbetuwe een flinke duw in de rug omdat het potentiële beveiligingsincidenten snel detecteert. Dit stelt haar in staat om hier, indien nodig, snel op te acteren.

Om de continuïteit van de ICT-dienstverlening te waarborgen zijn er verschillende maatregelen getroffen zoals dubbel uitgevoerde verbindingen (redundantie) en zijn er twee ('actief-actief')

[9] https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-door-het-oog-van-de-naald-bij-hack-2553
[10] TPM: Third Party Memorandum

datacenters voor de opslag van informatie en het serveren van applicaties. Dit wil zeggen dat bij uitval van een datacenter dezelfde applicatie voortgezet kan worden vanuit het andere datacenter.

Ondanks dat Overbetuwe maatregelen heeft getroffen om haar ICT te beveiligen volgen hieronder een aantal aandachtspunten:

- Overbetuwe heeft door middel van een Service Niveau Overeenkomst (SNO) en Producten en Diensten Catalogus (PDC) concrete afspraken gemaakt met de gemeente Lingewaard over de te leveren diensten. Zo zijn er afspraken gemaakt over de beschikbaarheidsniveaus, het maximaal aanvaardbare dataverlies, reactietijden voor (beveiligings)incidenten en crisismanagement, communicatie, wijzigingsbeheer, rapporteren en monitoring. Het is echter onduidelijk in welke mate deze afspraken in de praktijk worden nageleefd.
- Gebleken is dat de basisprocessen voor ICT nog onvoldoende op orde zijn. Zo is er nog geen beleid opgesteld dat de richtlijnen en regels voor een veilige ICT-infrastructuur bevat. Er zijn bijvoorbeeld geen procesbeschrijvingen voor wijzigingsbeheer, patchmanagement of configuratiemanagement, waardoor niet aangetoond en gecontroleerd kan worden of deze adequaat worden uitgevoerd;
- Gebleken is dat er nauwelijks ‘test’ en ‘acceptatie’ omgevingen zijn waardoor updates en wijzigingen vaak direct in de productie-omgeving worden doorgevoerd. Mocht een update of wijziging niet naar behoren werken dan heeft dit direct impact op de gebruikersorganisatie;
- Er vindt op dit moment in beperkte mate monitoring en detectie plaats in de ICT-infrastructuur waardoor de kans groter is dat cyberaanvallen of ongeautoriseerde handelingen door medewerkers niet of veel te laat worden gedetecteerd. Logbestanden worden over het algemeen reactief en sporadisch geraadpleegd waardoor een verhoogde kans is op het missen van indicaties die kunnen duiden op misbruik. Er wordt ook niet gerapporteerd over gedetecteerde gebeurtenissen door de firewall, Intrusion Detection & Prevention Systemen (IDS/IPS);
- De ICT-foto, waarin ICT de Informatiebeveiligingsdienst voorziet in alle soft- en hardware die door Overbetuwe en Lingewaard wordt gebruikt, wordt slechts 1x per jaar geactualiseerd. Hierdoor is een verhoogde kans op het missen van cruciale informatie met betrekking tot technische kwetsbaarheden die mogelijk wel van toepassing zijn op de ICT-infrastructuur;
- Gebleken is dat de werkplekken nog vatbaar zijn voor cyberaanvallen waarbij malware wordt afgeleverd via macro’s;
- Gebleken is dat uitgegeven mobiele telefoons worden beheerd via een Mobile Device Management (MDM) oplossing, maar dat de maatregelen echter beperkt zijn tot het kunnen wissen van het apparaat op afstand bij verlies of diefstal en toegang tot het interne netwerk en webmail;
- Bij uitval van een datacenter is het andere datacenter in staat om dezelfde dienstverlening voort te zetten, echter vergt dit handmatige handelingen. Er kan momenteel geen inschatting gemaakt worden van de benodigde tijd en capaciteit;
- Er worden niet periodiek continuïteitstesten verricht om vast te stellen of het continueren van de dienstverlening ook daadwerkelijk slaagt binnen een bepaalde periode. Er kan daarom geen inschatting gemaakt worden van de benodigde tijd en capaciteit. Er zijn ook geen business continuïteit plannen of disaster recovery plannen opgesteld waaruit blijkt hoe er gehandeld moet worden indien zich een calamiteit voordoet;

- Gebleken is dat beveiligingsincidenten niet altijd even goed worden geëvalueerd en opgevolgd *('leren van gemaakte fouten'*). Hierdoor is een verhoogde kans op herhaling van beveiligings-incidenten. Er wordt bijvoorbeeld geen root-cause analyse[11] uitgevoerd om de oorzaak van een verstoring inzichtelijk te maken;
- Gebleken is dat er ruimte voor verbetering is voor wat betreft het monitoren op technische kwetsbaarheden;
- De afdeling ICT van de gemeente Lingewaard is onderverdeeld in twee teams. Het ene team is primair werkzaam voor de gemeente Overbetuwe, en de ander voor de gemeente Lingewaard. Het team dat zich focust op Overbetuwe ervaart een te hoge werkdruk waardoor zij onvoldoende in staat zijn om aantoonbaar te voldoen aan de gevraagde eisen.

[11] Analyse om de oorzaak onweerlegbaar vast te stellen zodat de juiste oplossing kan worden toegepast.

6. Fysieke beveiliging

Fysieke beveiliging vormt de eerste beveiligingslaag voor organisaties. Zonder effectieve fysieke beveiliging hebben technische en administratieve maatregelen geen of in mindere mate effect. Fysieke beveiliging is noodzakelijk om ongeautoriseerde toegang tot ruimten en bedrijfsmiddelen te voorkomen waarmee de kans op diefstal, schade en misbruik daarvan wordt voorkomen. Hierbij kan gedacht worden aan het plaatsen van hekwerk rondom locaties van Overbetuwe, het plaatsen van cameratoezicht, het aanstellen van een beveiliger, het gebruik van toegangspoorten of kaartlezers en het beperken van toegang tot ruimten tot die medewerkers waarvoor dat noodzakelijk is. Mede door de Corona-crisis is het voor de onderzoeker niet mogelijk geweest om een observatie op locatie uit te voeren, waardoor er geen goed beeld gevormd kan worden van de mate waarin Overbetuwe fysieke toegangsbeveiliging heeft toegepast.

Ondanks het feit dat de fysieke (toegangs)beveiliging niet geobserveerd kon worden zijn er wel een aantal aandachtspunten:

- Er is geen fysiek toegangsbeleid opgesteld waaruit blijkt aan welke regels en richtlijnen gebouwen of specifieke ruimten moeten voldoen. Denk hierbij aan het toepassen van zonering of het definiëren van (on)gewenst gedrag;
- Er is geen documentatie aangeleverd waaruit blijkt welke gebouwen behoren tot de scope van het managementsysteem voor informatiebeveiliging;
- Er is geen documentatie aangeleverd waaruit blijkt dat beveiligingsrisico's voor alle aspecten van fysieke (toegangs)beveiliging zijn geïdentificeerd. Hierbij kan gedacht worden aan de plaatsing van apparatuur, het wegwerken van en het beschermen van bekabeling, sloten, ramen, deuren en personeelsingangen;
- Gebleken is dat medewerkers nog onvoldoende gewenst gedrag vertonen zoals het vergrendelen van schermen of het zorgvuldig opbergen van (gevoelige) informatie. Dit aspect is wel opgenomen in de bewustwordingscampagne.

7. Conclusies & aanbevelingen

Op basis van de bevindingen van het onderzoek zijn conclusies getrokken en worden aanbevelingen gedaan om de mate waarin Overbetuwe nu aan de eisen van de BIO voldoet verder te verbeteren.

Het op orde hebben van de informatiebeveiliging is van essentieel belang om diensten en producten te kunnen (blijven) leveren aan burgers en bedrijven, het voldoen aan wet- en regelgeving, het voorkomen en/of beperken van reputatie-, operationele- of financiële schade door bijvoorbeeld boetes van een toezichthouder of majeure beveiligingsincidenten. Concrete voorbeelden hiervan zijn:

- Het afsluiten van Digid of Suwinet aansluitingen;

- Het opleggen van een boete door Autoriteit Persoonsgegevens (privacy toezichthouder);

- Ongeautoriseerde toegang tot (informatie)systemen en/of netwerken;

- Het verlies van vertrouwen in bestuurders en/of de overheid door burgers en bedrijven;

Dit zijn allemaal zeer ongewenste situaties en deze dienen zoveel mogelijk voorkomen te worden door structureel aandacht te besteden aan informatiebeveiliging op alle lagen van de organisatie en in de samenwerking met ketenpartners.

7.1 Conclusies

Mens

Overbetuwe heeft zicht op de beveiligingsrisico's die gepaard gaan met menselijk gedrag en heeft hier ook aantoonbaar in geïnvesteerd om dit in positieve zin te beïnvloeden. De verantwoordelijkheden, taken en bevoegdheden ten aanzien van informatiebeveiliging zijn nog niet volledig vertaald naar de dagelijkse praktijk waardoor het lijnmanagement in de praktijk nog in onvoldoende mate informatie-beveiligingsactiviteiten uitvoert, hierop stuurt of controleert.

Proces

Overbetuwe heeft in onvoldoende mate zicht op naleving van de eisen van de BIO en de effectiviteit en doeltreffendheid van reeds getroffen beveiligingsmaatregelen. Ook heeft zij beveiligingsrisico's nog onvoldoende in kaart gebracht en wordt hierop nauwelijks gestuurd. De doelstellingen zijn niet SMART geformuleerd en er wordt niet gerapporteerd over de mate waarin de doelstellingen worden bereikt. Voor een groot deel van de BIO ontbreekt het aan tactische en operationele regels en richtlijnen, waardoor informatiebeveiliging nog niet op eenduidige wijze aantoonbaar wordt toegepast.

Techniek

Overbetuwe heeft nog onvoldoende inzicht in de mate waarin ICT voldoet aan de beheersmaatregelen van de BIO en stuurt / monitort hier niet actief op. Daarnaast vinden er geen controles plaats om vast te stellen of processen correct worden uitgevoerd of dat beveiligingsrisico's adequaat beheerst worden. De CISO en ISO hebben inhoudelijk overleg met ICT, maar vanuit het (senior) management is hier nog te weinig aandacht voor. Monitoren op technische kwetsbaarheden kan verder worden verbeterd en basisprocessen zijn niet aantoonbaar op orde.

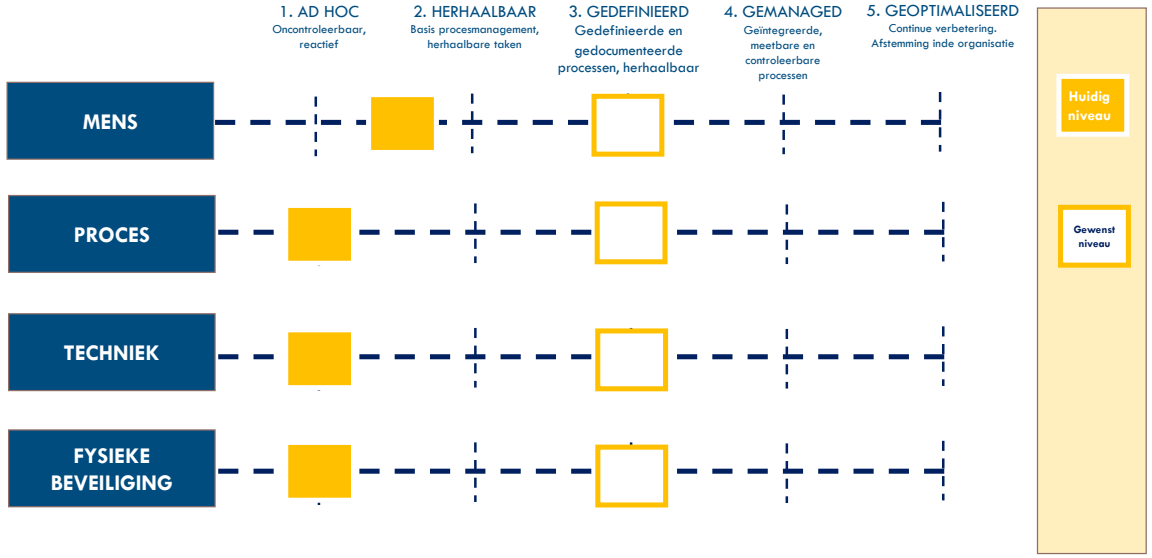
Fysieke beveiliging

Er is geen toegangsbeleid vastgesteld waaruit blijkt op welke wijze bedrijfsmiddelen beschermd (moeten) worden in gebouwen, specifieke zones of ruimten en welk gedrag daarbinnen (on)wenselijk is. De mate waarin beveiliging wordt toegepast binnen de gebouwen van de gemeente berust momenteel primair bij Buitenruimten en Vastgoed. Het is onduidelijk of alle aspecten van informatiebeveiliging hierbij in acht worden genomen.

Volwassenheid informatiebeveiliging Overbetuwe

De gemeten volwassenheid ten aanzien van de informatiebeveiliging van Overbetuwe is geplot op het volwassenheidsmodel voor informatiebeveiliging en weergeven in onderstaande figuur.

Volwassenheidsmodel informatiebeveiliging gemeente Overbetuwe (status oktober 2020)



Volledige BIO-compliancy betekent dat Overbetuwe op alle vier de hoofdgebieden aantoonbaar aan niveau 4 Gemanaged zou moeten voldoen (objectief vast te stellen in een externe audit). In 2018 is de komst van de BIO aangekondigd en dat deze per 01.01.2020 effectief in werking treedt, ergo verplicht is. Hierbij is gecommuniceerd dat 2019 een overgangsjaar is om de migratie van BIG naar BIO te bewerkstelligen. Concreet betekent dit dat Overbetuwe in 2020 minimaal aantoonbaar op niveau 2 zou moeten kunnen staan. Realistisch is om vervolgens verder door te groeien zodat eind 2021 aantoonbaar aan niveau 3 wordt voldaan en eind 2022 aan niveau 4. Dit is op dit moment niet het geval.

Noot: Omdat de fysieke (toegangs)beveiliging niet geobserveerd kon worden en er geen functionarissen zijn geïnterviewd die hier verantwoordelijk voor zijn, kan het daadwerkelijke volwassenheidsniveau hoger liggen. Omdat er geen documentatie is aangeleverd kon er geen verificatie plaatsvinden en is het volwassenheidsniveau 1. AD-HOC toegekend. Het gewenste niveau is op volwassenheidsniveau drie (Gedefinieerd) geplaatst omdat dit het niveau is waar Overbetuwe minimaal zou moeten willen staan. Als dit niveau behaald is verricht zij structureel diverse activiteiten waardoor opzet, bestaan en effectieve werking van beheersmaatregelen aantoonbaar gemaakt kunnen worden en worden beveiligingsrisico's adequaat beheerst. De BIO ervoor zorgt dat de gemeente haar processen met betrekking tot informatiebeveiliging heeft gedocumenteerd, structureel uitvoert en aantoonbaar maakt.

Onderzoeksvragen

In dit onderzoek dient onderstaande onderzoeksvraag beantwoord te worden:

In hoeverre heeft de gemeente Overbetuwe de BIO (aantoonbaar) geïmplementeerd?

Overbetuwe heeft geen inzicht in welke mate waarin zij momenteel (aantoonbaar) voldoet aan de eisen van de BIO. De laatste gap-analyse stamt uit 2017 en was gebaseerd op de BIG[12], het vervallen normenkader voor informatiebeveiliging. Uit de analyse van de ontvangen documentatie en de

[12] BIG: Baseline Informatiebeveiliging Gemeenten

interviews is gebleken dat er in zeer beperkte mate informatie beschikbaar is waaruit blijkt hoe Overbetuwe informatiebeveiliging in de bedrijfsprocessen heeft geborgd. In bijlage D is, voor zover dat mogelijk was, is op maatregel niveau toegelicht welke bevindingen er zijn. **Geconcludeerd kan worden dat aan het overgrote deel van de BIO niet aantoonbaar wordt voldaan.** Dit wil niet zeggen dat zaken ook niet geregeld zijn, maar wel dat dit in ieder geval nog onvoldoende kan worden aangetoond. Overbetuwe heeft software aangeschaft om controlewerkzaamheden en bewijslast ('evidence') te registreren en te onderhouden, maar maakt hier tot op heden nauwelijks gebruik van. In bijlage D is een overzicht opgenomen van de bevindingen op maatregelniveau van de BIO en ISO 27001.

Naast de hoofdvraag zijn er nog twee deelvragen gesteld:

1. *Hoe realistisch zijn de BIO-eisen vergeleken met de bestaande infrastructuur van Overbetuwe?*
2. *Naast de technische beveiliging is de gebruiker cruciaal. Wat is het bewustzijn van de gebruiker als het gaat om informatiebeveiliging (met name nu vanwege de Corona-crisis waar veelal vanuit huis gewerkt wordt)?*

Ad 1. De 114 beheersmaatregelen van de BIO zijn verplicht voor alle Nederlandse overheden, dus ook voor Overbetuwe. Het feit dat zij haar ICT volledig heeft uitbesteed zorgt ervoor dat het zorgdragen voor het aantoonbaar voldoen aan de BIO primair bij de gemeente Lingewaard ligt. Ongeveer 60% van de BIO-beheersmaatregelen heeft direct betrekking op ICT. Dit is echter **niet** de verantwoordelijkheid van Lingewaard, maar van Overbetuwe *('je kunt alles uitbesteden, behalve je verantwoordelijkheid'*).

Ad 2. Het beveiligingsbewustzijn is over alle medewerkers gezien nog onder de maat. Dit blijkt uit verschillende onderzoeken en metingen, maar Overbetuwe heeft flink geïnvesteerd om dit te structureel te verbeteren. In 2021 zal gemeten worden of de investeringen de gewenste resultaten hebben opgeleverd.

7.2 Aanbevelingen

Op basis van de conclusies zijn aanbevelingen gedaan waarmee Overbetuwe haar volwassenheid ten opzichte van de BIO kan verhogen. De aanbevelingen zijn voorzien van een kleur om de urgentie daarvan aan te geven. **Legenda:**

	Een plan van aanpak voor verbetermaatregelen dient **op korte termijn** (< 3 maanden) ontwikkeld en uitgevoerd te worden.
	Een plan van aanpak voor verbetermaatregelen dient **binnen een redelijke termijn** (< 6 maanden) te worden ontwikkeld en uitgevoerd.
	Een plan van aanpak voor verbetermaatregelen dient op **langere termijn** (< 12 maanden) ontwikkeld en uitgevoerd te worden.

Mens

#	Aanbeveling
1	Maak duidelijk welke verwachtingen het college heeft van de lijnmanagers ten aanzien van informatiebeveiliging en zorg ervoor dat zij met behulp van kennisoverdracht ook in staat zijn om hun taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging uit te voeren. Zij kunnen hierin geadviseerd en ondersteund worden door de CISO en ISO.
2	Hou vast aan de huidige aanpak van het structureel verhogen van het beveiligingsbewustzijn onder alle medewerkers. Zorg ervoor dat wordt vastgelegd welke basiskennis noodzakelijk is voor welke functies en of rollen. Afhankelijk van de functie of rol kan het benodigde beveiligingsbewustzijn variëren. Leg daarnaast vast welke medewerkers aan welke bewustwordingsactiviteiten hebben deelgenomen om de aantoonbaarheid te borgen en om medewerkers te kunnen aanspreken die niet hebben deelgenomen. Het implementeren van een Leermanagementsysteem (LMS) kan bijdragen aan het verbeteren en borgen van de aanbevelingen uit de categorie 'Mens'.
3	Integreer informatiebeveiliging nadrukkelijker in het indiensttredingsproces zodat nieuwe medewerkers *'secure-by-design'* worden ingewerkt. Laat hen bijvoorbeeld kennisnemen van geldend beleid, processen en procedures en laat hen een verklaring ondertekenen waarin zij verklaren kennis te hebben genomen van en dit zullen naleven. Hiermee wordt ook direct aantoonbaarheid geborgd. De CISO kan hierbij ondersteunen.

Proces

#	Aanbeveling
1	Identificeer de kritische bedrijfsmiddelen, voorzie deze van de betrouwbaarheidseisen en koppel deze aan eigenaren. Zo weet het management waar adequate beveiliging de hoogste prioriteit heeft en heeft het lijnmanagement scherp waarvoor zij verantwoordelijk is.
2	Geadviseerd wordt om minimaal de verplichte beleidsstukken van de BIO op te stellen en formeel vast te stellen waarmee op een gedetailleerder niveau invulling gegeven wordt aan de strategische doelstellingen van Overbetuwe. Daarnaast stelt dit het management in staat om gericht controlewerkzaamheden uit te voeren waarmee vastgesteld kan worden of de gewenste resultaten zijn bereikt.
3	Introduceer integraal risicomanagement zodat alle risico's, dus niet alleen in het kader van informatiebeveiliging, op dezelfde manier worden geïdentificeerd, geclassificeerd en behandeld. Voer zo snel mogelijk risicoanalyses uit voor de bedrijfskritische processen en bedrijfsmiddelen zodat deze adequaat beheerst kunnen worden.
4	Geadviseerd wordt om het college te vragen om een uitgebreid plan (roadmap) op te laten stellen waarin zij beschrijft hoe de naleving van de BIO en daarmee ook de volwassenheid ten aanzien van informatiebeveiliging op korte termijn aantoonbaar wordt verbeterd.
5	Zorg ervoor dat de planning met betrekking tot informatiebeveiliging alle verplichte activiteiten bevat voor het continu verbeteren daarvan. Denk hierbij aan documentatiereview, risicomanagement, interne - en externe audits, concretiseren van doelstellingen, leveranciersmanagement en in - en externe onderwerpen die van invloed kunnen zijn op het managementsysteem voor informatiebeveiliging, et cetera.

6	Betrek het college en de raad meer en vaker bij het onderwerp informatiebeveiliging. Zorg ervoor dat zij vaker pro-actief worden geïnformeerd worden over de status van informatiebeveiliging en op de hoogte worden gehouden van de belangrijkste ontwikkelingen daarin.
7	Zorg ervoor dat bewijslast (*'evidence'*), waarmee aangetoond kan worden dat wordt voldaan aan BIO-eisen, wordt vastgelegd op een centrale locatie, zodat een helder overzicht ontstaat van de tekortkomingen ten opzichte van de BIO. Het management is zo beter in staat om gericht actie te ondernemen waar nodig;
8	Overweeg om een strategisch programma voor informatiebeveiliging binnen Overbetuwe te starten zodat informatiebeveiliging structureel wordt verbeterd en geborgd. Hierdoor kan bereikt worden dat uiterlijk eind 2022 aantoonbaar aan de eisen van de BIO wordt voldaan (volwassenheidsniveau 4. Gemanaged). Concreet betekent dit dat de implementatie van de BIO voortvarend moet worden opgepakt zodat al eind 2021 volwassenheidsniveau 3. Gedefinieerd bereikt kan worden. Het actuele niveau kan door middel van een externe audit worden vastgesteld.

Techniek

#	Aanbeveling
1	Voer op korte termijn een nieuwe penetratietest uit op de ICT-infrastructuur om inzicht te verkrijgen in (mogelijke) kwetsbaarheden. Daarnaast wordt sterk aanbevolen om geautomatiseerde kwetsbaarhedenscans uit te voeren waarmee periodiek gemonitord wordt op kwetsbaarheden. Met name vanwege een tekort aan detectiemogelijkheden is het tijdig verhelpen van kwetsbaarheden van essentieel belang om misbruik te voorkomen.
2	Zorg dat de basisprocessen van ICT op orde worden gebracht en monitor deze nauwlettend om ongewenste situaties te voorkomen. De Informatiebeveiligingsdienst (IBD) biedt advies en hulpmiddelen aan die kunnen helpen om dit proces te versnellen. De BIO is niet heel technisch van aard, daarom wordt sterk aanbevolen om minimaal de zes basismaatregelen van het *Center for Internet Security* (CIS)[13] volledig te implementeren. Wanneer aan deze basis wordt voldaan kan ongeveer 80% van de meest voorkomende cyberaanvallen worden afgewend.
3	Zorg dat ICT over de benodigde middelen beschikt om documentatie op orde te brengen en te houden en er periodiek hersteltesten uitgevoerd kunnen worden zodat vastgesteld kan worden of backups succesvol teruggeplaatst kunnen worden of dat de overeengekomen afspraken ook daadwerkelijk gerealiseerd kunnen worden (Service Niveau Overeenkomst & Producten en Diensten Catalogus).

[13] https://www.cisecurity.org/controls/cis-controls-list/

Fysieke beveiliging

#	Aanbeveling
1	Zorg dat duidelijk is op welke locaties zich bedrijfsmiddelen van Overbetuwe bevinden, zodat daar adequate beveiliging op kan worden toegepast. Voer risicoanalyses uit om inzicht te verkrijgen in fysieke beveiligingsrisico's. Zorg er daarnaast voor dat er voor iedere locatie een verantwoordelijke is voor fysieke (toegangs)beveiliging.
2	Overweeg om de *Crime Prevention Through Environmental Design (CPTED)* principes toe te passen om gewenst gedrag te stimuleren en om ongewenst gedrag te beperken. CPTED maakt op slimme wijze gebruik van de omgeving om beveiligingsrisico's te verkleinen.

Bestuurlijke reactie college

De Rekenkamer
Ds. H. Smeets

Uw brief van	Uw kenmerk	Ons kenmerk	Datum	Verzonden d.d.
		20uit26676	5 januari 2021	
Onderwerp:		**Behandeld door**	**Telefoonnummer**	**Bijlage(n)**
Bestuurlijke reactie onderzoek informatiebeveiliging		S. van Eldik-Giesbers	14 0481	

Geachte heer Smeets en overige leden van de Rekenkamer,

Wij danken u voor het “Volwassenheidsonderzoek informatiebeveiliging gemeente Overbetuwe”. Graag maken wij gebruik van de mogelijkheid om hierop te reageren.

Informatieveiligheid is een belangrijk en actueel thema. De krantenberichten over hacks bij de Universiteit Maastricht en de gemeente Hof van Twente onderstrepen het belang van een goede informatiebeveiliging. Ons college is dan ook blij dat de Rekenkamer zich over dit onderwerp heeft gebogen en een aantal aanbevelingen doet. We doen daar graag ons voordeel mee om onze informatieveiligheid nog verder te verbeteren.

De BIO bestaat pas kort. Gelet op onze uitgangspositie en gelet op de beperkte mogelijkheden die een middelgrote organisatie als de onze heeft, hebben wij snel grote stappen vooruit gezet in de beveiliging van onze informatie. Maar we zijn er nog niet.

Met gemeente Lingewaard, die onze ICT verzorgt, zullen wij daarom op de kortst mogelijke termijn afspraken maken om de verbeteringen die de hoogste prioriteit hebben uit te voeren. De aanbevelingen van de Rekenkamer helpen ons daarbij. Omdat menselijk gedrag de factor is waar we de grootste winst kunnen behalen, zullen wij blijven inzetten op dat aspect en daarbij ook de rol van het management verder aanscherpen.

Wij zijn positief over het rapport en blij met de aanbevelingen. Deze ziin voor ons waardevol en hiermee kunnen wij ons voordeel doen. Toch staan er een aantal punten in het rapport dat ons bevreemdt. U schrijft bijvoorbeeld op punten dat er niet voldoende bewijslast is overlegd en daardoor niet aan de gestelde norm wordt gedaan. In een aantal gevallen hadden wij eenvoudig deze bewijslast kunnen aanleveren, maar heeft u daar niet om verzocht. Ook geeft u aan dat er “een beperkt aantal uren beschikbaar is gesteld waardoor niet voor alle aspecten van informatiebeveiliging de volledige diepte in gedoken kan worden”. De conclusies zijn op onderdelen dan ook niet volledig waardoor een vertekend beeld ontstaat.

Dat zal ons echter niet beletten om met uw aanbevelingen in de hand, vol in te zetten op het versterken van de informatiebeveiliging. U verzoekt ons jaarlijks te rapporteren over de stand van zaken met betrekking tot de BIO. Naast dat we dit middels ENSIA doen, zullen wij dit doen en u ook afzonderlijk informeren over de BIO.

Hoogachtend,

burgemeester en wethouders,
de gemeentesecretaris, de burgemeester,

P.J.E. Breukers R.P. Hoytink-Roubos

Dorpsstraat 67, Elst/Postbus 11, 6660 AA Elst T 14 0481
E info@overbetuwe.nl www.overbetuwe.nl IBAN: NL03BNGH0285092030 BIC:BNGHNL2G
KvK nummer 51178567 Btw nr NL809032375B01

Nawoord rekenkamercommissie

Wij hebben kennis genomen van de reactie van het college van B&W. Wat betreft het door het college aangegeven punt van de niet gevraagde bewijslast waardoor er mogelijk een vertekend of onjuist beeld zou kunnen ontstaan, hebben wij de onderzoeker verzocht om, nadat wij de aanvullende informatie hadden ontvangen, hier aanvullend naar te kijken. Dit heeft inderdaad geleid tot een bescheiden bijstelling van onze bevindingen. Deze zijn in het eindrapport verwerkt.

Wij waarderen de voortvarendheid die spreekt uit de bestuurlijke reactie.

Dorpsstraat 67
6661 EH Elst
Postbus 11
6660 AA Elst
telefoon 14 0481
fax (0481) 372 482

info@overbetuwe.nl
www.overbetuwe.nl

gemeente Overbetuwe