Baseline Informatiebeveiliging Gemeente Deventer

Opdrachtgever: H. van den Berg, TM IAO
Auteur: J.H.B. van Maanen
Versie : 1.0
Datum : 15 december 2011

"INFORMATIEBEVEILIGING IS HET GEHEEL VAN PREVENTIEVE-, REPRESSIEVE- EN HERSTELMAATREGELEN ALSMEDE PROCEDURES WELKE DE BESCHIKBAARHEID, EXCLUSIVITEIT EN INTEGRITEIT VAN ALLE VORMEN VAN INFORMATIE GARANDEREN MET ALS DOEL DE CONTINUÏTEIT VAN DE ORGANISATIE TE WAARBORGEN EN DE EVENTUELE GEVOLGEN VAN BEVEILIGINGSINCIDENTEN TOT EEN ACCEPTABEL, VOORAF BEPAALD, NIVEAU TE BEPERKEN."

Inhoudsopgave

Inleiding

Met deze nota wordt een volgende stap gezet in een proces dat moet leiden tot een beter inzicht in de informatiebeveiliging binnen de gemeentelijke organisatie en uiteindelijk tot een hoger niveau van informatiebeveiliging.
Medio 2007 is door B&W de Nota Informatiebeveiliging (notanr. 2007.10943) vastgesteld.
Hiermee zijn de beleidsuitgangspunten[1] voor informatiebeveiliging binnen de Deventer gemeentelijke organisatie vastgesteld. Deze geven de basisregels voor informatiebeveiliging, een gemeenschappelijke basis voor het ontwikkelen van beveiligingsnormen en een kader voor te nemen maatregelen. In deze fase zijn eveneens de meest kritische informatiesystemen geïdentificeerd en geclassificeerd naar belangrijkheid op de drie hoofdaspecten van informatiebeveiliging.

Tevens is met de nota opdracht gegeven tot een vervolgproject (fase 2), om de vastgestelde beleidsuitgangspunten in te vullen door het opstellen van een 'baseline' informatiebeveiligingsplan voor de gemeente. Hierin worden de beleidsuitgangspunten nader uitgewerkt en worden (minimum) beveiligingseisen en -maatregelen opgenomen die gemeentebreed voor alle processen en systemen gelden. De classificatie uit fase 1 bepaalt mede het (minimum) beveiligingsniveau voor gedeelde zaken. Onderdeel van het plan is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- & controlcyclus (PDCA) binnen de (kwaliteitshandhaving van de) bedrijfsvoeringsprocessen.

Het nu voorliggende baseline informatiebeveiligingsplan is het resultaat van het project.

Leeswijzer

Deze nota bestaat uit twee delen:

Het eerste deel begint met een algemene inleiding over informatiebeveiliging en over het project. Vervolgens worden de bevindingen uit het project gepresenteerd, en er worden beleids- en beheermaatregelen voorgesteld om de informatiebeveiliging te verbeteren.

Het tweede deel bestaat uit een analyse van de informatiebeveiliging bij de gemeente Deventer, afgezet tegen de normen van de Code voor Informatiebeveiliging. Dit vormt de basis voor de conclusies en de voorgestelde beleidsmaatregelen in het eerste deel.

Hoofdstuk 1 geeft een algemene inleiding op het thema Informatiebeveiliging en de toepassing hiervan binnen gemeente Deventer, alsmede een schets van het project en het vervolgtraject.
Hoofdstuk 2 beschrijft de voornaamste conclusies uit het project.
Hoofdstuk 3 geeft aanbevelingen voor informatiebeveiliging; het voorgestelde beleid.

Hoofdstuk 4 tot en met hoofdstuk 15 geven de analyse voor het voorgestelde beleid. Per item wordt naast het normenkader een beschrijving van de feitelijke situatie gegeven en daar waar van toepassing worden de risico's van de bestaande toestand weergegeven en worden voorstellen gedaan om de feitelijke situatie in overeenstemming te brengen met de gewenste situatie.

De toegepaste hoofdstukken uit de Code voor informatiebeveiliging (NEN-ISO/IEC 27002:2007) voor de baseline Informatiebeveiliging Gemeente Deventer zijn:

Hoofdstuk 5 Beveiligingsbeleid;
Hoofdstuk 6 Organisatie van informatiebeveiliging;
Hoofdstuk 7 Beheer van bedrijfsmiddelen;
Hoofdstuk 8 Beveiliging van personeel;
Hoofdstuk 9 Fysieke beveiliging en beveiliging van de omgeving;
Hoofdstuk 10 Beheer van communicatie en bedieningsprocessen;
Hoofdstuk 11 Toegangsbeveiliging;
Hoofdstuk 12 Verwerving, ontwikkeling en onderhoud van informatiesystemen;
Hoofdstuk 13 Beheer van informatiebeveiligingsincidenten;
Hoofdstuk 14 Bedrijfscontinuïteitsbeheer;
Hoofdstuk 15 Naleving.

[1] Zie bijlage 1.

1 Informatiebeveiliging

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van informatiesystemen en van de informatie daarin. Het beoogt het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade voor de gemeente door het trachten te voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

Het begrip "informatiebeveiliging" heeft betrekking op drie hoofdaspecten[2]:

- *vertrouwelijkheid / exclusiviteit*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *betrouwbaarheid / integriteit:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- *beschikbaarheid / continuïteit:* het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.

Deze aspecten kunnen meer tastbaar worden gemaakt door ze te zien als het antwoord op de volgende drie vragen:

- "wat vind je er van als je gegevens door iedereen gelezen worden?"
- "wat vind je er van als er onzekerheid is over de betrouwbaarheid van de gegevens?"
- "wat vind je er van als gegevens of systemen niet beschikbaar zijn?".

1.1 Waarom informatiebeveiliging?

Informatie is een van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor "behoorlijk bestuur": voor een gemeente die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt.

Het in control hebben van informatiebeveiliging is om een aantal redenen noodzakelijk:

- Gegevens- en informatieverwerkende systemen (al dan niet geautomatiseerd) zijn vitale bedrijfsmiddelen voor de gemeente. De gemeente is voor vrijwel al haar processen afhankelijk van informatie; zonder deze ligt vrijwel de gehele gemeentelijke organisatie stil.
- De afhankelijkheid van informatie(technologie) wordt steeds groter: de automatiseringsgraad stijgt nog steeds en informatiesystemen worden steeds meer gekoppeld, zowel binnen de gemeente als tussen gemeenten (zoals DOWR) als tussen de gemeente en ketenpartners. De organisatie werkt hierbij in steeds sterkere mate proces-georiënteerd in plaats van product-georiënteerd (kanteling, ontschotting, horizontalisering). Hierdoor neemt ook de kwetsbaarheid toe.
- De kwetsbaarheid stijgt eveneens doordat (deels als gevolg van rijksbeleid, deels door eigen keuzes) steeds meer informatiesystemen toegankelijk worden voor de 'buitenwereld'; bijvoorbeeld internet, netwerken, samenwerkingsverbanden, telewerken, draadloze verbindingen. Het Nieuwe Werken en thuiswerken brengen ook grotere risico''s met zich mee. De complexiteit en de dynamiek van de omgeving nemen nog steeds toe.
- De gemeente is beheerder van veel privacygevoelige (persoon)gegevens en andere informatie van haar inwoners, bedrijven/organisaties, medewerkers en anderen. Uit een recent onderzoek van het College Bescherming Persoonsgegevens (CBP) blijkt dat veel gemeenten niet voldoen aan de minimumeisen die de wet Persoonsregistraties stelt. Uit de uitgevoerde analyse blijkt helaas dat Deventer hierop geen uitzondering vormt.
- In toenemende mate worden in wet- en regelgeving[3] bindende resultaatverplichtingen tot een passend niveau van informatiebeveiliging opgenomen – waarbij de lat voor het begrip 'passend' steeds hoger komt te liggen, omdat de technologische mogelijkheden toenemen.
- Rampen (brand, overstroming), menselijk falen, virussen, vandalisme, miscommunicatie, technische storingen e.d. maar ook de toenemende dynamiek en complexiteit van de omgeving waarin de gemeente zich bevindt zijn mogelijke bedreigingen, die niet alleen in aantal maar ook in omvang toenemen.

[2] Met een ezelsbruggetje zijn deze aspecten bekend als CIA: confidentiality, integrity & availability.
[3] Bijvoorbeeld WBP, Wet GBA, WOB, Archiefwet, Auteurswet, Wet Computercriminaliteit, Suwinet, EU-richtlijnen maar ook accountancy-eisen.

- Het op orde hebben van informatiebeveiliging is een voorwaarde voor het bereiken van OO fase 3 (voorheen INK-3) en voor de ambities van de gemeente op de onderdelen dienstverlening en kwaliteitsverbetering.
- Deventer gaat steeds meer ICT- en andere diensten verrichten voor buurgemeenten (zoals de DOWR-samenwerkingen). Bij het leveren van diensten aan externe partijen zullen zaken als continuïteit, integriteit, exclusiviteit en beschikbaarheid aantoonbaar geborgd moeten zijn.

Al deze bedreigingen kunnen van invloed zijn op de vertrouwelijkheid, integriteit en continuïteit van de informatie binnen de gemeente. Het is daarom van groot belang om maatregelen te treffen om deze bedreigingen, die een grote impact kunnen hebben op de continuïteit van de bedrijfsvoering van de gemeente dan wel op de integriteit of vertrouwelijkheid van gegevens te voorkomen of te minimaliseren.

1.2 Reikwijdte en afbakening informatiebeveiliging

-Informatiebeveiliging betreft niet alleen ICT, computers en automatisering, maar is veel breder. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen), alle mogelijke informatiedrager (ether, papier, elektronisch, magnetisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatieverwerkende middelen/systemen: de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen en vooral ook mensen en processen. Studies leren dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en tekort schietende organisatie.
-De baseline geldt voor de gehele organisatie, voor alle processen, organisatieonderdelen, objecten en gegevens(verzamelingen).

-Informatiebeveiliging is geen apart specialisme, maar een integraal onderdeel van de bedrijfsprocessen, en daarmee ook een (management)verantwoordelijkheid voor de proceseigenaar.
-Een 100% informatiebeveiliging is niet mogelijk. Niet alleen kunnen en zullen er steeds weer nieuwe risico's ontstaan, ook leidt volledig afdichten van alle risico's – dus maximale beveiliging – tot een ondoelmatige situatie waarin de kosten voor de bedrijfsvoering te hoog worden. Optimale beveiliging is het bij alle risico's vinden van een balans tussen beveiliging en bedrijfsvoering; tussen kosten en baten. Informatiebeveiliging is in die zin te beschouwen als risicomanagement, waarbij: risico = (kans x schade). Er zal altijd een restrisico overblijven; de kunst is echter om daarin bewust keuzes te maken.
-Alle informatie is vrij beschikbaar, tenzij er wettelijke belemmeringen zijn in het kader van privacy, vertrouwelijkheid, veiligheid en auteursrechten; of indien het economische of financiële belang van de organisatie of van anderen onnodig wordt geschaad.

1.3 Probleemstelling

- De gemeente Deventer heeft onvoldoende inzicht in de beveiliging van informatie. Er zijn uiteraard op diverse terreinen (meestal niet gedocumenteerde) maatregelen getroffen, echter, voor de meeste processen en informatiesystemen geldt dat een systematische analyse van de te beveiligen processen en/of gegevens en mogelijke risico's ontbreekt.
- Het is hierdoor niet duidelijk of processen/gegevens voldoende beveiligd zijn, en evenmin of de juiste balans bestaat tussen de afhankelijkheid die de gemeente kent ten aanzien van de (geautomatiseerde) informatievoorziening en de kwetsbaarheden (risico's) die aanwezig zijn.
- Verder maakt Informatiebeveiliging onvoldoende deel uit van de bedrijfsvoeringprocessen en/of kwaliteitsprocedures binnen de organisatie.
- Het bewustzijn van het belang van informatiebeveiliging binnen de organisatie is onvoldoende.

1.4 Doelstelling en beoogd resultaat

Met dit project worden de vastgestelde beleidsuitgangspunten op het gebied van informatiebeveiliging voor de gemeentelijke organisatie nader uitgewerkt, resulterend in een 'baseline' informatiebeveiligingsplan voor de gemeentelijke organisatie. Hierin zijn niet alleen de vastgestelde beleidsuitgangspunten voor informatiebeveiliging nader uitgewerkt, maar worden ook (minimum) beveiligingseisen en -maatregelen opgenomen die gemeentebreed voor alle processen en systemen gelden. Een onderdeel hiervan zijn beheermaatregelen, waarmee de verantwoordelijkheden voor informatiebeveiliging binnen de gemeentelijke organisatie worden belegd en informatiebeveiliging

wordt ingebed in de reguliere planning- & controlcyclus (PDCA) binnen de (kwaliteitshandhaving van de) bedrijfsvoeringsprocessen.

Een bijkomend doel van het project is het vergroten van de bewustwording voor het belang van informatiebeveiliging en het creëren van draagvlak voor informatiebeveiliging en informatiebeveiligingsmaatregelen in de gemeentelijke organisatie.
Het uiteindelijke doel is te komen tot een hoger niveau van informatiebeveiliging; het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade voor de gemeente door het trachten te voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

1.5 Aanpak

Het informatiebeveiligingsplan plan beschrijft het basis beveiligingsniveau dat geldt voor de gehele gemeentelijke organisatie.

Hiervoor is een analyse gemaakt van aanwezig beleid / beschikbare stukken inzake informatiebeveiliging; inclusief externe (bijvoorbeeld wettelijke) eisen. In de praktijk bleek binnen de organisatie overigens weinig geformaliseerd en gedocumenteerd te zijn.

Voor de totstandkoming van het informatiebeveiligingsplan zijn verder diverse workshops gehouden en gesprekken gevoerd met deskundigen en (proces)verantwoordelijken. Een deel van de gesprekken met leden van het team ICT is gevoerd door externen van Getronics. Voor de workshops is het beleidsterrein opgeknipt in relatief afgebakende deelgebieden. Omdat de aandachtsgebieden die het plan bestrijkt (ICT, gegevensbeheer, financieel en administratie, documentmanagement, juridische zaken, personeel en organisatie en facilitaire zaken) voornamelijk zijn belegd bij de (v/h) eenheid Bedrijfsvoering hebben met name vanuit deze eenheid deskundigen deelgenomen aan de workshops. Hierbij is niet alleen gekeken naar de situatie binnen het eigen team of de eenheid, maar ook gebruik gemaakt van de aanwezige kennis vanuit de ondersteunende diensten van de organisatie als geheel.

De workshops zijn gebruikt om een beeld te krijgen van de risico's die bestaan op het betreffende deelgebied, en om een beeld te krijgen van de ter beheersing van risico's al getroffen maatregelen. Ter voorbereiding op de workshops is een gezamenlijke bijeenkomst gehouden met de deelnemers aan de verschillende workshops. Dit om bewustwording voor het onderwerp te creëren en alvast het denkproces over het eigen deelproces op gang te brengen.
Net zoals bij de B&W nota uit 2007 is de Code voor Informatiebeveiliging[4] gebruikt als gemeenschappelijke basis voor het ontwikkelen van beveiligingsnormen en als kader voor te nemen maatregelen. De uitkomsten van de workshops (de bestaande situatie) zijn afgezet tegen het gehanteerde normenkader uit de Code voor Informatiebeveiliging. De gebundelde uitkomsten van de workshops hebben geresulteerd in het informatiebeveiligingsplan en de aanbevelingen met betrekking tot te nemen maatregelen.

Er is niet gestreefd naar volledigheid, maar naar het in kaart brengen van de belangrijkste, zichtbare risico's. Hiermee wordt een proces in gang gezet, waarmee door periodieke analyses steeds meer risico's in beeld worden gebracht en zo nodig afgedicht.

1.6 Vervolg

Met dit project wordt een basis gelegd voor het doen toenemen van de mate van informatiebeveiliging. Maar met deze nota en met het uitvoeren van de voorgestelde maatregelen is het onderwerp "informatiebeveiliging" echter nog niet af. De opgestelde baselinebeveiliging is het begin van een proces; niet het eindpunt.

Verder geldt voor informatiebeveiliging in zeer sterke mate dat beleid alleen niet voldoende is; zonder verankering in de praktijk van dagelijks handelen neemt het beveiligingsniveau niet toe.

1.6.1 Cyclisch proces

Met de hier voorgestelde maatregelen komt informatiebeveiliging op een hoger niveau. Echter, informatiebeveiliging is geen absoluut, statisch gegeven. Het is in feite risicomanagement, waarbij de mate van beveiliging de resultante is van een proces van risicoafwegingen.

[4] NEN-ISO/IEC 27001, uitgave 2007, een algemeen aanvaard standaardwerk met normen en best practices op het gebied van informatiebeveiliging.

Informatiebeveiliging is hierbij nooit ‘af’, en moet worden gezien als een cyclisch proces, als een activiteit die steeds weer terugkeert, omdat:
- er steeds weer nieuwe risico’s ontstaan;
- er nieuwe technieken ontstaan om risico’s af te dichten;
-omdat niet alles tegelijk kan; het implementeren van maatregelen kost tijd (en soms geld) en kan beter worden gespreid;
-bewustwording en bewust blijven van mogelijke risico’s van het grootste belang is; een veranderproces dat lange tijd nodig zal hebben.

Door het vergroten van het bewustzijn en het expliciet verankeren in de bedrijfsvoeringsprocessen wordt dit cyclische proces gestart, waarmee de organisatie op een stijgende lijn van veiligheid komt. Dit beveiligingsplan moet hierbij worden gezien als een eerste aanzet.

De baseline informatiebeveiliging wordt vastgelegd voor de periode 2011-2014 en wordt jaarlijks bijgesteld aan de hand van actuele ontwikkelingen en de operationele stand van zaken. Het is aldus een ‘levend document’, dat periodiek tegen het licht zal worden gehouden en zal worden bijgesteld.

1.6.2 Bewustwording

De meeste incidenten op het gebied van informatiebeveiliging komen niet van kwaadwillende hackers, gemaskerde inbrekers of falende computersystemen.
De meeste incidenten ontstaan door menselijke fouten, van onze eigen medewerkers, veelal ingegeven door onwetendheid. Doorgaans doordat mensen er niet bij stil staan dat hun handelen (of het nalaten daarvan) invloed kan hebben op de beschikbaarheid, vertrouwelijkheid of betrouwbaarheid van informatie, kortom op informatiebeveiliging.

Een goed ‘papieren’ beleid biedt hierbij geen enkele beveiliging, wanneer dit in de praktijk niet wordt nageleefd omdat de mensen het belang er onvoldoende van inzien.
Enkele voorbeelden:
-Onze computersystemen zijn met individuele wachtwoorden en complexe autorisatiesystemen beveiligd, maar de praktijk leert dat de meeste mensen de wachtwoorden op gele briefjes schrijven en deze bij de PC opplakken.
-De buitendeuren zijn voorzien van goede sloten en een pasjessysteem, maar wanneer iemand met een medewerker mee loopt naar binnen, dan wordt netjes de deur open gehouden – zelfs al kennen we de persoon niet.
-De kantoren staan vol afsluitbare kasten, maar toch liggen de bureaus vol met vertrouwelijke informatie.
-Alle printers kennen een functie ‘beveiligd afdrukken’, maar toch liggen er stapels vertrouwelijke, niet beveiligd afgedrukte printjes naast, die veelal niet eens worden opgehaald.

Informatiebeveiliging moet worden verankerd in bewust handelen in de dagelijkse praktijk, zodat mensen zich realiseren welke risico’s er zijn.
Het creëren van bewustwording en draagvlak is dan ook noodzakelijk.

1.6.3 Fase 3

Met dit project is een baseline-informatiebeveiligingsplan opgesteld, met daarin basis eisen op het gebied van informatiebeveiliging voor de gehele organisatie; alle processen, onderdelen en medewerkers.

In fase 3 van het ‘traject Informatiebeveiliging’ zal hierop worden voortgeborduurd. Voor die processen, informatiesystemen of organisatieonderdelen waar de baseline-beveiliging niet voldoende is, zullen aanvullende risico-analyses (afhankelijkheids- en kwetsbaarheidsanalyses) worden uitgevoerd, waarna een kosten/batenafweging resulteert in een verbeterplan met maatregelen: een beveiligingsplan.

Daarnaast zal een traject gericht op het vergroten van de bewustwording worden gestart.

2 Conclusies

In dit hoofdstuk worden kort de belangrijkste conclusies weergegeven zoals die uit de in de hoofdstukken 4 – 15 gepresenteerde analyse naar voren komen.

Organisatie, beleid en beheer

- Informatiebeveiliging is niet iets waar de organisatie zich actief mee bezig houdt.
- Voor het grootste deel van de organisatie bestaat er onvoldoende inzicht in welke informatie aanwezig is en in hoeverre deze beveiligd dient te worden.
- Er is binnen de gemeentelijke organisatie weinig op het gebied van informatiebeveiliging expliciet vastgelegd. Het coördineren, vormgeven en uitwerken van rollen en verantwoordelijkheden voor de informatiebeveiliging in de lijn en alle lagen van de organisatie is onvoldoende. Ook ontbreken eisen met betrekking tot het rapporteren en omgaan met incidenten, en is er onvoldoende geregeld inzake scholing, training, bewustwording en de gevolgen met betrekking tot het niet naleven van beleid. Het beoordelen en toetsen van het informatiebeveiligingsbeleid is niet vastgelegd.
- Hierdoor is onvoldoende inzicht in de risico's die de organisatie loopt, en zijn er geen mechanismen om dit tekort op te vangen; om te komen tot het structureel uitvoeren en borgen van beheersmaatregelen.
- Deventer hanteert als uitgangspunt voor het toedelen van verantwoordelijkheden binnen de organisatie het principe van integraal management. Dit houdt onder meer in dat alle teamleiders / procesverantwoordelijken integraal verantwoordelijk zijn voor alle bedrijfsvoeringsprocessen binnen het eigen gebied, zoals P&O, informatiemanagement, documentmanagement, juridische zaken maar ook informatiebeveiliging. Er is met uitzondering van het financiële domein op de verschillende aspecten van informatiebeveiliging geen traditie van gemeentebrede voorschriften of van control vanuit een centrale eenheid. Richtlijnen op het gebied van informatiebeveiliging ontbreken grotendeels, of nemen de vorm aan van adviezen - met bijbehorende keuzevrijheid. In advisering vanuit de teams binnen bedrijfsvoering wordt incidenteel aandacht besteed aan informatiebeveiliging.
  Dit maakt dat het niveau van informatiebeveiliging sterk afhangt van de mate waarin de individuele teamleiders en procesverantwoordelijken er aandacht aan besteden of zich zelfs maar bewust zijn van eventuele risico's die worden gelopen.
- Er zijn grote verschillen te constateren tussen de verschillende teams binnen de organisatie (zowel binnen de primaire als binnen de ondersteunende processen) en de mate waarin informatiebeveiliging 'op de agenda' staat. In de meeste gevallen is men zich onvoldoende bewust van het verschijnsel, en van de risico's die gelopen worden. Ook bestaande wettelijke voorschriften zijn in veel gevallen onbekend, en daarmee ook vaak de naleving van de voorschriften.
- De meeste input voor deze baseline is afkomstig vanuit de ondersteunende teams binnen Bedrijfsvoering (BV). Binnen BV hebben de teams het onderwerp informatiebeveiliging binnen het eigen verantwoordelijkheidsgebied redelijk onder controle. Binnen de teams is een significant verschil in de mate waarin men zich verantwoordelijk voelt voor dan wel betrokken acht bij informatiebeveiliging binnen de rest van de organisatie. Binnen bepaalde teams leeft dit sterk, binnen andere is de opstelling meer een faciliterende: alleen bij een expliciete vraag wordt er geleverd.
- De informatiebeveiliging onder verantwoordelijkheid van de teams ICT-beheer en DM voldoet adequaat aan de vigerende regelgeving en de Code voor Informatiebeveiliging. Het niveau van informatiebeveiliging van de aandachtgebieden ICT en documentair in de rest van de organisatie verschilt sterk, en is vaak te laag.

Personeel en externen

- Informatiebeveiligingsaspecten maken standaard geen deel uit van het personeelsbeleid (aanname, tijdens dienstverband, uit dienst gaan.) Dit geldt ook voor cont(r)acten met externen.
- Medewerkers krijgen geen training of voorlichting en de mate van bewust zijn van informatie-beveiliging is in de meeste gevallen laag.

- De meeste incidenten op het gebied van informatie beveiliging ontstaan door menselijke fouten van onze eigen medewerkers, veelal ingegeven door onwetendheid. Door dit tekortschietend besef van de mogelijke gevolgen neemt het risico van menselijk falen toe.
- Er is geen formeel disciplinair proces vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

Fysiek en toegang

- Hoewel bij toegang tot de panden van een systeem met toegangspasjes gebruik wordt gemaakt is de praktijk dat het voor buitenstaanders relatief gemakkelijk is om ongemerkt toegang te krijgen tot de gebouwen van de gemeente. Bezoekers en eigen personeel zijn niet als zodanig te herkennen. De receptiefunctie is niet adequaat geregeld.
- Basisvoorzieningen tegen inbraak en voor branddetectie zijn aanwezig.
- De centrale ICT-voorzieningen zijn adequaat beveiligd.
- Er zijn geen regels gesteld of voorzieningen getroffen voor het werken thuis of extra beveiliging zoals encryptie op mobiele apparatuur.
- Clean desk en clear screen worden slechts sporadisch toegepast.

Bediening en autorisaties

- Documentatie over bediening, functionaliteiten en/of wijzigingen van applicaties ontbreken in veel gevallen. De toegang tot applicaties en het beheer van autorisaties is onvoldoende geregeld.
- Er wordt slechts zeer beperkt gewerkt met SLA's.
- Wachtwoorden voor de toegang tot applicaties worden veelvuldig opgeschreven en bewaard in de nabijheid van de PC. Ook worden wachtwoorden voor bepaalde applicaties gedeeld door meerdere gebruikers. Soms worden persoonlijke wachtwoorden door medewerkers ter beschikking gesteld aan anderen.
- De schermbeveiliging op de PC's wordt weinig gebruikt.

Incidenten en continuïteit

- Er is geen procedure voor het vastleggen en rapporteren van beveiligingsincidenten, en in de praktijk gebeurt dit ook maar zelden.
- De gemeente kent fragmentarisch continuïteitsmaatregelen of –plannen. Het proces is niet geborgd en continuïteit wordt niet getest.

Naleving

- Er is geen overzicht van relevante regelgeving en verplichtingen vastgelegd. Dit geldt zo wel voor de organisatie als geheel als voor informatiesystemen.
- Er zijn geen procedures ten aanzien van het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten.
- Er zijn weinig tot geen organisatiebrede voorschriften of richtlijnen over het omgaan met relevante regelgeving.
- De gemeente voldoet in grote lijnen aan de eisen zoals deze zijn gesteld in de regelgeving ten aanzien van de officiële archivering, echter, het terugvinden van informatie uit de archiefsystemen en/of de ('onofficiële') werkbestanden is vaak moeizaam daar waar het uitsluitend digitaal vastgelegde informatie betreft.
- De gemeente handelt in de praktijk regelmatig in strijd met de vereisten van de Wet Bescherming Persoonsgegevens (zowel met betrekking tot de eigen medewerkers als ook wat betreft klanten/burgers), de auteurswet of de Wet op de Ondernemingsraden.
- Er zijn geen extra richtlijnen of procedures om naleving op relevante beveiligingsvoorschriften te controleren en/of af te dwingen. Er zijn geen extra audits op het gebied van informatiebeveiliging.

3 Aanbevelingen

Algemeen
Informatiebeveiliging is geen project, maar maakt onderdeel uit van de reguliere bedrijfsvoering. In de huidige werkwijze krijgt het onderwerp echter niet de aandacht die het zou moeten hebben. Daarom wordt een aantal maatregelen voorgesteld om informatiebeveiliging explicieter onderdeel te laten zijn van de reguliere werkzaamheden.

Zoals in hoofdstuk 1 al uiteen is gezet, is er grote winst op het gebied van informatiebeveiliging te behalen door de medewerkers bewust te maken van het belang van informatiebeveiliging. Daarom wordt er een aantal concrete acties die gericht zijn op het bevorderen van dit bewustzijn voorgesteld.

Verder zijn er concrete aanbevelingen om op diverse terreinen beveiligingsrisico's te verminderen.

Ten slotte wordt voor tal van andere, meer gedetailleerde en gespecialiseerde aanbevelingen verwezen naar de analyse in de hoofdstukken hierna.

Bewustwording en voorlichting
- Organiseer bewustwordingsworkshops inzake informatiebeveiliging voor alle medewerkers en het management.
- Maak de grote lijnen van het informatiebeveiligingsbeleid helder en in begrijpbare taal kenbaar maken aan alle medewerkers binnen de gemeente Deventer, bijvoorbeeld door dit als content op te nemen binnen het intranet, het periodiek op te nemen in het werkoverleg van de lijnmanagers, het als onderwerp te laten opnemen in de P&C, teamplannen, enzovoort.
- Richt een teamsite in voor informatiebeveiliging met als doel: gerichte informatie en bewustwording.
- Bepaal eisen met betrekking tot beveiligingsscholing, -training en bewustwording, bijvoorbeeld door het plannen van een jaarlijkse informatiebeveiligingsweek, workshops en periodieke communicatie-uitingen om de bewustwording te vergroten.
- Neem in de teamplannen een onderdeel informatiebeveiliging op, gericht op het jaarlijks uitvoeren van een risicoanalyse met betrekking tot informatiebeveiliging.
- Neem bij het aanstellen van nieuw personeel, informatiebeveiliging expliciet op in het introductieprogramma.
- Stel een beknopt beleidsdocument op waarin in grote lijnen het goedgekeurde beveiligingsbeleid door B&W is opgenomen om kenbaar te maken aan medewerkers en meer in het bijzonder externe partijen, zoals ICT-dienstverleners maar ook andere partijen zoals aannemers of reinigingsbedrijven.
- Besteedt actief aandacht aan het bestaan van beveiligd afdrukken.

Organisatie, beleid en beheer
- Maak informatiebeveiliging meer specifiek en leg het meer expliciet vast, door bijvoorbeeld het rapporteren van beveiligingsincidenten, zowel voor de (decentrale) organisatie / proces-verantwoordelijke waar zich het incident voordoet als ook een centrale rapportage en registratie.
- Neem nadat het organisatiebrede informatiebeveiligingsbeleid vorm heeft gekregen de beoordeling hiervan in de P&C-cyclus op. Neem in de teamplannen een onderdeel informatiebeveiliging op, gericht op het jaarlijks uitvoeren van een risicoanalyse met betrekking tot informatiebeveiliging.
- Besteed bij elke verandering ('change') binnen een proces of team standaard aandacht aan informatiebeveiliging (risico analyse). Dit omvat ten minste het in- en uit stromen van medewerkers of ingehuurde diensten, het afsluiten van contracten, het (de)installeren of aanpassen van informatiesystemen of gegevensverzamelingen.
- Zorg dat in contacten met de organisatie door de adviseurs vanuit Intern Ondersteunen expliciet aandacht wordt gevraagd voor en geadviseerd over informatiebeveiliging.
- Stel formeel - maar vooral feitelijk - een beveiligingscoördinator in binnen het team IAO (Intern Ondersteunen) die vanuit deze rol als aanjager en vraagbaak functioneert voor informatiebeveiliging.

Belast deze beveiligingscoördinator met het uitbrengen van periodieke rapportages binnen de planning & control cyclus over beveiligingsincidenten binnen de organisatie, met de uitvoer van audits binnen de organisatie en met de verantwoordelijkheid voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit de baseline. De beveiligingscoördinator rapporteert periodiek aan het managementteam, zo nodig zonder tussenkomst van het teamhoofd. Onder een beveiligingscoördinator wordt verstaan: een functionaris die kennis en ervaring heeft op het gebied van informatiebeveiliging en op dit terrein een adviserende en coördinerende rol kan vervullen. De beveiligingscoördinator is verantwoordelijk voor:

- Voorbereiding informatiebeveiligingsbeleid en –plan.
- Rapportage (beveiligingsincidenten).
- Het beheer en toezicht op de naleving van de beveiligingsprocedures.
- Het minstens eenmaal per jaar verzorgen van het geven van voorlichting en instructie aan medewerkers door middel van toetsing van de opgestelde beveiligingsprocedures in de praktijk.
- Het introduceren en bekendmaken van nieuwe medewerkers met de beveiligingsprocedures.

Personeel en externen

- Stel een procedure op m.b.t. beëindiging en wijziging dienstverband opstellen waarin aandacht wordt besteed aan de diverse aspecten van informatiebeveiliging.
- Toets functiebeschrijvingen op en pas eventueel aan aan de rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging. Voor nieuw personeel: extra screenen op positieve referenties, correctheid van C.V., bevestiging van professionele kwalificaties, verklaring omtrent het gedrag.
- Schenk in de proefperiode nadrukkelijk aandacht aan de juiste kwalificaties van de medewerker.
- Laat personeel en externen die toegang krijgen tot de panden en/of informatie van de gemeente een verklaring tekenen omtrent het omgaan met te beveiligen informatie.
- Leidt alle medewerkers moeten adequaat op opdat gebruikersfouten tot een minimum worden beperkt. Hierbij dienen de cursussen toegesneden te zijn op de taken van de functionarissen. Medewerkers die werkzaam zijn op gebieden met een verhoogd risico jaarlijks (bij)scholen.
- Expliciteer de gevolgen van het niet naleven van informatiebeveiligingsbeleid, bijvoorbeeld disciplinaire maatregelen, strafrechtelijke procedures, ontslag, aansprakelijkheid, enz.
- Stel een basiscontract op voor de toegang tot de IT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin kaders staan voor de toegang tot IT-voorzieningen door derden.

Fysiek en toegang

- Voer een deugdelijke administratie in voor afgifte, periodieke controle en inname van toegangspasjes.
- Richt bij alle locaties een receptiefunctie in en begeleid bezoekers persoonlijk in en uit de panden.
- Neem het onderwerp informatiebeveiliging expliciet mee bij de eisen die aan het ontwerp voor de nieuwbouw voor de gemeentelijke huisvesting worden gesteld en zo veel mogelijk bij de uit te voeren acties in het kader van het opknappen van de bestaande huisvesting.
- Ga zo veel mogelijk over op digitale archivering i.v.m. fysieke bedreigingen (zoals brand.)
- Voer werken volgens het clean desk-principe in.
- Stel richtlijnen op voor het gebruik van apparatuur buiten het gemeentehuis (thuiswerken of werken op externe locatie).
- Ga bij het vervangen van de printers over op standaard beveiligd afdrukken.

Bediening en autorisaties

- Voorzie alle informatiesystemen met gevoelige of kritieke informatie van logische toegangsbeveiliging.
- Registreer toegangsrechten van medewerkers in systemen en toets periodiek op actualiteit.
- Overweeg het in gebruik nemen van een systeem voor single sign on.
- Zorg voor (het onderhouden van) documentatie met betrekking tot de bediening, functionele specificaties, procedures en wijzigingen van de informatiesystemen.

- Ga per informatiesysteem of proces na of functiescheiding doorgevoerd kan worden en implementeer dit zo nodig.
- Formaliseer het wijzigingsproces, gebruik hiervoor de ITIL best practice als leidraad.
- Start met het opzetten van een SLA voor basis-dienstverlening.
- Voer een clear screen beleid in.
- Stel weer anti-virusbescherming voor thuisgebruik beschikbaar.
- Verbied expliciet het noteren en toegankelijk maken van wachtwoorden en het afstaan van wachtwoorden aan anderen. Communiceer hier actief over richting medewerkers.
- Zorg voor uniforme voorschiften voor het opnemen van informatie in de financiële systemen, communiceer hierover en zorg voor controle en handhaving.

Incidenten en continuïteit

- Stel een beveiligingsincidentmeldingsformulier op waarmee beveiligingsincidenten kunnen worden gemeld en geregistreerd. Stel ze beschikbaar aan de informatiebeveiligingscoördinator.
- Bespreek informatiebeveiligingsincidenten standaard in het teamoverleg van het desbetreffende team.
- Voer per team/proces een risicoanalyse uit gericht op het waarborgen van beschikbaarheid van informatie, waarbij met name ook aandacht wordt besteed aan uitval en vervangbaarheid van medewerkers. Besteed zo nodig aandacht aan proces- en werkbeschrijvingen en onderlinge uitwisselbaarheid.
- Stel voor de hele organisatie een Bedrijfs Continuïteits Plan (BCP) op. Het doel van een BCP is het adequaat kunnen reageren op verstoringen van bedrijfsactiviteiten en het beschermen van kritieke bedrijfsprocessen tegen de effecten van grote storingen of calamiteiten.

Naleving

- Stel voor de organisatie als geheel en voor elk informatiesysteem de relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen expliciet vast en implementeer een procedure om deze actueel te houden.
- Stel een procedure op voor het omgaan met materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.
- Stel een regeling op voor het omgaan met specifiek geadresseerde inkomende post (‘briefgeheim’) en zorg dat deze bekend wordt en gehandhaafd wordt in de gehele keten van postafhandeling.
- Stel een protocol op omtrent het omgaan met persoonsgegevens.
- Stel een protocol op voor het meenemen van informatie naar huis en voor thuiswerken.
- Maak uitsluitend gebruik van software waarvoor een licentieovereenkomst is afgesloten. Controleer dit periodiek.
- Ontdoe informatie die wordt gepubliceerd of wordt verspreid van niet noodzakelijke persoonsgegevens en adresgegevens.
- Voorzie alvorens documenten te publiceren op internet of op intranet deze van de voor het terugvinden benodigde metadata.
- Sta schaduwarchieven (thuis, op kantoor, in the cloud; fysiek of digitaal) met vertrouwelijke informatie niet langer toe.
- Leg voorgenomen besluiten met consequenties voor de privacy van de medewerkers van de gemeente ter instemming voor aan de ondernemingsraad.

Deel 2 – Analyse

4 Analyse baseline informatiebeveiliging

Bij het opstellen van het baseline informatiebeveiligingsplan is gebruik gemaakt van een methodiek gebaseerd op de A&K-analyse (Afhankelijkheids- en Kwetsbaarheidsanalyse), waarbij de gebieden waarvoor beleidsuitgangspunten zijn vastgesteld als leidraad worden gehanteerd.

De meeste informatie is verkregen in een aantal workshops met sleutelfiguren, zoals functioneel beheerders, (verantwoordelijke) teammanagers en andere medewerkers. Verder is de (beperkt) aanwezige schriftelijke informatie geanalyseerd.

Er is niet gestreefd naar volledigheid, maar naar het in kaart brengen van de belangrijkste, zichtbare risico's. Zoals in hoofdstuk 1 al is gememoreerd wordt hiermee een proces in gang gezet, waarmee door periodieke analyses steeds meer risico's in beeld worden gebracht en zo nodig afgedicht.

De aandachtsgebieden komen uit de Code voor Informatiebeveiliging van het Nederlands Normalisatie Instituut ((NEN-ISO/IEC 27001), uitgave 2007, een algemeen aanvaard standaardwerk met normen en best practices op het gebied van informatiebeveiliging.

Deze norm bevat 11 hoofdstukken met beveiligingsbeheersmaatregelen, die gezamenlijk 39 hoofdbeveiligingscategorieën omvatten, met in totaal meer dan 500 items. Deze zijn niet allemaal relevant voor de Deventer gemeentelijke organisatie. Daar waar er geen of nauwelijks relevantie is, zijn de betreffende paragrafen uit de norm niet vertaald naar de Deventer situatie.

De elf hoofdstukken zijn:

1. beveiligingsbeleid;
2. organisatie van de informatiebeveiliging;
3. beheer van bedrijfsmiddelen;
4. personele beveiligingseisen;
5. fysieke beveiliging en beveiliging van de omgeving;
6. beheer van communicatie- en bedieningsprocessen;
7. toegangsbeveiliging;
8. aanschaf, ontwikkeling en onderhoud van informatiesystemen;
9. beheersen van informatiebeveiligingsincidenten;
10. beheerproces bedrijfscontinuïteit;
11. naleving.

Deze worden hier achtereenvolgend behandeld. Elk van de paragrafen bevat:

1. een beheersdoelstelling die vermeldt wat er moet worden bereikt;
2. één of meer beheersmaatregelen die kunnen worden toegepast om het doel te kunnen bereiken;
3. de feitelijke situatie binnen de gemeente Deventer;
4. de risico's die bestaan (confrontatie 3 met 2);
5. voorgestelde acties om de risico's te beperken.

5 Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

Doelstelling:

Directie richting en ondersteuning bieden voor informatiebeveiliging overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften. De directie behoort een duidelijke beleidsrichting aan te geven in overeenstemming met de bedrijfsdoelstellingen en te demonstreren dat het informatiebeveiliging ondersteunt en zich hiertoe verplicht, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid voor de hele organisatie.

Beheersmaatregelen

- Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.
- Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

Feitelijke situatie gemeente Deventer

In de Nota Informatiebeveiliging, zoals vastgesteld door B&W op 10 juli 2007, is de aanzet gegeven voor meer gedetailleerde beleidsdocumenten inzake informatiebeveiliging. Deze baseline informatiebeveiliging vormt daarop een eerste aanvulling. Met de vaststelling van de Nota Informatiebeveiliging is een begin gemaakt met de implementatierichtlijnen van de NEN-ISO/IEC 27002:2007. Echter het huidige beleid omvat niet:

- eisen met betrekking tot scholing, training, bewustwording,
- het vermelden van specifieke verantwoordelijkheden (zoals rapporteren over beveiligingsincidenten),
- de gevolgen van het niet naleven van het beleid,
- een heldere samenvatting in heldere, begrijpbare taal voor alle medewerkers.

Met uitzondering van de extern gedreven audits, zoals de GBA-audit, is het beoordelen en toetsen van het informatiebeveiligingsbeleid nog niet vastgelegd. De vastgestelde Nota informatiebeveiligingsbeleid voorziet wel in het periodiek evalueren en bijstellen maar dit is nog niet opgenomen in de P&C-cyclus.

De meeste beleidsuitgangspunten uit de nota moeten nog geïmplementeerd worden.

Risico's

De risico's voor het niet vastleggen van een aantal implementatierichtlijnen voor beleidsdocumenten voor informatiebeveiliging, in het bijzonder de hierboven vermelde omissies, is dat de bedreigingen van menselijk falen en menselijke aard toe kunnen nemen. Bewustwording, adequate scholing en training, maar ook de wetenschap dat onjuist handelen ook consequenties kan hebben voor het individu, zijn mechanismes die deze dreigingen bestrijden. Een adequate verankering in beleid en goede communicatie hierover is belangrijk en de relatief lage kosten die hiermee gemoeid zijn, wegen goed op tegen de baten.

De ambities op het gebied van OO-fase 3 (systeem georiënteerd) vereisen een periodieke beoordeling en verbetering van beleid. De ontwikkelingen op gebied van technologie, wet- en regelgeving, basisregistraties en de interne veranderingen binnen de gemeentelijke organisatie hebben invloed op het informatiebeveiligingsbeleid. Het niet beoordelen en bijstellen van het informatiebeveiligingsbeleid kan leiden toe extra risico's in de volle breedte van de bedreigingen en negatieve invloed hebben op de beschikbaarheid, de integriteit en vertrouwelijkheid van informatie. De kosten van de beoordeling kunnen significant zijn, veroorzaakt door het aanwenden van interne en externe expertise. Het expliciet toewijzen van een eigenaar om de periodiciteit en omvang van de beoordeling te bepalen, is derhalve noodzakelijk om niet onnodige kosten te maken.

Acties

- Meer specifiek en expliciet opnemen van de verantwoordelijkheden van informatiebeveiliging, waaronder het rapporteren van beveiligingsincidenten, zowel voor de (decentrale) organisatie / procesverantwoordelijke waar zich het incident voordoet als ook een centrale rapportage en registratie.
- Het opnemen van eisen met betrekking tot beveiligingsscholing, -training en bewustwording, bijvoorbeeld door het plannen van een jaarlijkse informatiebeveiligingsweek, workshops en periodieke communicatie uitingen om de bewustwording te vergroten.
- De gevolgen van het niet naleven van informatiebeveiligingsbeleid expliciteren, bijvoorbeeld disciplinaire maatregelen, strafrechtelijke procedures, ontslag, aansprakelijkheid, enzovoort.
- De grote lijnen van het informatiebeveiligingsbeleid helder en in begrijpbare taal kenbaar maken aan alle medewerkers binnen de gemeente Deventer, bijvoorbeeld door dit als content op te nemen binnen het intranet, het periodiek opnemen in het werkoverleg van de lijnmanagers, het als onderwerp te laten opnemen in de P&C, teamplannen, enz.
- Een beknopt beleidsdocument opstellen waarin in grote lijnen het goedgekeurde beveiligingsbeleid door B&W is opgenomen om kenbaar te maken aan medewerkers en meer in het bijzonder externe partijen, zoals ICT-dienstverleners maar ook andere partijen zoals aannemers, en reinigingsbedrijven.
- Nadat het organisatiebrede informatiebeveiligingsbeleid vorm heeft gekregen de beoordeling hiervan in de P&C-cyclus opnemen.
- Binnen IAO (Intern Ondersteunen) een beveiligingscoördinator instellen die belast wordt met periodieke rapportages binnen de planning & control cyclus over beveiligingsincidenten binnen de organisatie en die audits uitvoert binnen de organisatie.
- In de teamplannen een onderdeel informatiebeveiliging opnemen, gericht op het jaarlijks uitvoeren van een risicoanalyse met betrekking tot informatiebeveiliging.
- Bij elke verandering (‘change’) binnen een proces of team standaard aandacht besteden aan informatiebeveiliging(risico analyse). Dit omvat ten minste het in- en uit stromen van medewerkers of ingehuurde diensten, het afsluiten van contracten, het (de)installeren of aanpassen van informatiesystemen of gegevensverzamelingen.

6 Organisatie van de informatiebeveiliging

6.1 Interne organisatie

Doelstelling:

Beheren van de informatiebeveiliging binnen de organisatie.

Er behoort een beheerkader te worden vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.

De directie behoort het informatiebeveiligingsbeleid goed te keuren, beveiligingsrollen toe te wijzen en de implementatie van de beveiliging binnen de organisatie te coördineren en te beoordelen.

Indien nodig behoort binnen de organisatie een bron van deskundig advies voor informatiebeveiliging te worden aangewezen en beschikbaar gesteld. Er behoort contact te worden gelegd met externe beveiligingsspecialisten of -groepen, waaronder de relevante autoriteiten, zodat men op de hoogte blijft van industriële trends, normen en beoordelingsmethoden en er geschikte contactpersonen aanwezig zijn in geval van informatiebeveiligingsincidenten. Het verdient aanbeveling de informatiebeveiliging multidisciplinair te benaderen.

Beheersmaatregelen

- De directie behoort actief beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.
- Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies.
- Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.
- Er behoort een goedkeuringsproces voor nieuwe IT-voorzieningen te worden vastgesteld en geïmplementeerd.
- Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.
- Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.
- Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.
- De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheersdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging.

Feitelijke situatie gemeente Deventer

Het college heeft de verantwoordelijkheid voor informatiebeveiliging belegd in de lijnorganisatie, in lijn met het beginsel van integraal management. Het expliciet coördineren, vormgeven en uitwerken van rollen en verantwoordelijkheden voor de informatiebeveiliging in de lijn en andere lagen van de organisatie is echter onvoldoende. De verantwoordelijkheid wordt in veel gevallen niet gevoeld en opgepakt.

Het goedkeuringsproces voor nieuwe IT-voorzieningen is vastgesteld, en verloopt via een regiegroep informatisering en (change)coördinatoren binnen ICT-beheer. Het changemanagementproces voor ICT-voorzieningen is op werkinstructieniveau vastgelegd. In deze procedures zijn informatiebeveiligingaspecten niet expliciet opgenomen.

Contacten met andere overheidsorganisaties en/of ketenpartners worden niet structureel onderhouden om elkaar bij informatiebeveiligingsincidenten tijdig en juist te informeren om adequaat actie te kunnen ondernemen.

Medewerkers onderhouden geen structurele contacten met speciale belangengroepen inzake informatiebeveiliging om te waarborgen dat kennis over vakgebied informatiebeveiliging volledig en actueel blijft (m.u.v. specifieke software producten zoals Microsoft software).

Er vindt geen systematische beoordeling plaats van de doelmatigheid van de implementatie van het informatiebeveiligingsbeleid.

Er wordt niet systematische aandacht besteed aan eisen van vertrouwelijkheid en geheimhouding.

Er vinden geen onafhankelijke interne of externe beoordelingen plaats met betrekking de informatiebeveiliging, met uitzondering van de expliciet voorgeschreven wettelijke GBA-audit.

Risico's
Het niet expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, levert een verhoogd risico op met betrekking tot het daadwerkelijke en structureel uitvoeren en borgen van de beheersmaatregelen.

Acties
- Om zorg te dragen voor een jaarlijkse evaluatie en bijstelling van onderhavige baseline is het noodzakelijk de rol van informatiebeveiligingscoördinator in te stellen. Deze heeft de verantwoordelijkheid toe te zien op naleving van de informatiebeveiligingsmaatregelen en –procedures zoals onder andere uitgewerkt in deze baseline.
- De eisen voor vertrouwelijkheid of geheimhoudingsovereenkomsten dienen te worden vastgelegd en regelmatig (juridisch) te worden beoordeeld. Het gaat hierbij onder meer om classificaties en definities van vertrouwelijkheid, eigendom van informatie, het recht om activiteiten te auditen en te controleren en de te verwachten handelingen die moeten/kunnen worden ondernomen bij inbreuk op de overeenkomsten.
- Het is zinvol lid te worden van bijvoorbeeld het Platform van Informatiebeveiliging (PvIB) om op de hoogte te blijven van ontwikkelingen op het gebied van informatiebeveiliging. Ook biedt GovCert, het computer emergency response team van de overheid, verschillende zinvolle diensten
- Het is belangrijk regelmatig contact te houden met ketenpartners (en deze contacten te registreren) om bij informatiebeveiligingsincidenten tijdig de relevante externe partijen te informeren. Hiervoor dient een overzicht te worden opgesteld, mede in overleg met de functioneel beheerders, met welke externe partijen contact dient worden opgenomen en wie de contactpersonen hiervoor zijn.
- Het is belangrijk de beoordeling van de informatiebeveiliging periodiek (bijvoorbeeld 2-jaarlijks) door een onafhankelijke organisatie uit te laten voeren, bijvoorbeeld een peer-to-peer beoordeling door een andere gemeente uit te laten voeren of door een commerciële organisatie.
- Het is belangrijk binnen de huidige procedures, werkinstructie en checklisten van het change management proces (zowel met betrekking tot ICT-wijzigingen als ook personele en organisatorische wijzigingen) meer expliciet informatiebeveiligingsaspecten op te nemen. Er dient een risicoanalyse op de aspecten beschikbaarheid, betrouwbaarheid en vertrouwelijkheid te worden uitgevoerd.

6.2 Externe partijen

Doelstelling

Beveiligen van de informatie en IT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

De beveiliging van de informatie en IT-voorzieningen van de organisatie behoort niet te worden verminderd door het invoeren van producten of diensten van externe partijen.

Elke toegang tot de IT-voorzieningen en het verwerken en communiceren van informatie door externe partijen behoort te worden beheerst.

Waar het zakelijk gezien onvermijdelijk is om met externe partijen te werken die toegang nodig kunnen hebben tot de informatie en IT-voorzieningen van de organisatie, of voor het verkrijgen of leveren van een product en dienst van of aan een externe partij, behoort een risicobeoordeling te worden uitgevoerd om de beveiligingsimplicaties en de beheersmaatregelen te bepalen. Over deze beheersmaatregelen behoort overeenstemming te worden bereikt en ze behoren te worden vastgelegd in een overeenkomst met de externe partij.

Beheersmaatregelen

- De risico's voor de informatie en IT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.
- Alle geïdentificeerde beveiligingseisen behoren te worden behandeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.
- In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.

Feitelijke situatie gemeente Deventer

Er zijn geen regels gesteld omtrent informatiebeveiliging en externe partijen. De wijze waarop hier mee om wordt gegaan, verschilt sterk binnen de organisatie.

Externe partijen worden niet gescreend met betrekking tot informatiebeveiligingsrisico's.

De contracten met externe partijen en personen omvatten geen specifieke aspecten met betrekking tot informatiebeveiliging. Service Level Agreements (SLA) of Dossiers van Afspraken (DAB) met betrekking tot vertrouwelijkheid, integriteit of continuïteit komen slechts sporadisch voor. Binnen het centrale ICT-domein omvatten de contracten juridische aansprakelijkheidsaspecten en zijn vaak afgesloten met een vast leveranciersbestand.

Externe partijen of personen krijgen slechts in beperkte gevallen instructies op het gebied van informatiebeveiliging.

Risico's

De dreiging met betrekking tot externe partijen is aanwezig en dient daarom adequaat te worden beperkt met passende maatregelen. De bedreigingen zijn relevant voor zowel de aspecten vertrouwelijkheid als integriteit als ook met betrekking tot de continuïteit van de te leveren service. Het is belangrijk de juridische en financiële gevolgen van falen door en bedreigingen van externen af te dekken. Omdat de maatregelen vooral te zoeken zijn op gebieden van contracten en procedures zijn de kosten om dit af te dekken relatief laag en bestrijden de dreiging adequaat.

Acties

- In contracten met externe partijen worden relevante informatiebeveiligingseisen (vertrouwelijkheid, integriteit, continuïteit) opgenomen.
- Het extern personeel dat toegang verkrijgt tot systemen dient te zijn geregistreerd en autorisatie dient te worden geverifieerd in overleg met de betreffende leveranciers, waaronder ook tijdelijk personeel, stagiaires en andere kortlopende aanstellingen.
- Extern personeel krijgt instructies op het gebied van informatiebeveiliging en tekent alvorens voor de gemeente werkzaamheden te verrichten een geheimhoudingsverklaring.
- Het is aan te bevelen een risicobeoordeling uit te voeren voor domeinspecifieke informatiesystemen voor de toegang door leveranciers, door de functioneel beheerders van deze systemen in overleg met Inkoop en IAO / ICT-beheer.
- Er dienen werkvoorschriften en procedures te worden opgesteld om informatiebeveiligingsincidenten en potentiële schade af te handelen en de voorwaarden waaronder in geval van incidenten de toegang door externen kan worden voorgezet.

7 Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstellingen

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

Alle bedrijfsmiddelen behoren te zijn verantwoord en aan een 'eigenaar' te zijn toegewezen.
Voor alle bedrijfsmiddelen behoort een eigenaar bekend te zijn en er behoort te worden vastgelegd wie verantwoordelijk is voor het handhaven van geschikte beheersmaatregelen. De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.

Beheersmaatregelen:

- Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.
- Alle informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen behoren aan een 'eigenaar' te zijn toegewezen in de vorm van een aangewezen deel van de organisatie.
- Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen.

Feitelijke situatie gemeente Deventer

Er zijn verschillende typen bedrijfsmiddelen, waaronder gegevens, programmatuur, apparatuur, diensten, en mensen.

Bij ICT-beheer wordt een CMDB (configuratiemanagement database) gebruikt waarin de relevante *hardware configuration items* staan vermeld. Tevens wordt een spreadsheet bij gehouden met daarin de door ICT-beheer op de centrale systemen geïnstalleerde applicaties inclusief beheerder en eigenaar. Daarmee is grotendeels inzichtelijk welke ICT-bedrijfsmiddelen aanwezig zijn. Daarnaast worden door de verantwoordelijken voor modulebouw met een Excel spreadsheet de details over het maatwerk bijgehouden. Voor MDA's (mobile digital assistents), iPads, telefoons en simkaarten wordt voor ontvangst getekend. Het buiten gebruik nemen er van wordt niet bijgehouden.

Er is een database voor contracten en overeenkomsten.

Er is een archief en een archiefverordening.

Van presentatiemiddelen (laptops, beamers) onder beheer van FZ wordt een lijst bijgehouden. Daarnaast beschikken diverse teams over eigen hardware en in eigen beheer gemaakte software oplossingen (m.n. kantoorautomatisering). Hier is geen overzicht van.

P&O houdt een overzicht bij van mensen die in reguliere dienst zijn. Werkzaamheden, kennis, opleiding e.d. worden niet systematisch geregistreerd. Van mensen die niet in reguliere dienst (inhuur) zijn vindt geen centrale registratie plaats.

Facilitaire zaken houdt een overzicht bij van de geleasede printers, die door een externe partij beheerd worden.

Facilitaire zaken houdt een overzicht bij met de algemene (nuts)voorzieningen zoals verwarming, airconditioning, energievoorzieningen, verlichting en meubilair, waaronder beveiligde kasten.

Risico's:

Niet voor alle ICT-configuratie items wordt vastgelegd wie de daadwerkelijke eigenaar/hoofdgebruiker is, zoals van in eigen beheer ontwikkelde software configuratie items. Hierdoor valt de CMDB voor dit onderdeel niet volwaardig te gebruiken. Software configuratie items staan in separate overzichten (MS Excel) en niet in de CMDB.
Het eigenaarschap van gegevensbestanden is niet altijd duidelijk

Acties

- Vul CMDB aan met ontbrekende eigenaargegevens en overweeg om de relevante softwareconfiguratie items in de CMDB op te nemen.

- Leg voor alle informatie-items vast wie de eigenaar is. Besteed hier bij organisatieveranderingen expliciet aandacht aan.

7.2 Classificatie van Informatie

Doelstellingen

Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.

Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn. Er behoort een informatieclassificatieschema te worden gebruikt om adequate niveaus van bescherming te definiëren en de noodzaak voor aparte verwerkingsmaatregelen te communiceren.

Beheersmaatregelen

- Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

Feitelijke situatie gemeente Deventer

Classificatie van bedrijfsmiddelen gebeurt niet of nauwelijks, daar waar het gebeurt is het een intuïtief Verder geldt dat in het kader van de WBP persoonsgegevensverzamelingen moeten zijn aangemeld en voldoen aan de regels van de wet of het GBA besluit en vernietigingstermijnen geborgd moeten zijn. Ook hier ontbreekt voldoende inzicht in de situatie.
proces. Wel wordt voor ontvangst getekend bij de uitlevering van goederen aan de organisatie.

Risico's

Het zicht ontbreekt op welke componenten (zowel hardware als software) het belangrijkst zijn voor de primaire processen. Bij crises en calamiteiten zal het gebrek aan inzicht zich doen voelen.

Acties

- Gebruik een classificatietabel zoals beschreven in de Nota Informatiebeveiliging (2007) voor alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten.

8 Beveiliging van personeel

8.1 Voorafgaand aan het dienstverband

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

De verantwoordelijkheden ten aanzien van beveiliging behoren vóór het dienstverband te worden vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.

Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers behoren op geschikte wijze te worden gescreend, in het bijzonder voor vertrouwensfuncties.

Werknemers, ingehuurd personeel en externe gebruikers die IT-voorzieningen gebruiken behoren een overeenkomst te tekenen over hun beveiligingsrollen en –verantwoordelijkheden.

Beheersmaatregel

- De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.
- Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoort te worden uitgevoerd in overeenstemming met relevante wetten, voorschriften en ethische overwegingen, en behoort evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.
- Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.

Feitelijke situatie gemeente Deventer

Voor het aspect ‘beveiliging personeel’ zijn betrekkelijk weinig maatregelen genomen binnen de gemeente Deventer.
Personeel dat in dienst komt en overige mensen die bij de gemeente taken uitvoeren en toegang hebben tot gemeentelijke informatie (zoals bijvoorbeeld inhuur/uitzendkrachten, afstudeerders, stagiairs, mensen in re-integratie trajecten) worden niet gescreend met betrekking tot informatie-beveiligingsrisico’s. In een zeer beperkt aantal gevallen wordt een verklaring omtrent het gedrag vereist of een antecedentenonderzoek gedaan.

Medewerkers en/of inhuurkrachten krijgen slechts in beperkte gevallen instructies op het gebied van informatiebeveiliging.

Medewerkers en inhuurkrachten hoeven slechts in enkele gevallen een overeenkomst te tekenen met betrekking tot verantwoordelijkheden op het gebied van informatiebeveiliging.

Risico’s

Het aannemen van nieuw personeel, het inhuren van extra personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht omdat menselijk falen en bedreigingen van menselijke aard significante invloed kan hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de gemeente Deventer. Meer aandacht besteden aan screening, duidelijkheid in rollen en verantwoordelijkheden en de daarbij behorende contactuele verplichtingen is zinvol om risico’s op dit gebied te beperken.

Acties

- Functiebeschrijvingen toetsen en eventueel aanpassen op de rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging. Voor nieuw personeel extra screenen op positieve referenties, correctheid van C.V., bevestiging van professionele kwalificaties, verklaring omtrent het gedrag.
- In de proefperiode nadrukkelijk aandacht schenken aan de juiste kwalificaties van de medewerker.

- Inhuur en inzet van externen (ook van leveranciers) die toegang krijgen tot vertrouwelijke informatie en /of handelingen kunnen plegen die significant invloed kunnen hebben op de beschikbaarheid en integriteit van informatie, vooraf een verklaring laten tekenen. Het huidige personeel deze verklaring ook laten tekenen als vervanging van eventuele bestaande huidige geheimhoudingsverklaring. De verklaring opstellen conform de eisen van de NEN-ISOIEC 27002:2007.

8.2 Tijdens het dienstverband

Doelstelling

Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.

De verantwoordelijkheden van de directie behoren te worden gedefinieerd om te waarborgen dat beveiliging wordt toegepast gedurende het hele dienstverband van de persoon bij de organisatie.

Alle werknemers, al het ingehuurd personeel en alle externe gebruikers behoren over een passend niveau van bewustwording, opleiding en training in beveiligingsprocedures en het juiste gebruik van IT voorzieningen te kunnen beschikken om mogelijke beveiligingsrisico's te minimaliseren. Er behoort een formeel disciplinair proces te worden vastgesteld voor het omgaan met beveiligingsinbreuken.

Beheersmaatregel

- De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.
- Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.
- Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

Feitelijke situatie gemeente Deventer

Er is geen introductieprogramma en/of trainingsprogramma dat voorziet in het beperken van risico's op het gebied van informatiebeveiliging. Er is geen specifiek disciplinair proces vastgesteld bij inbreuk op de informatiebeveiliging.
Bij een beperkt aantal teams (o.a. IAO en ICT-beheer) staan (deel)aspecten van informatiebeveiliging regelmatig in de belangstelling bij werkoverleg en de dagelijkse werkzaamheden.

Risico's

De meeste incidenten op het gebied van informatie beveiliging ontstaan door menselijke fouten van onze eigen medewerkers, veelal ingegeven door onwetendheid en doordat mensen niet stil staan dat hun handelen (of het nalaten daarvan) invloed kan hebben op informatiebeveiliging.
Door dit tekortschietend besef van de mogelijke gevolgen neemt het risico van menselijk falen toe.

Acties

- Alle medewerkers moeten adequaat worden opgeleid opdat gebruikersfouten tot een minimum worden beperkt. Hierbij dienen de cursussen toegesneden te zijn op de taken van de functionarissen. Medewerkers die werkzaam zijn op gebieden met een verhoogd risico jaarlijks (bij)scholen.
- Bewustwordingsworkshops inzake informatiebeveiliging dragen mee aan houding en "mindset."
- Een teamsite inrichten voor informatiebeveiliging met als doel gerichte informatie en bewustwording.
- Bij het aanstellen van nieuw personeel, informatiebeveiliging expliciet in het introductieprogramma opnemen.
- Alle gebruikers moeten op de hoogte te zijn van de toegang beveiligingsprocedure.
- Meer aandacht besteden aan de risico's die de organisatie loopt als men onvoldoende aandacht besteed aan informatiebeveiliging.

- Het kennisniveau van de applicatiebeheerders en de functioneel beheerders moet op zodanig niveau worden gebracht dat zij het beheer op adequate wijze kunnen uitvoeren.

8.3 Beëindiging of wijziging van dienstverband

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.

Er behoort een beheerverantwoordelijkheid in de organisatie te zijn om te waarborgen dat alle apparatuur wordt teruggegeven en dat alle toegangsrechten worden ingetrokken wanneer een werknemer, ingehuurde medewerker of externe gebruiker de organisatie verlaat.

Veranderen van verantwoordelijkheden en dienstverband binnen de organisatie behoort te worden behandeld als de beëindiging van de desbetreffende verantwoordelijkheid of het desbetreffende dienstverband in overeenstemming met dit hoofdstuk; elk nieuw dienstverband behoort te worden behandeld als beschreven in hoofdstuk 8.1. van de NEN-ISO/IEC 27002:2007.

Beheersmaatregel

- De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.
- Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.
- De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoren na wijziging te worden aangepast.

Feitelijke situatie gemeente Deventer

Bij de beëindiging of wijziging van het dienstverband van medewerkers binnen de gemeente Deventer, zowel personeel in reguliere dienst als anderszins (zoals bijvoorbeeld inhuur/-uitzendkrachten, afstudeerders, stagiairs, mensen in re-integratie trajecten) is geen sluitende procedure vastgelegd dat zeker stelt dat verantwoordelijkheden volledig en correct worden overgenomen, bedrijfsmiddelen worden geretourneerd en toegangsrechten in alle systemen worden ingenomen, ook in geval van een onmiddellijk, onvrijwillig ontslag of vertrek. Ook wordt de beschikbaarheid en overdracht van informatie (op bijvoorbeeld persoonlijke opslaglocaties) niet gewaarborgd.

Risico's

Een belangrijk risico dat ontstaat als toegangsrechten niet tijdig worden ingetrokken is het gevaar van valse identiteit en het ongeautoriseerd gebruik van programma's. Anderen zijn mogelijk in het bezit van gebruikersnamen en wachtwoorden van de vertrokken medewerker (en omgekeerd) en disciplinaire maatregelen kunnen niet meer toegepast worden. Het nemen van maatregelen om zeker te stellen dat rollen en verantwoordelijkheden zijn overgenomen, bedrijfsmiddelen zijn geretourneerd en toegangrechten in alle systemen zijn geblokkeerd, is een relatief eenvoudige en goedkope maatregel en voorkomt dat bedreigingen van menselijke aard manifest worden. Een veel voorkomend probleem is het onterecht behoud van rechten bij het wisselen van functie wat eveneens het risico van menselijke aard verhoogd. Er wordt informatie op persoonlijke netwerkschijven opgeslagen, waar na beëindiging van het dienstverband soms moeilijk of niet bij te komen is.

Acties

- Een procedure beëindiging en wijziging dienstverband opstellen en invoeren.
- Het is belangrijk dat geen accounts worden aangemaakt voor medewerkers die niet onder beheer staan van het team Personeel & Organisatie. Het is wenselijk hiervoor een procedure/check in te voeren.
- Het registreren van toegangsrechten van medewerkers in systemen en periodiek toetsen op actualiteit.

- Een noodprocedure opstellen voor het intrekken van toegangsrechten en inname van bedrijfsmiddelen bij specifieke situaties (onvrijwillig ontslag, juridische procedures van allerlei aard, non-actief stelling, overlijden, enz.).
- Voer een exit gesprek met elke medewerker die de organisatie verlaat (en) besteed expliciet aandacht aan aspecten van informatiebeveiliging.

9 Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiligde ruimten en apparatuur

Doelstelling

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

IT-voorzieningen die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermt door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.

De geboden bescherming behoort in overeenstemming te zijn met de vastgestelde risico's.

Het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
Apparatuur behoort te zijn beschermd tegen fysieke bedreigingen en gevaren van buitenaf.

Bescherming van apparatuur (waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen) is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade. Ook bij het verplaatsen of verwijderen van apparatuur behoort hiermee rekening te worden gehouden. Er kunnen bijzondere beheersmaatregelen nodig zijn om de apparatuur te beschermen tegen fysieke bedreigingen en ter bescherming van de ondersteunende voorzieningen zoals stroomvoorziening en bekabelingsinfrastructuur.

Beheersmaatregelen

- Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.
- Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.
- Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.
- Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.
- Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.
- Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT-voorzieningen, om onbevoegde toegang te voorkomen.
- Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.
- Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.
- Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.
- Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeerd.
- Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

- Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.
- Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

Feitelijke situatie gemeente Deventer

Alle panden zijn voorzien van een bliksemafleidingsinstallatie en van een branddetectieinstallatie waarmee automatisch signalen worden doorgegeven. Er zijn geen sprinklerinstallaties; wel zijn er brandslangen en blussers op alle locaties.

In alle panden is alarm aanwezig op de deuren. Tot 19.00 kunnen medewerkers naar binnen, daarna pas na het volgen van de 'procedure aanvragen overwerk. Het alarm wordt dan uitgeschakeld. Voor bepaalde panden en functies zijn mensen 7 x 24 uur geautoriseerd (voorbeeld: sociale rechercheurs). Het alarm geeft een akoestisch signaal en is verbonden met een meldkamer, waarmee responstijden zijn afgesproken.

Het (extern ingehuurde) schoonmaakpersoneel is veelal na kantoortijden onbeheerd aan het werk in de panden van de gemeente. Externen werken niet onbeheerd in de beschermde ICT-ruimtes.

Voor technische onderhoudswerkzaamheden zijn contracten met externe partijen afgesloten.

De BHV (o.a. ontruiming) is voor alle panden geregeld, en er wordt regelmatig geoefend op ontruimingen.
De ICT-serverruimtes zijn adequaat gekoeld, zijn voorzien van alarminstallaties en fysiek deugdelijk ingericht. De deuren zijn voorzien van adequate vergrendeling en sloten en de toegang is procedureel geborgd. De meeste actieve netwerkcomponenten patchkasten zijn fysiek beschermd tegen toegang door niet-geautoriseerd personeel; echter niet alle. In de buitengebouwen zijn de SER's / patchkasten niet overal adequaat beveiligd (de parkeergarage stadskantoor en de Openbare Bibliotheek in het bijzonder.)
Op de meest cruciale ICT-systemen zijn no-break-installaties aangesloten waardoor deze tegen spanningsverschillen en stroomuitval beveiligd zijn. Standaard wordt elke vier jaar de ICT-apparatuur vernieuwd en er is voorzien in adequate Service Level Agreements en support en onderhoudscontracten, inclusief contractuele vervolgschadevoorwaarden. Er is een uitwijkmogelijkheid voor de ICT-servers. Er is adequate voorraad voor kritieke apparatuur beschikbaar. Reserveapparatuur en media worden adequaat beheerd, op veilig afstand, in kluizen indien noodzakelijk. Reserveapparatuur en media met reservekopieën zijn met voldoende afstand van de hoofdlocatie opgeslagen in secundaire gemeentelijke locaties. De apparatuur is zodanig opgesteld dat de risico's van schade, storing van buitenaf en ongeautoriseerde toegang beperkt zijn.

Voor de serverruimten van ICT-beheer is een noodstroomvoorziening getroffen; niet voor de rest van de organisatie.

De locatie Stadhuis kent een receptiefunctie, die is uitbesteed aan een extern bedrijf. Een van de ingangen hier is niet afgesloten en openbaar toegankelijk. De receptie heeft hier weinig tot geen zicht op. Via deze ingang zijn de werkkamers van o.a. de bestuursdienst en het college bereikbaar, en de vergaderruimten in het landshuis. FZ verzorgt de receptiefunctie op de locatie Leeuwenbrug, en Dienstverlenen op de locatie Smedenstraat. De overige locaties kennen geen receptiefunctie.

Alle buitendeuren hebben een fysiek slot met (speciale) sleutel, en worden door de bodes 's morgens van het slot gedraaid. Hierna zijn ze te openen met de toegangspasjes. Alle buitendeuren van de panden en de binnendeuren aangrenzend aan voor het publiek of andere organisaties toegankelijke ruimten zijn voorzien van een slot met een pasjessysteem. De toegang tot de ICT-serverruimtes is met aparte toegangspasjes is afgeschermd.

Enkele panden kennen meer gebruikers dan alleen de gemeente. Bij het SAB lopen de organisaties van Saxion Hogeschool en de gemeente (letterlijk) door elkaar. De locatie Smedenstraat kent meerdere gebruikers, waarbij medewerkers van andere organisaties door een kavel van de gemeente moeten lopen om hun werkruimtes te bereiken. De locaties Leeuwenbrug en De Welle hebben meer gebruikers, en hier worden buitendeur, trappenhuis en sanitaire voorzieningen gedeeld. Voor de toegang naar de werkruimtes (etages) wordt een pasjessysteem gebruikt.

Het is bij bepaalde binnendeuren mogelijk om deze door middel van een magneet vast te zetten, waarmee het toegangspasjessysteem omzeild kan worden. Het is mogelijk om met iemand mee te lopen naar binnen, er is geen individueel sluis/tourniquet systeem.

Er zijn verschillende toegangspasjessystemen in gebruik binnen de gemeente (binnenstad, Leeuwenbrug, Smedenstraat, Brandweer). Voor de parkeergarages en fietsenstallingen zijn aparte pasjes of sleutels in gebruik.

De aanvraag van toegangspasjes gaat via de afdelingssecretariaten. FZ geeft de pasjes altijd uit wanneer deze door de juiste persoon (secretariaat) zijn aangevraagd; er vindt geen extra controle plaats. De pasjes worden op naam geregistreerd. De naam staat niet op de pasjes. In de passystemen bij de deuren is uitleesbaar met welk pasje de deur geopend is.

Medewerkers en/of bezoekers hebben geen naambadges of zijn als zodanig herkenbaar. Extern bezoek wordt bij de eerste binnenkomst in een pand bij de toegangsdeur opgehaald en begeleidt. Extern personeel dat langere tijd (meerdere dagen) werkzaam is, krijgt vrij automatisch een toegangspas tot de gemeentelijke panden, of wordt bij de deur vrije toegang verleend. Hetzelfde geldt voor technisch onderhoudspersoneel.

Wanneer mensen uit dienst gaan, of op een ander locatie komen te werken, worden ze geacht de pasjes weer in te leveren. Ook bij het veranderen van functies moet een check worden uitgevoerd op de correctheid van de autorisaties van de pasjes. Dit gaat via het officemanagement. Er is niet voldoende inzicht of dit daadwerkelijk gebeurt.

Alle medewerkers beschikken over een standaard werkplek, met onder meer een afsluitbaar ladenblok en een afsluitbare kast. Op aanvraag kan in een brandwerende kast worden voorzien. In de praktijk worden de kasten/laden meestal niet afgesloten en ligt er veel informatie ‘open en bloot’ op de bureaus. Het clean desk principe wordt op enkele werkplekken toegepast.

De printers zijn voorzien van een optie ‘beveiligd afdrukken.’ In de praktijk wordt hier te weinig gebruik van gemaakt en ligt er eerder als regel dan als uitzondering vertrouwelijke informatie naast de printers.

De archiefruimten voldoen aan de landelijke “Regeling bouw en inrichting archiefruimten en archiefbewaarplaatsen”, met hierin onder meer bouwkundige eisen alsmede eisen aan brandpreventie, klimaat en inrichting. De officiële gemeentelijke archieven voldoen eveneens aan de eisen van de archiefinspectie. Alleen de kelder aan de locatie Polstraat voldoet niet geheel aan de gestelde eisen. Het risico wordt hier als beperkt ingeschat omdat hier alleen de op termijn vernietigbare documenten worden opgeslagen.

De personeelsdossiers zitten in een kast die als regel op slot zit.

Voor het veilig thuis of op externe locatie werken is geen beleid geformuleerd, en zijn geen voorzieningen getroffen.

Risico’s

De toegang tot de kritieke systemen of informatie leunt sterk op het (pasjes) toegangsysteem. Voor bezoekers worden geen pasjes uitgereikt en het bezoek wordt dus niet geregistreerd. Hiermee is de herleidbaar naar individuen na incidenten ‘audit-trail’ niet mogelijk en dit geeft een verhoogd risico op het gebied van bedreiging van menselijke aard. Gezien het grote en wisselende aantal externen en het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan. De controle op de toegangspasjes is gebrekkig.

Door informatie zichtbaar op bureaus te laten liggen wordt een verhoogd risico gelopen met betrekking tot vertrouwelijkheid.

Er zijn geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.

Acties

- Richt bij alle locaties een receptiefunctie in.
- Zorg er voor dat alle bezoekers in de voor het publiek afgesloten gedeeltes van de panden van de gemeente persoonlijk worden opgehaald bij de ingang en na afloop weer naar buiten begeleid; ook op de locatie Stadhuis.
- Overweeg een praktische registratiemethode voor bezoekers.
- Overweeg een individueel toegangssysteem, bijvoorbeeld tourniquets.
- Overweeg een systeem met persoonbadges.

- Voer een deugdelijke administratie in voor afgifte, periodieke controle en inname van toegangspasjes.
- De toegang tot de ruimte voor systeembeheer wordt beperkt tot degenen die daar werken. Toegangspassen voor anderen worden ingetrokken.
- Voer werken volgens het clean desk principe in.
- Berg papieren en computermedia in kasten op met deugdelijke sloten wanneer zij niet gebruikt worden in het bijzonder buiten werktijd en bewaar gevoelige of kritieke bedrijfsinformatie achter slot en grendel als het kantoor gesloten is. Stel hier richtlijnen voor op.
- Sluit deuren en ramen als er niemand aanwezig is.
- Harde schijven en andere media dienen adequaat te worden gewiped of vernietigd bij afstoting of hergebruik indien vertrouwelijke informatie is opgeslagen en/of licentieplichtige programmatuur hierop is geïnstalleerd.
- Plaats ondersteunende apparatuur zoals faxen, copiers op een geschikte plaats binnen de beveiligde zone.
- Besteed actiever aandacht aan het bestaan van beveiligd afdrukken. Ga bij het vervangen van de printers over op standaard beveiligd afdrukken.
- Beperk de toegang tot alle actieve componenten tot team ICT-beheer geautoriseerd personeel.
- Breng geschikte anti-inbraaksystemen aan voor compenenten die een extra risico vormen, met name bij de patchkasten in de parkeergarage Stadskantoor en de Openbare Bibliotheek.
- Neem het onderwerp informatiebeveiliging expliciet mee bij de eisen die aan het ontwerp voor de nieuwbouw voor de gemeentelijke huisvesting worden gesteld en zo veel mogelijk bij de uit te voeren acties in het kader van het opknappen van de bestaande huisvesting.
- Stel richtlijnen op voor het gebruik van apparatuur buiten het gemeentehuis (thuiswerken of werken op externe locatie).
- Stel procedures op voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Ga zo veel mogelijk over op digitale archivering i.v.m. fysieke bedreigingen (zoals brand.)

10 Beheer van communicatie- en bedieningsprocessen

10.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling

Waarborgen van een correcte en veilige bediening van IT-voorzieningen. Er behoren verantwoordelijkheden en procedures te worden vastgesteld voor beheer en bediening van alle IT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies. Er behoort waar van toepassing, functiescheiding te worden toegepast om het risico van nalatigheid of opzettelijk misbruik van het systeem te verminderen.

Beheersmaatregelen

- Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.
- Wijzigingen in IT-voorzieningen en informatiesystemen behoren te worden beheerst.
- Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
- Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

Feitelijke situatie gemeente Deventer

Voor de meeste applicaties is functioneel beheer geregeld, in de meeste gevallen decentraal bij de verantwoordelijk proceseigenaar. Applicatiebeheer (wijzigingen) wordt in de meeste gevallen uitgevoerd door de externe leverancier van de applicatie. Technisch (systeem)beheer vindt plaats bij ICT-beheer.

Het beeld aangaande documentatie van de bediening van de applicaties, van de functionaliteiten of van wijzigingen is diffuus. In bepaalde gevallen is er documentatie voorhanden, bij andere applicaties niet of zeer beperkt.

De procedures met betrekking tot wijzigingen in en vervangen van software zijn niet beschreven.

Functiescheiding: gelet op de grootte van de organisatie krijgt in de meeste situaties onderlinge vervangbaarheid grotere prioriteit dan functiescheiding. Binnen de grotere applicaties wordt een onderscheid in rollen gemaakt. Binnen de financiële discipline wordt sterk gebruik gemaakt van functiescheidingen en controles, zowel binnen de informatiesystemen als ook in de te verrichten handelingen.

Voor de financiële systemen geldt dat gegevens niet altijd op een uniforme wijze worden ingevoerd/ingeboekt, wat tot problemen bij het onderlinge vergelijken en het krijgen van managementinformatie kan leiden.

De gemeente Deventer heeft formele procedures voor het doorvoeren van wijzigingen binnen de systemen van ICT-beheer opgesteld. Er is momenteel niet overal een operationeel fysiek gescheiden testomgeving ingericht. De productieprogrammatuur is in een datakluis opgeslagen. De wijzigingen in de ICT-omgeving worden geregeld via een change coördinator (proces coördineren en inhoudelijke/-beoordelende component.) Voor de bedrijfskritische systemen is er een CAB. OTAP: voor alle (bedrijfskritische) informatiesystemen), met uitzondering van het netwerk, is er een testomgeving die afgescheiden is van productieomgeving. Voor de acceptatie van software zijn afspraken met betrekking tot technische en functionele acceptatietesten beperkt geregeld. Software doorloopt dus feitelijk een acceptatieprocedure. Deze procedures zijn niet beschreven en vastgelegd.

Risico's

Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
Aanpassingen in de netwerkinfrastructuur kunnen worden getest in de productieomgeving; dit belemmert het robuust testen van de wijzigingen en resulteert in beperkte informatiebeveiligings-risico's. Het niet vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan

kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een significant verhoogd risico.

Acties

- Zorg voor (het onderhouden van) documentatie met betrekking tot de bediening, functionele specificaties, procedures en wijzigingen van de informatiesystemen.
- Ga per informatiesysteem of proces na of functiescheiding doorgevoerd kan worden en implementeer dit zo nodig.
- Zorg voor uniforme voorschiften voor het opnemen van informatie in de financiële systemen, communiceer hierover en zorg voor controle en handhaving.
- Formaliseer het wijzigingsproces, gebruik hiervoor de ITIL best practice als leidraad.
- Om tot adequate en beheersbare veranderingen binnen systemen te komen, is het gewenst de volgende maatregelen te treffen:
    - Voor het inrichten van een testomgeving dient bij voorkeur gebruik te worden gemaakt van een fysiek gescheiden testomgeving. Indien dit niet mogelijk is, richt dan een logische testomgeving in.
    - Het opstellen van een testplan passend bij de wijziging (door functioneel beheer).
    - Het uitvoeren van het testplan door een geselecteerde groep gebruikers (door functioneel beheer).
    - Overweeg in een logboek bij te houden welke versie wanneer op welk systeem operationeel is geweest voor die systemen waar dat van belang is.
    - Alle systeemdocumentatie moet worden beveiligd tegen ongeautoriseerde toegang. Het is aan te bevelen dit in een afgesloten ruimte te bewaren.

10.2 Beheer van de dienstverlening door een derde partij

Doelstelling

Geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.

De organisatie behoort de implementatie van overeenkomsten te controleren, naleving van de overeenkomsten te bewaken en wijzigingen te beheren om te waarborgen dat de geleverde diensten aan alle eisen voldoen die met de derde partij zijn overeengekomen.

Beheersmaatregelen

- Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.
- De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.
- Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de (on)misbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

Feitelijke situatie gemeente Deventer

Er zijn maar beperkt SLA’s; dit wordt deels gecompenseerd omdat in een middelgrote organisatie het in het algemeen intuïtief wel helder is wat belangrijk is en wat enig uitstel kan dulden.

Risico’s

De risico’s die bestaan door het niet hebben vastgelegd van het niveau van dienstverlening / informatiebeveiliging nemen toe. De gemeente gaat steeds meer samenwerken (en informatie uitwisselen) in ketens, besteedt taken uit en gaat meer diensten verlenen aan andere gemeenten en organisaties. SLA’s zijn hierbij essentieel. De gemeente is ook verantwoordelijk voor de informatiebeveiliging in dat deel van de keten waarbij het beheer bij een andere partij ligt.

Acties

- Start met het opzetten van een basis-SLA voor dienstverlening waarin aandacht wordt besteed aan informatiebeveliging.
- Stel een basiscontract op voor de toegang tot de IT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin kaders staan voor de toegang tot IT-voorzieningen door derden.
- Richt applicatiebeheer en functioneel beheer dusdanig in dat de naleving van de gemaakte afspraken kan worden gemonitord.

10.3 Systeemplanning en -acceptatie

Doelstelling

Het risico van systeemstoringen tot een minimum beperken.

Een voorafgaande planning en voorbereiding zijn noodzakelijk om afdoende capaciteit en beschikbaarheid van middelen te waarborgen die nodig zijn om de vereiste systeemprestaties te leveren.

Er behoren prognoses te worden gemaakt van toekomstige capaciteitseisen om het risico van overbelasting van het systeem te verminderen.

De operationele eisen van nieuwe systemen zouden moeten worden vastgesteld, gedocumenteerd en getest voordat de systemen worden geaccepteerd en in gebruik worden genomen.

Beheersmaatregelen

- Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.
- Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.

Feitelijke situatie gemeente Deventer

Capaciteitsbeheer is reactief geregeld. Maandelijks worden overzichten over de bezetting van schijven en de groei in de afgelopen periode gegenereerd.

Het gebruik van testdata: de verantwoordelijk ligt bij de eigenaar van de data (meestal niet ICT). De mate van bewustwording is laag. Testdata is meestal een extract uit de productie, waardoor hier risico ontstaat dat data relatief makkelijk beschikbaar is.

Risico's

De risico's zijn in de praktijk beperkt

Acties:

- Het implementeren van het ITIL –proces Capacity Management. Dit heeft geen hoge prioriteit.

10.4 Bescherming tegen virussen en 'mobile code'

Doelstelling

Beschermen van de integriteit van programmatuur en informatie.

Er behoren voorzorgen te worden getroffen om de introductie van virussen en ongeautoriseerde 'mobilecode' te voorkomen en te ontdekken.

Programmatuur en IT-voorzieningen zijn kwetsbaar voor invoer van virussen, zoals computervirussen, netwerkwormen, Trojaanse paarden en logische bommen. Gebruikers behoren bewust te worden gemaakt van de gevaren van virussen. Managers behoren zo nodig bijzondere beheersmaatregelen te treffen om virussen te voorkomen, te ontdekken en te verwijderen en 'mobile code' te beheersen.

Beheersmaatregelen

- Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.
- Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

Feitelijke situatie gemeente Deventer

De elementaire maatregelen zijn getroffen. Processen rondom virusbestrijding zijn onvoldoende beschreven. Met name de rollen en verantwoordelijkheden als onverhoopt toch virussen binnen geraken.

Software wordt gekocht bij standaard bekende leveranciers. Richting gebruikers in de organisatie is gecommuniceerd dat installeren van illegale software niet is toegestaan en door het beperken van installatierechten is dit zeer beperkt mogelijk. De nodige maatregelen zijn getroffen om er voor te zorgen dat programma's met virussen zoveel mogelijk buiten de deur gehouden worden.

Voor thuisgebruik is een aantal jaren geleden een licentie voor McAfee Security Centre (anti-virus en spyware, firewall, etc.) verstrekt aan alle medewerkers. De laatste licenties liepen in 2009 af, en zijn door de organisatie niet verlengt.

Risico's

Bij daadwerkelijke infectie met virussen o.i.d. is bestrijding niet formeel geregeld. Dit zal tot veel ad hoc acties en besluiten leiden.
Het ontbreken van een regeling voor anti-virus bescherming thuis leidt tot hogere beveiligingsrisico's.

Acties

- Stel een actieplan /noodplan op en test dit.
- Laat jaarlijks Legal Hack uitvoeren om de bewustwording te vergroten rondom de risico's die gelopen worden.
- Stel weer anti-virusbescherming voor thuisgebruik beschikbaar.

10.5 Back-up

Doelstelling

Handhaven van de integriteit en beschikbaarheid van informatie en IT-voorzieningen. Er behoren routineprocedures te worden vastgesteld voor uitvoering van het overeengekomen back-upbeleid en de -strategie, ten aanzien van het maken van back-ups van gegevens en het oefenen van een tijdig herstel ervan.

Beheersmaatregelen

Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.

Feitelijke situatie gemeente Deventer

De back-up van programmatuur en data op het netwerk is afdoende geregeld. Er zijn diverse generaties beschikbaar op drie afzonderlijke locaties.

Gegevens zoals die één werkdag geleden waren, kunnen binnen één werkdag worden gereconstrueerd.

De back-up gegevens worden in een andere ruimte bewaard dan de ruimte waarin de apparatuur is opgesteld.

Er zijn beperkt voorzieningen getroffen om een reconstructie van de mutaties die na de laatste back-up zijn aangebracht, te kunnen uitvoeren.

Het transport van de back-up tapes naar de externe bewaarlocatie is beveiligd door middel van het gebruik van een 'datakoffer' tijdens het transport.

In de praktijk blijkt dat soms nog op lokale (C-)schijven wordt gewerkt met bedrijfskritische of vertrouwelijke informatie. Hiervoor bestaat geen back-up voorziening, en evenmin voor thuisgebruik of voor draagbare media.

Risico's
Deze zijn beperkt.

Acties
- Periodiek oefenen in het terugzetten van back-ups. Met name de administratieve processen.
- Wijs de medewerkers periodiek op de risico's van lokale opslag en het ontbreken van back-ups.

10.6 Beheer van netwerkbeveiliging

Doelstelling

Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

Veilig beheer van netwerken die de grens van de eigen organisatie kunnen overschrijden verdient bijzondere aandacht, vooral wat betreft gegevensstromen, juridische implicaties, controle en bescherming.

Beheersmaatregel
- Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.
- Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

Feitelijke situatie gemeente Deventer

De initiële autorisatie is goed geregeld, maar het beheer op bestaande accounts is niet afdoende geregeld (verwijderen accounts, autorisatie accounts etc.)

Kritische documentatie staat in afgeschermde ruimten. Onduidelijk is of documentatie in het geval van calamiteit, zoals brand, voldoende beschikbaar/toegankelijk is.

Het uitwisselen van informatie: het bewustzijn van het belang er van is aanwezig, maar het proces is niet beschreven. (Wie is bevoegd welke info op welke wijze aan wie te verstrekken.)

Er zijn richtlijnen voor het gebruik van e-mail en internet opgesteld en beschikbaar gesteld.

Risico's
De integriteit en exclusiviteit van informatie kan niet gegarandeerd worden omdat het beheer van autorisaties niet goed geregeld is.

Acties:
- Formaliseer het autorisatieproces en laat periodiek toetsen of de autorisaties nog adequaat zijn.
- Toets richtlijnen periodiek op actualiteit en tegen eventuele nieuwe ontwikkelingen in de techniek.
- Bij wijzigingen in functies of bezetting dienen de toegangsrechten opnieuw te worden bezien. Er moet meer gewerkt worden met rollen.

10.7 Behandeling van media

Doelstelling

Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

Media behoren te worden beheerst en fysiek te worden beschermd.

Er behoren passende procedures te worden vastgesteld om documenten, opslagmedia (bij voorbeeld banden, schijven), in- en uitvoergegevens en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

Beheersmaatregel
- Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.

- Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn,overeenkomstig formele procedures.
- Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.
- Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.

Feitelijke situatie gemeente Deventer
Tot de verwijderbare media worden gerekend: banden, schijven, flashgeheugenkaarten, verwijderbare harde schijven, cd's, dvd's en gedrukte media.

Er zijn geen formele procedures opgesteld over het beheer van verwijderbare media. Binnen ICT-beheer wordt er adequaat mee omgegaan. Het zicht op de rest van de organisatie is beperkt.

Onduidelijk is of systeemdocumentatie in het geval van calamiteit, zoals brand, voldoende beschikbaar/toegankelijk is.

Risico's
De beschikbaarheid en exclusiviteit van informatie kan niet volledig gegarandeerd worden omdat het beheer niet afdoende geregeld is.

Acties:
- Stel procedures op voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Harde schijven en andere media dienen adequaat te worden gewiped of vernietigd bij afstoting of hergebruik indien vertrouwelijke informatie is opgeslagen en/of licentieplichtige programmatuur hierop is geïnstalleerd.
- Berg papieren en computermedia in kasten op met deugdelijke sloten wanneer zij niet gebruikt worden in het bijzonder buiten werktijd en bewaar gevoelige of kritieke bedrijfsinformatie achter slot en grendel als het kantoor gesloten is. Stel hier richtlijnen voor op.
- Neem mobiele apparatuur (zoals laptops, pda's, iPads) in wanneer deze niet meer wordt gebruikt.
- Heroverweeg het besluit rondom encryptie en stel encryptie verplicht voor informatie op mobiele apparatuur en USB-sticks indien het gaat om informatie met het classificatielabel vertrouwelijk en zeer geheim.

10.8 Uitwisseling van informatie

Doelstelling

Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

De uitwisseling van informatie en programmatuur tussen organisaties behoort te zijn gebaseerd op een formeel uitwisselingsbeleid, dat in lijn is met de uitwisselingsovereenkomsten, en behoort te worden uitgevoerd in overeenstemming met relevante wetgeving

Er behoren procedures en normen te worden vastgesteld ter bescherming van informatie en fysieke media die informatie bevatten die wordt getransporteerd.

Beheersmaatregel
- Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
- Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
- Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.
- Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.

Feitelijke situatie gemeente Deventer

Er is geen specifiek beleid, procedures of beheerprocessen over het uitwisselen van informatie of programmatuur. Deze zijn ook niet opgenomen in de contracten met leveranciers of ketenpartners.

Er is bewust gekozen om geen encryptie op MDA's, laptops e.d. toe te passen en er is gekozen om geen specifiek beleid op stellen inzake het gebruik van USB-sticks of andere opslagmedia voor het uitwisselen van informatie.

Bij communicatie via Suwinet wordt wel van beveiligde, versleutelde verbindingen gebruik gemaakt en bij Publiekszaken wordt gebruik gemaakt van een (beperkte) bewerkerovereenkomst, die wordt afgesloten met partijen die bewerkingen doen met GBA gegevens voor de gemeente.

Risico's

De kans op verlies of diefstal van laptops, USB-sticks, iPads of MDA's is aanzienlijk – en daarmee dus ook de kans dat informatie in verkeerde handen komt.

Acties

- Formaliseer de bestaande feitelijke situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.
- Stel een basisraamwerk op met randvoorwaarden voor gegevensuitwisseling met ketenpartners.
- Laat vastleggen dat geen gevoelige informatie (classificatie vertrouwelijk en zeer geheim) bekend gemaakt wordt via telefoon of fax, in verband met bijvoorbeeld afluisteren.
- Door het creëren van bewustzijn over de te lopen risico's zal de sociale controle ook toenemen en zal het risico op het lekken van informatie via telefoon e.d. afnemen.

10.9 Diensten voor e-commerce

Doelstelling

Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan.

Er behoort aandacht te worden besteed aan de beveiligingsimplicaties die gepaard gaan met diensten voor e-commerce, waaronder onlinetransacties en de eisen voor beheersmaatregelen. Ook aan de integriteit en beschikbaarheid van informatie die elektronisch is gepubliceerd via openbaar toegankelijke systemen behoort aandacht te worden besteed.

Beheersmaatregel

- Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.
- Informatie die een rol speelt bij onlinetransacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.
- De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen.

Feitelijke situatie gemeente Deventer

Dit onderdeel moet nog nader worden onderzocht.

10.10 Controle

Doelstelling

Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

Systemen behoren te worden gecontroleerd en informatiebeveiligingsgebeurtenissen behoren te worden geregistreerd. Er behoort gebruik te worden gemaakt van logbestanden van operators en storingsregistraties om te waarborgen dat de informatiesysteemproblemen worden vastgesteld.

Een organisatie behoort te voldoen aan alle relevante wettelijke eisen die van toepassing zijn op haar controle- en registratieactiviteiten.

Er behoort systeemcontrole te worden toegepast om de doelmatigheid van de aanvaarde beheersmaatregelen te controleren en de overeenstemming met een model voor toegangsbeleid te verifiëren.

Beheersmaatregelen

- Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
- Er behoren procedures te worden vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.
- Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.
- Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.

Feitelijke situatie gemeente Deventer

Audit en logbestanden: de mogelijkheden zijn bekend en het hangt van de individuele beheerder af wat geïmplementeerd is/wordt.

Risico's

Deze zijn beperkt.

Acties

- Formaliseer de bestaande situatie. Logging alleen na een expliciete vraag en volgens een vastgestelde procedure.
- Er op toezien dat alle storingen, problemen en oplossingen worden vastgelegd door ICT-beheer in HP OpenView (of een soortgelijk systeem): geen actie zonder vastlegging.

11 Toegangsbeveiliging

11.1 Bedrijfseisen ten aanzien van toegangsbeheersing

Doelstelling

Beheersen van de toegang tot informatie.

De toegang tot informatie, IT-voorzieningen en bedrijfsprocessen behoort te worden beheerst op grond van bedrijfsbehoeften en beveiligingseisen.

In de regels voor toegangsbeveiliging behoort rekening te worden gehouden met beleid ten aanzien van informatieverspreiding en autorisatie.

Beheersmaatregel

- Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

Feitelijke situatie gemeente Deventer

De fysieke toegangsbeveiliging is beschreven in hoofdstuk 9; zie ook aldaar. Er is geen beleid vastgelegd of gedocumenteerd ten aanzien van toegangsbeveiliging. De bestaande toegangsmaatregelen zijn veelal op basis van intuïtie en gewoonte tot stand gekomen.
De logische toegangsbeveiliging voor informatiesystemen (inloggen; autorisaties) wordt per systeem ingesteld door de functioneel beheerder.

Risico's

Toegangsbeheersing is niet expliciet gebaseerd op een risicoanalyse waardoor niet duidelijk is of het juiste niveau van beveiliging wordt gehanteerd.
De kans op verstoringen door onoordeelkundig gebruik van ICT-ruimtes of ICT-componenten (met name in buitengebouwen) waar ook niet ICT-teams toegang hebben is relatief groot.

Acties

- Stel beleid op met betrekking tot toegangsbeveiliging. Baseer dit op een risicoanalyse.

11.2 Beheer en verantwoordelijkheid van toegangsrechten van gebruikers

Doelstelling

Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

Er behoren formele procedures te zijn voor de beheersing van toewijzing van toegangsrechten tot informatiesystemen en -diensten.

In de procedures behoren alle fasen in de levenscyclus van gebruikerstoegang te worden vastgelegd, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben. Indien van toepassing behoort bijzondere aandacht te worden besteed aan de noodzaak toewijzing van speciale toegangsrechten waarmee gebruikers de normale beveiliging van een systeem kunnen passeren te controleren.

Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT-voorzieningen.

Doeltreffende beveiliging vereist de medewerking van geautoriseerde gebruikers.

Gebruikers behoren op de hoogte te worden gebracht van hun verantwoordelijkheid voor het handhaven van doeltreffende toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur.

Er behoort een ‘clear desk’- en ‘clear screen’-beleid te worden ingevoerd om het risico van ongeoorloofde toegang of schade aan papieren, media en IT-voorzieningen te verminderen.

Beheersmaatregelen

- Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
- De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.
- De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.
- De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.
- Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.
- Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.
- Er behoort een ‘clear desk’-beleid voor papier en verwijderbare opslagmedia en een ‘clear screen’-beleid voor IT-voorzieningen te worden ingesteld.

Feitelijke situatie gemeente Deventer

Voor de toegang tot het netwerk zijn gebruikersprofielen beschikbaar en wordt gewerkt met individuele accounts en wachtwoorden. Het Domein Admin User account wachtwoord ligt in een kluis en administrators (ICT-beheer) gebruiken persoonlijke, individueel herleidbare accounts. Er is geen specifiek, vastgelegd beleid met betrekking tot gebruikerprofielen, bijbehorende op need to know principe toewijzing van applicaties en netwerkbronnen. De gebruikersprofielen zijn organisatie-element georiënteerd.

De toegang tot domeinspecifieke applicaties valt onder het beheer van de functioneel beheerders, meestal in de lijnorganisatie. Autorisatieverzoeken lopen via de lijn maar zijn niet procedureel gestandaardiseerd vastgelegd met een aanvraagprocedure. Met name door interne verplaatsingen van personeel kan de toegang tot netwerkfolders mogelijk vervuild zijn voor wat betreft exclusiviteit. Elke twee maanden worden door het team ICT-beheer overzichten voorgelegd aan de verantwoordelijke manager ter extra controle van de toegang tot applicaties inzake autorisatie, toewijzing van wachtwoorden voor need to know benodigde systemen. Dit geldt niet voor folders en de rechten binnen de applicatie.

Alle gebruikers hebben de beschikking over één persoonsgebonden account. Op deze wijze zijn alle computeractiviteiten terug te voeren tot de individuele personen. Het aanloggen geschiedt op basis van identificatie (user-id) en authenticatie (password). Hierna worden de gebruikers via een verplichte route naar een menu geleid. De gebruikers kunnen alleen middels dit gesloten menu applicaties opstarten. Er is een consequent, systeemtechnisch afgedwongen en vastgelegd wachtwoordbeleid voor alle systemen en eindgebruikers (1 maal per 3 maanden gedwongen wijzigen van wachtwoord).

De meeste applicaties zijn voorzien van separate logische toegangsbeveiliging met autorisaties. De agenda/mailomgeving, het intranet en persoonlijke/team-netwerkfolders hangen onder de algemene inlog. Voor de meeste applicaties is het proces van autorisatie niet beschreven.

Alle medewerkers hebben toegang tot meerdere applicaties, die elk voorzien zijn van een eigen inlog ID met wachtwoord. De praktijk leert dat het onthouden van meerdere ID’s en wachtwoorden problemen geeft, en wachtwoorden worden veelvuldig opgeschreven en bewaard in de nabijheid van de PC. Ook worden wachtwoorden voor bepaalde applicaties gedeeld door meerdere gebruikers.

Een zeer veelvoorkomend verschijnsel is dat gebruikers verplicht worden door hun leidinggevenden om bij afwezigheid (ziekte, vakantie) hun algemene (mail, netwerk, intranet) of domeinspecifieke wachtwoorden bekend te maken, om anderen onder hun ID in te laten loggen.

Op de PC’s wordt na 15 minuten inactiviteit automatisch de schermbeveiliging geactiveerd. Deze is door de gebruiker met een wachtwoord weer te deactiveren en kan ook handmatig worden aangezet. Op de PC aangesloten PDA’s blijven actief, ook wanneer de schermbeveiliging aan staat. De meeste gebruikers laten hun pc tijdens hun afwezigheid aan staan, zonder de schermbeveiliging direct te activeren. De informatie is derhalve voor iedereen toegankelijk voordat de schermbeveiliging automatisch geactiveerd wordt.

Risico's

Het leeuwendeel van de vastgelegde profielen staan feitelijk in de productieomgeving (active directory) en is niet beleidsmatig vastgelegd op basis van een need to know principe. Hierdoor kan wildgroei ontstaan en is bij ernstige verstoringen de reproduceerbaarheid complex. Dit kan impact hebben op de gewenste vertrouwelijkheidseisen. De praktijk is dat de discipline om toegangsrechten van medewerkers op basis van controlelijsten te controleren, erg afhankelijk is van de medewerking van de lijnmanagers binnen de organisatieonderdelen en teams buiten het team ICT-beheer.

Het noteren en op een toegankelijke plek bewaren van wachtwoorden levert een aanzienlijk risico op, evenals het afstaan van inlog ID's en wachtwoorden.

Het niet 'locken' van de PC terwijl men de kamer verlaat levert vooral een risico op in kantoren waar men alleen zit maar ook tijdens pauzes en vergaderingen waarbij de gehele kamer leeg wordt achtergelaten.

Acties

- Voorzie alle informatiesystemen met gevoelige of kritieke informatie van logische toegangsbeveiliging.
- Leg een procedure vast voor het aanvragen en toewijzen van autorisaties.
- Onderzoek welke werkstations binnen de organisatie een verhoogd risico opleveren. Hiervoor moet een time-out worden ingesteld na enkele minuten
- Voor een clear screen beleid in: stel het uitschakelen, uitloggen of blokkeren ('locken') van de PC bij het verlaten van de werkplek verplicht en communiceer over het doel hiervan richting de medewerkers.
- Wijs als lijnmanagement de gebruikers op regelmatige tijden op clear desk en clear screen beleid.
- Overweeg het in gebruik nemen van een systeem voor single sign on.
- Verbied expliciet het noteren en toegankelijk maken van wachtwoorden. Communiceer hier actief over richting medewerkers.
- Verbied expliciet het afstaan van wachtwoorden aan anderen. Communiceer hier actief over richting medewerkers en leidinggevenden en wijs deze laatsten op alternatieven voor het organiseren van de continuïteit van de werkprocessen.
- Formaliseer het huidige de facto wachtwoordstandaardbeleid voor lengte, historie, samenstelling en levensduur.
- Stel functieprofielen op met toegangsbeleid voor afzonderlijke autorisaties/rechten en applicaties, beheer ze en borg het geheel met adequate periodieke controles.
- Ga over tot het registreren/documenteren van gebruikers(groepen) en het procedureel afhandelen van toegangsverzoeken.
- Rapporteer periodiek naar zowel het lijnmanagement als P&O (formatie) ter controle over toegangsrechten, speciale bevoegdheden en autorisatie van medewerkers. Controleer in overleg met P&O maandelijks mutaties in de formatie (HRM systeem) en koppel terug aan de verantwoordelijke managers.
- Draag zorg voor nauwlettende beheersing van het gebruik van systeemhulpmiddelen waarmee de normale beveiliging in systemen en toepassingen kan worden omzeild .

11.3 Toegangsbeheersing voor netwerken en besturingssystemen

Doelstelling

Het voorkomen van onbevoegde toegang tot netwerkdiensten.

De toegang tot zowel interne als externe netwerkdiensten behoort te worden beheerst.

De gebruikerstoegang tot netwerken en netwerkdiensten behoort de veiligheid hiervan niet in gevaar brengen. Dit kan worden gerealiseerd door te zorgen voor:
a) geschikte interfaces tussen het netwerk van de organisatie en netwerken van andere organisaties, en openbare netwerken;
b) geschikte authenticatiemiddelen voor gebruikers en apparatuur;
c) strikte beheersing van toegang tot informatiediensten.

Voorkomen van onbevoegde toegang tot besturingssystemen.

Er behoren beveiligingsvoorzieningen te worden gebruikt om de toegang tot besturingssystemen te beperken tot bevoegde gebruikers. De voorzieningen behoren in staat te zijn tot:

- het authenticeren van bevoegde gebruikers in overeenstemming met een gedefinieerd toegangsbeleid;
- het registreren van geslaagde en mislukte pogingen tot systeemauthenticatie;
- het registreren van het gebruik van speciale systeembevoegdheden;
- het genereren van een alarm wanneer inbreuk wordt gemaakt op het beleid voor toegangsbeveiliging;
- het bieden van passende middelen voor authenticatie;
- het indien nodig beperken van de verbindingstijd van gebruikers.
- Het voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

Er behoren beveiligingsvoorzieningen te worden getroffen om toegang tot en binnen toepassingssystemen te beperken.

Logische toegang tot toepassingsprogrammatuur en informatie behoort te worden beperkt tot bevoegde gebruikers.

Toepassingssystemen behoren:

- de toegang tot de functies van de informatie- en toepassingssystemen te beheersen in overeenstemming met het vastgestelde toegangsbeleid;
- bescherming te bieden tegen onbevoegde toegang tot alle hulpprogramma's en programmatuur van het besturingssysteem en virussen waarmee beheersmaatregelen in systemen of toepassingen kunnen worden gepasseerd;
- de beveiliging niet in gevaar te brengen van andere systemen waarmee informatiebronnen worden gedeeld.

Beheersmaatregelen

- Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.
- Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.
- Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authenticeren.
- De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.
- Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
- Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen (zie 11.1).
- Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.
- Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.
- Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
- Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
- Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd, behoort te worden beperkt en behoort strikt te worden beheerst.

- Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.
- De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.
- Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.
- Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.

Feitelijke situatie gemeente Deventer

Het netwerk binnen de gemeente Deventer is de facto standaard ingericht en toegang tot netwerkbronnen en applicaties wordt met name via de Active Directory beheerd en via de domeinspecifieke systemen waar van toepassing.

De acceptatie en productie netwerkomgeving zijn logisch/virtueel gescheiden zonder trust.

Externe toegang (Outlook Web Acces en intranet/SharePoint) is met het Secure Socket Layer (SSL) protocol versleuteld en de toegang tot informatie met de classificatie vertrouwelijk en hoger is afgesloten (beperkt tot openbare informatie van het intranet). Remote toegang voor UNIX/Oracle/SAP is procedureel vastgelegd en herleidbaar tot een individuele medewerker van PinkRoccade (CAG Connect).

Er zijn geen (logisch) gescheiden netwerken voor de verschillende niveaus van vertrouwelijkheid (openbaar, bedrijfsgeheim, vertrouwelijk en zeer geheim).

Het thuiswerken met (domein) specifieke applicaties is niet mogelijk. Er is wel toegang tot de Outlook (mail/agenda) omgeving en het intranet.

Een firewall wordt toegepast voor externe verbindingen/Internet, beheerd in samenwerking met een externe partij. Voor specifieke verbindingen, zoals SUWINET, GBA (VPN/SSL, PKI certificaten, GemNet) wordt voldaan aan de extern opgelegde eisen.

VPN tokens voor leveranciers en beheerder worden gebruikt.

Risico's

De beveiliging van het netwerk zelf, is voor een belangrijk deel afhankelijk van de fysieke beveiliging hiervan. Een professionele hacker die toegang weet te krijgen tot het netwerk kan toegang krijgen tot vertrouwelijke informatie, ongemerkt gegevens veranderen en denial-of-service aanval inzetten. Dit kan significante impact hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie. Het gebruik van gescheiden netwerken, extra encryptie en extra fysieke maatregelen is relatief duur.

Acties

- Onderzoek de inzet van een Intrusion Detection & Protection systeem.
- Neem beveiliging op dit terrein expliciet mee bij de eisen voor een nieuw stadskantoor.

11.4 Draagbare computers en telewerken

Doelstelling

Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.

De vereiste bescherming behoort in overeenstemming te zijn met de risico's die zijn verbonden aan deze manier van werken. Bij draagbare computers behoort rekening te worden gehouden met de risico's van werken in een onbeschermde omgeving, en behoren geschikte beschermingsmaatregelen te worden genomen. Bij telewerken behoort de organisatie bescherming aan te brengen op de locatie waar het telewerken plaatsvindt en te waarborgen dat geschikte voorzieningen zijn aangebracht voor deze manier van werken.

Beheersmaatregelen

- Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.
- Er behoren beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

Feitelijke situatie gemeente Deventer

De inzet van laptops, MDA's en iPads binnen Gemeente Deventer is beperkt, maar het gebruik neemt toe. MDA's kunnen in noodgevallen op afstand worden gedeactiveerd, bijvoorbeeld in geval van diefstal. Binnen de huidige demilitarized zone (DMZ) omgeving is een beperkt aantal applicaties beschikbaar. Het structureel en meer toepassen van telewerken is beleidsmatig nog niet vastgesteld.

Informatie op mobiele apparatuur wordt niet versleuteld.

Voor de laptops voor algemeen gebruik binnen de organisatieonderdelen zijn de betrokken onderdelen zelf verantwoordelijk. Laptops in gebruik bij specifieke medewerkers zijn bij ICT-beheer geregistreerd in HP OpenView (alle systemen die aan het netwerk zijn gekoppeld zijn onder beheer van het team ICT-beheer).

Risico's

De inzet van laptops levert een relatief hoog risico op. De eindgebruiker dient zelf te zorgen voor backups en de fysieke bescherming. Het toepassen van encryptie en het regelmatig updaten van laptops door het team ICT-beheer vermindert risico's (antivirus, security patches, updates, etc.). Het toepassen van cryptografische oplossingen voor laptops vermindert het risico aanzienlijk en is relatief betaalbaar.

Te nemen maatregelen

- Heroverweeg het besluit om geen encryptie toe te passen op laptops andere mobiele apparatuur.
- Formuleer beleid ten aanzien van telewerken voor een veilige toegang tot applicaties, en de SharePoint omgeving waarbij de beschikbaarheid van de systemen gegarandeerd blijft.
- Stel een goede registratie op over het aantal in gebruik zijnde MDA's, iPads en laptops. Leg hierin in elk geval vast, wie de verantwoordelijke gebruiker is en welke applicaties benaderd kunnen worden met het apparaat.

12 Verwerving, ontwikkeling en onderhoud van informatiesystemen

Acties
Geen specifieke aanbevelingen die niet elders behandeld zijn.

13 Beheer van informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling

Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Er behoren formele procedures voor rapportage van gebeurtenissen en escalatie te zijn. Alle werknemers, ingehuurd personeel en externe gebruikers behoren op de hoogte te zijn van de procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen. Zij behoren te worden verplicht om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

Beheersmaatregel

- Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
- Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en –diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

Feitelijke situatie gemeente Deventer

Er worden over het algemeen geen beveiligingsincidenten vastgelegd. Er wordt niet over beveiligingsincidenten gerapporteerd. Het kennisniveau is in het grootste deel van de organisatie vrij laag.

Voor het omgaan met verdachte poststukken (‘poederbrieven’) is een protocol opgesteld met betrekking tot afhandeling en rapportage.

Er hebben zich echter wel (potentiële) incidenten voorgedaan. Deze worden soms besproken op teamniveau. In de praktijk wordt er intuïtief met incidenten omgegaan, op grond van ervaring en inschatting; en alleen wanneer iemand dat nodig acht.

Risico’s

Omdat niet geregistreerd wordt is niet duidelijk wanneer en waar er zich daadwerkelijk incidenten voor doen. Op deze wijze wordt er onvoldoende lering uit getrokken om deze incidenten in de toekomst te kunnen voorkomen en/of de gevolgen op te vangen. De ervaringen kunnen zowel worden gebruikt daar waar het incident zich heeft voorgedaan als ook elders in de organisatie.

Acties

- Creëer bewustwording bij medewerkers en management.
- Stel een beveiligingsincidentmeldingsformulier op waarmee beveiligingsincidenten kunnen worden gemeld en geregistreerd.
- Informatiebeveiligingsincidenten worden standaard besproken in het teamoverleg van het desbetreffende team.
- Alle informatiebeveiligingsincidentformulieren worden beschikbaar gesteld aan de informatiebeveiligingscoördinator.
- Alle beveiligingsincidenten die te maken hebben met geautomatiseerde gegevensverwerking worden door een medewerker van team ICT-beheer afgehandeld en als dit van toepassing is, gerapporteerd aan het betreffende teamhoofd en de formulieren worden gearchiveerd.
- Applicatiebeheerders moeten begeleid worden in het administreren en begeleiden van problemen in de informatiesystemen.

13.2 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling

Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

Er behoren verantwoordelijkheden en procedures te zijn voor het doeltreffend behandelen van informatiebeveiligingsgebeurtenissen en zwakke plekken, zodra ze zijn gerapporteerd. Er behoort een proces van continue verbetering te worden toegepast op het reageren op, controleren, beoordelen en beheer van informatiebeveiligingsincidenten.

Waar bewijs vereist is behoort het te worden verzameld om naleving van wettelijke eisen te waarborgen.

Beheersmaatregel

- Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.
- Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.

Feitelijke situatie gemeente Deventer

Het beheer(s)en van incidenten kan pas opgepakt worden als de registratie van incidenten goed verloopt. Dit proces is nog niet ingeregeld binnen de gemeente Deventer.

Risico's

Het niet beheren van informatiebeveiligingsincidenten kan betekenen dat bij het bijstellen van beleid onvoldoende informatie beschikbaar is om herhaling te verkomen en de voortgang van het nemen van adequate maatregelen onvoldoende bewaakt wordt.

Acties

- Voer op korte termijn eerst de acties uit met betrekking tot rapportage van informatiebeveiligings-gebeurtenissen en zwakke plekken.

14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Doelstelling

Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

Er behoort een beheerproces van bedrijfscontinuïteit te worden geïmplementeerd om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie (als gevolg van bijvoorbeeld natuurrampen, ongevallen, uitval van apparatuur en opzettelijke handelingen) en het herstellen daarvan tot een aanvaardbaar niveau te beperken, door een combinatie van preventieve maatregelen en herstelmaatregelen. Dit proces behoort de kritische bedrijfsprocessen te identificeren. Het behoort de informatiebeveiligingseisen voor de bedrijfscontinuïteit te integreren met andere continuïteiteisen, die betrekking hebben op aspecten als operaties, personeel, materialen, transport en voorzieningen.

De gevolgen van rampen, beveiligingsincidenten, uitval van diensten en de beschikbaarheid van diensten behoren te worden beoordeeld aan de hand van een business impact analyse. Er behoren continuïteitsplannen te worden ontwikkeld en geïmplementeerd om het tijdig hervatten van essentiële bedrijfsprocessen te waarborgen. Informatiebeveiliging behoort een integraal onderdeel te zijn van het totale bedrijfscontinuïteitproces en andere beheerprocessen binnen de organisatie.

Het beheerproces van bedrijfscontinuïteit behoort beheersmaatregelen te omvatten voor het identificeren en verminderen van risico's, als aanvulling op het algemene risicobeoordelingsproces, het beperken van de consequenties van incidenten die schade toebrengen en veiligstellen dat informatie die vereist is voor het bedrijfsproces vlot weer beschikbaar is.

Beheersmaatregel

- Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden. Onderdeel daarvan is ook een beheerd proces voor de naleving van eisen voor de informatiebeveiliging die nodig is voor de continuïteit van de bedrijfsvoering.
- Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.
- Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.
- Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.
- Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdate, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

Feitelijke situatie gemeente Deventer

Fragmentarisch zijn plannen aanwezig (GBA, SUWI) en zijn continuïteitsmaatregelen genomen zoals het dubbel uitvoeren van infrastructuurcomponenten. Echter, het proces is niet geborgd en continuïteit wordt niet getest.

Onlangs is voor delen van de organisatie een continuïteitsplan voor het opvangen van een grieppandemie gemaakt.

Bewustwording van informatiebeveiliging als continuïteitsverhogende maatregel is betrekkelijk laag. Continuïteit is alleen relatief goed geregeld bij die processen waar extra druk aanwezig is (GBA). Echter bij een moderne architectuur (bijvoorbeeld midoffice) is het uitwijken van een systeem niet meer toereikend. Het gaat niet over continuïteit van systemen maar over continuïteit van processen.

Dit laatste is in een architectuur van front- mid en back-officetoepassingen complexer dan bij traditionele client-server-toepassingen.

Ook op een lager niveau van bijvoorbeeld individuele medewerkers (kennis, vaardigheden) en/of systemen dient de continuïteit gewaarborgd te zijn.

Risico's

Binnen de organisatie is tot op heden, buiten het afsluiten van een uitwijkcontract, weinig invulling gegeven aan continuïteitsplanning. Naast een vals gevoel van veiligheid is er ook grote kans op ad hoc maatregelen als een calamiteit zich daadwerkelijk voordoet.

Het risico op het uitvallen van medewerkers (ziekte, sterven, ontslag) vormt een reële bedreiging.

Acties

- Stel een Bedrijfs Continuïteits Plan (BCP) op. Het doel van een BCP is het adequaat kunnen reageren op verstoringen van bedrijfsactiviteiten en het beschermen van kritieke bedrijfsprocessen tegen de effecten van grote storingen of calamiteiten. Continuïteitsplanning is vereist om kritieke bedrijfsprocessen te beveiligen tegen omvangrijke storingen of calamiteiten. Er dienen procedures te worden opgesteld voor het ontwikkelen en handhaven van herstelplannen ter beveiliging van kritieke bedrijfsprocessen en diensten. Het doel van continuïteitsplanning is het beperken van de risico's als gevolg van doelbewuste of onvoorziene bedreigingen van vitale diensten; het zo spoedig mogelijk herstellen en handhaven van kritieke bedrijfsactiviteiten na een omvangrijke storing of calamiteit.
    - Geadviseerd wordt om een continuïteitsplan op te stellen waarin de kritische processen en diensten zijn opgenomen.
    - Per kritisch proces moet worden bepaald wat de eventuele gevolgen zijn van de verschillende calamiteiten voor de bedrijfsactiviteiten.
    - Alle verantwoordelijkheden en noodvoorzieningen moeten worden gespecificeerd en goedgekeurd.
    - Alle overeengekomen procedures en processen moeten worden gedocumenteerd.
    - Het personeel moet worden getraind in hoe te handelen in geval van een calamiteit.
    - De procedures dienen periodiek getest en aangepast te worden, ook na belangrijke wijzigingen in de organisatie/systemen.
- Een bedrijfscontinuïteitsplan (calamiteitenplan) is algemeen geldend voor de gehele organisatie en heeft niet exclusief betrekking op computerbeveiliging.
- Geadviseerd wordt om voorzieningen te treffen om te kunnen uitwijken, hetgeen aantoonbaar dient te worden gemaakt door het overleggen van een schriftelijke uitwijkprocedure en een uitwijkovereenkomst met een uitwijkleverancier.
    - Verbeter de uitwijkprocedure, waarbij ook rekening gehouden dient te worden met het werken (dus niet alleen opstarten) op een alternatieve locatie.
    - Breidt de uitwijktest uit met een beproeving van het interne deel van de procedure en leg de resultaten hiervan vast.
    - Breidt de rapportage van de uitwijktest uit met het interne deel van de beproeving c.q. breidt de uitwijktest uit met het interne deel van de beproeving.
- Laat in 2012 of na belangrijke wijzigingen in de ICT-infrastructuur, een volledige *legal hack* / penetratietest uitvoeren. Dit creëert enerzijds bewustwording bij bestuur, management en medewerkers en is anderzijds een goed startpunt om technische onvolkomenheden structureel op te pakken.
- Voer per team/proces een risicoanalyse uit gericht op het waarborgen van beschikbaarheid van informatie, waarbij met name ook aandacht wordt besteed aan uitval en vervangbaarheid van medewerkers. Besteed zo nodig aandacht aan proces- en werkbeschrijvingen en onderlinge uitwisselbaarheid.

15 Naleving

15.1 Naleving van wettelijke voorschriften

Doelstelling

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseis.

Ontwerp, bediening, gebruik en beheer van informatiesystemen kunnen zijn onderworpen aan eisen uit weten regelgeving en contractuele beveiligingseisen.

Er behoort advies over specifieke juridische eisen te worden ingewonnen bij de juridische adviseurs van de organisatie of bij gekwalificeerde juristen. Wettelijke eisen verschillen van land tot land en kunnen verschillen voor informatie die in het ene land wordt gecreëerd en naar een ander land wordt verzonden (d.w.z. grensoverschrijdend gegevensverkeer).

Beheersmaatregelen

- Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden voor elk informatiesysteem en voor de organisatie.
- Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.
- Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
- De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.
- Gebruikers behoren ervan te worden weerhouden IT-voorzieningen te gebruiken voor onbevoegde doeleinden.
- Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

Feitelijke situatie gemeente Deventer

Er is geen overzicht over relevante regelgeving en verplichtingen vastgelegd. Er kan niet eenvoudig worden nagegaan in hoeverre de organisatie de voorschriften naleeft. Er is geen procedure voor documentatie en actualisatie. Dit geldt zowel voor de organisatie als geheel als voor informatiesystemen.
Er zijn geen procedures ten aanzien van het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten.
Er zijn weinig tot geen organisatiebrede voorschriften of richtlijnen over het omgaan met relevante regelgeving.

De gemeente voldoet in grote lijnen aan de eisen zoals deze zijn gesteld in de regelgeving ten aanzien van de officiële archivering. De centrale documentmanagementorganisatie heeft de informatiebeveiliging adequaat geregeld. Daarnaast zijn er decentrale archieven (werkarchieven). Hiervan is het thans onvoldoende duidelijk of volgens de voorschriften gehandeld wordt. Dit geldt voor zowel de vertrouwelijkheid, betrouwbaarheid als ook beschikbaarheid, maar ook voor zaken als bijvoorbeeld de verplichte vernietiging (op termijn.)

Het terugvinden van informatie uit de archiefsystemen en/of de werkbestanden is vaak moeizaam daar waar het uitsluitend digitaal vastgelegde informatie betreft. Het toekennen van metadata aan bestanden is niet algemeen gebruikelijk. Dit maakt het efficiënt en effectief voldoen aan een informatieverzoek op basis van de Wet Openbaarheid Bestuur (WOB) een potentieel moeilijke zaak.

Voor het behandelen van specifieke geadresseerde inkomende post is een regeling opgesteld. Deze is echter niet algemeen bekend en wordt (daardoor) niet altijd gevolgd.

In de praktijk zijn er tal van voorbeelden aan te dragen waarin de gemeente Deventer heeft gehandeld in strijd met de vereisten van de Wet Bescherming Persoonsgegevens (zowel met betrekking tot de eigen medewerkers als ook wat betreft klanten/burgers) of de auteurswet.

Bij veel besluiten omtrent het registreren of het verwerken van persoonsgegevens van medewerkers wordt verzuimd instemming aan de ondernemingsraad te vragen. Het zelfde geldt voor (softwarematige of in andere vorm) controle instrumenten voor het personeel.

De inrichting van de ICT onder beheer van het team ICT-beheer voldoet adequaat aan de relevante wetgeving. De belangrijke applicaties en gegevensverzamelingen zijn adequaat beschermd tegen verlies, vernietiging en vervalsing. Maatregelen zijn genomen om het door gebruikers zelf installeren van (illegale) software en hardware niet mogelijk te maken of tot het minimum te beperken. Het team ICT-beheer werkt zelf uitsluitend met gelicenceerde software. Er is onvoldoende inzicht in (het bestaan van) de softwareovereenkomsten voor software die ten behoeve van de organisatieonderdelen wordt geïnstalleerd.

Risico's

Het niet voldoen aan wettelijke eisen kan leiden tot reputatie- en imagoschade, tot ernstige problemen bij juridische procedures en kan eventueel (financiële) sancties tot gevolg hebben.

Het probleem van het terugvinden van relevante informatie in digitale bestanden is reëel, en neemt naarmate meer digitaal gewerkt gaat worden toe.

Acties

- Stel formeel - maar vooral feitelijk - een beveiligingscoördinator aan die vanuit deze rol als aanjager en vraagbaak functioneert voor informatiebeveiliging.
- Deze beveiligingscoördinator is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit de baseline. De beveiligingscoördinator rapporteert periodiek aan het managementteam, zo nodig zonder tussenkomst van het teamhoofd. Onder een beveiligingscoördinator wordt verstaan: een functionaris die kennis en ervaring heeft op het gebied van informatiebeveiliging en op dit terrein een adviserende en coördinerende rol kan vervullen.
- De beveiligingscoördinator is verantwoordelijk voor:
    - Voorbereiding beveiligingsbeleid en –plan.
    - Rapportage (beveiligingsincidenten).
    - Het beheer van en toezicht op de naleving van de beveiligingsprocedures.
    - Het minstens eenmaal per jaar verzorgen van voorlichting en instructie aan medewerkers door middel van toetsing van de opgestelde beveiligingsprocedures in de praktijk.
    - Het introduceren en bekendmaken van nieuwe medewerkers met de beveiligingsprocedures.
- Stel voor de organisatie als geheel de relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen expliciet vast en implementeer een procedure om deze actueel te houden.
- Doe dit zelfde voor elk informatiesysteem.
- Stel een procedure op voor het omgaan met materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.
- Zorg dat in contacten met de teams door de adviseurs vanuit Intern Ondersteunen expliciet aandacht wordt gevraagd voor informatiebeveiliging.
- Stel een regeling op voor het omgaan met specifiek geadresseerde inkomende post ('briefgeheim') en zorg dat deze bekend wordt en gehandhaafd in de gehele keten van postafhandeling.
- Informatie die op internet wordt gepubliceerd of per (elektronische) post wordt verspreid wordt ontdaan van persoonsgegevens en niet noodzakelijke adresgegevens.
- Informatie die op intranet of op een shared schijfruimte wordt gepubliceerd, wordt ontdaan van niet noodzakelijke persoonsgegevens en adresgegevens.
- Schaduwarchieven (thuis, op kantoor, in de cloud; fysiek of digitaal) met vertrouwelijke informatie worden niet langer toegestaan.

- Stel een protocol op voor het meenemen van informatie naar huis en voor thuiswerken.
- Voorzie alvorens documenten te publiceren op internet of op intranet deze van de voor het terugvinden benodigde metadata.
- Leg alvorens een persoonsregistratie voor de bij de gemeente werkzame personen wordt aangelegd of wordt besloten over vaststellen, wijzigen of intrekken van een regeling op het gebied van verwerken of de bescherming van persoonsgegevens van de bij de gemeente werkzame personen deze registratie of dit besluit ter instemming voor aan de ondernemingsraad.
- Leg alvorens een besluit wordt genomen tot vaststelling, wijziging of intrekking van een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de bij de gemeente werkzame personen dit besluit ter instemming voor aan de ondernemingsraad.

15.2 Naleving van beveiligingsbeleid en -normen en technische naleving

Doelstelling

Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

De beveiliging van informatiesystemen behoort regelmatig te worden beoordeeld.

Dergelijke beoordelingen behoren te worden uitgevoerd op basis van het desbetreffende beveiligingsbeleid en technische platforms en informatiesystemen behoren te worden beoordeeld op naleving van toepasselijke normen voor de implementatie van de beveiliging en gedocumenteerde beveiligingsmaatregelen.

Beheersmaatregelen

- Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.
- Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.

Feitelijke situatie gemeente Deventer

Er zijn geen extra richtlijnen of procedures om naleving op relevante beveiligingsvoorschriften af te dwingen. Het installeren van hardware en software is deels verhinderd met beperkende policies binnen de netwerkomgeving c.q. het standaard werkstation.
Informatiesystemen worden niet regelmatig gecontroleerd op naleving van implementatie van beveiligingsnormen.

Risico's

In zijn algemeenheid geldt dat beleid dat niet wordt vertaald naar concrete voorschriften en/of nageleefd c. q. afgedwongen wordt in de praktijk verwordt tot loze letters.

Acties

- Maak uitsluitend gebruik van software waarvoor een licentieovereenkomst is afgesloten.
- Verhinder het zelf kunnen installeren en gebruiken van niet geautoriseerde software en hardware.
- Maak duidelijk dat misbruik of niet volgen van de in de baseline vastgelegde afspraken uiteindelijk ook tot disciplinaire maatregelen zal leiden.
- Draag als management (eventueel gemandateerd aan team ICT-beheer) nog meer actief uit dat het kopiëren (en dus ook installeren) van software niet legaal is, tenzij de leverancier hiervoor toestemming heeft gegeven.
- Stel concrete richtlijnen op inzake relevante regelgeving en organisatiebeleid.
- Geef meer aandacht aan de richtlijnen en de handhaving daarvan.
- Stel, omdat de gemeente verantwoordelijk is voor de op de pc's geïnstalleerde software, periodiek vast dat zich geen illegale software op de werkstations bevindt.

15.3 Overwegingen bij audits van informatiesystemen

Doelstelling

Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

Er behoren beheersmaatregelen te worden genomen om productiesystemen en audithulpmiddelen te beveiligen tijdens informatiesysteemaudits.

Bescherming is ook vereist om de integriteit van hulpmiddelen voor audits te waarborgen en misbruik van deze hulpmiddelen te voorkomen.

Beheersmaatregelen

- Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.
- Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbuik of compromittering te voorkomen.

Feitelijke situatie gemeente Deventer

Behoudens de wettelijk voorgeschreven audits vinden er geen (door het college of door IAO/ ICT-beheer) reviews of audits plaats op het gebied van informatiebeveiliging.

Risico's

Het is niet geborgd dat alle systemen en processen voldoen aan de eisen die zijn vastgelegd. Eventuele incidenten, komen dan pas laat of niet aan de oppervlakte.

Acties

- Stel een procedure op om ervoor zorg te dragen dat de in dit plan gehanteerde beveiligingsnormen worden nageleefd. Laat regelmatige interne of externe audit deel uitmaken van deze procedure.

Bijlagen

Bijlage 1 – beleidsuitgangspunten[5]

De gemeente Deventer hanteert de volgende 10 uitgangspunten bij het informatiebeveiligingsbeleid. Deze uitgangspunten zijn ontleend aan het standaard raamwerk voor informatiebeveiliging: de Code voor Informatiebeveiliging van het Nederlands Normalisatie Instituut ((NEN-ISO 17799), uitgave 2002.

1. Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid voor de hele gemeente.
2. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het College van B & W als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd. Daar waar derden toegang hebben tot de informatievoorziening worden aanvullende beveiligingsmaatregelen genomen om de beschikbaarheid/-continuïteit, betrouwbaarheid/integriteit en vertrouwelijkheid/exclusiviteit van de (geautomatiseerde) gegevensverwerking te waarborgen.
3. De gemeente beschikt over een overzicht van alle belangrijke ICT-bedrijfsmiddelen zoals gegevens, programmatuur, fysieke middelen en diensten. De gegevens en ICT-bedrijfsmiddelen hebben een expliciet gedefinieerde eigenaar, die verantwoordelijk is voor de juiste beveiligingsmaatregelen. De verantwoordelijkheid voor de implementatie van beveiligingsmaatregelen mag worden gedelegeerd, maar de eigenaar blijft verantwoordelijk. Alle belangrijke ICT-bedrijfsmiddelen worden geclassificeerd naar de beveiligingsaspecten: vertrouwelijkheid, beschikbaarheid en betrouwbaarheid. Door middel van beveiligingsclassificaties worden de prioriteiten voor beveiliging aangegeven.
4. Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle gebruikers van informatiesystemen worden getraind in het gebruik van beveiligingsprocedures. Zij worden geïnformeerd over hun toegangsrechten en beperkingen. Er is een formele procedure of calamiteitenplan, waarin staat hoe men om moet gaan met beveiligingsincidenten, zodat deze zo snel mogelijk via de juiste kanalen gerapporteerd worden.
5. ICT-voorzieningen die bedrijfskritische of gevoelige activiteiten binnen de gemeente ondersteunen, worden in beveiligde ruimten ondergebracht. De fysieke beveiliging van de ruimten is zodanig dat alleen bevoegd personeel toegang kan krijgen. In beveiligde ruimten is detectieapparatuur geïnstalleerd, zoals warmte- en rookdetectors en inbraak- en waterdetectors. Tevens is de stroomvoorziening van bedrijfskritische Richtapparatuur adequaat beveiligd.
6. De gemeente bepaalt verantwoordelijkheden en procedures voor het beheer en de bediening van alle communicatie- en bedieningsprocessen. Er zijn maatregelen genomen voor preventie en detectie van virussen en andere van buitenaf komende dreigingen. Ook stelt men adequate procedures op om het bewustzijn bij gebruikers te vergroten. De gemeente installeert programmatuur tegen virussen en andere bedreigingen en vernieuwt deze periodiek. Binnenkomende informatiedragers worden op virussen en andere bedreigingen gecontroleerd. Het gebruik van illegale software is expliciet verboden en er zijn sancties indien men hieraan niet voldoet. Daarnaast zijn adequate maatregelen getroffen voor het maken van reservekopieën (back-ups).
7. Het toegangsbeleid voor informatiesystemen is gedefinieerd en gedocumenteerd. De eigenaar van een toepassing is verantwoordelijk voor het toegangsbeleid van de desbetreffende toepassing en alle gebruikers beschikken over een unieke user-id en password.
8. Beveiligingseisen worden onderkend en goedgekeurd voordat ICT-systemen worden geïmplementeerd. Hiervoor wordt een analyse van de beveiligingseisen uitgevoerd tijdens het specificeren van de eisen voor elk nieuw project. Het ontwikkelen/invoeren en testen van nieuwe systemen wordt gescheiden van de operationele systemen om continuïteit en betrouwbaarheid te behouden. De gemeente stelt onderhoudsroosters en ondersteunende onderhoudscontracten op voor alle ICT-apparatuur.
9. Continuïteitsmanagement en -planning wordt gebruikt ter beveiliging van de bedrijfskritische processen tegen omvangrijke storingen of calamiteiten. Hiertoe beschikt de gemeente over continuïteitsplannen voor alle bedrijfskritische processen en diensten. Ook beschikt de gemeente over een zodanige (externe) uitwijkmogelijkheid voor de informatievoorziening dat in geval van een calamiteit of noodsituatie binnen redelijke termijn de noodzakelijke systemen en gegevens weer beschikbaar zijn.
10. Het ontwerp, de bediening, het gebruik en beheer van informatiesystemen zijn onderworpen aan statutaire, wettelijke of contractuele beveiligingseisen. De gemeente zorgt voor de naleving van wettelijke en contractuele voorschriften. Door interne controle en periodiek externe toetsing wordt ervoor gezorgd dat de informatievoorziening voldoet aan het vastgestelde beveiligingsbeleid en aan de geldende beveiligingsnormen. Hierbij gaat het onder andere om zaken als het gebruik van illegale programmatuur, de naleving van licentieovereenkomsten en beveiliging van persoonsgegevens.

[5] Uit: B&W Nota Informatiebeveiliging (notanr. 2007.10943)

Bijlage 2 – Workshops baseline informatiebeveiliging

Workshops
Voor de totstandkoming van de baseline is het beleidsterrein in relatief afgebakende deelgebieden opgeknipt. Per deelgebied is een workshop gehouden met procesdeskundigen en de procesverantwoordelijken (beslissers) op dit specifieke gebied.

Omdat de aandachtsgebieden die het plan bestrijkt voornamelijk zijn belegd bij de (inmiddels opgeheven) eenheid Bedrijfsvoering hebben met name vanuit deze eenheid deskundigen deelgenomen aan de workshops. Hierbij is nadrukkelijk niet alleen gekeken naar de situatie binnen het eigen team of de eenheid, maar ook gebruik gemaakt van de aanwezige kennis bij de ondersteunende diensten van de organisatie als geheel.

De volgende workshops zijn gehouden:

- Documentair/archivering;
- Fysieke beveiliging/facilitair;
- Financieel/administratief;
- Juridisch/inkoop;
- Personeel & organisatie;
- Algemeen; ter voorbereiding op de workshops is een gezamenlijke bijeenkomst gehouden met de deelnemers aan de verschillende workshops. Dit om bewustwording voor het onderwerp te creëren en alvast het denkproces over het eigen deelproces op gang te brengen, ter voorbereiding op de workshops.

De workshops zijn gebruikt om:

- een beeld te krijgen van de risico's die bestaan op het betreffende deelgebied binnen de organisatie (afhankelijkheid, kwetsbaarheid);
- een beeld te krijgen van de ter beheersing van risico's al getroffen maatregelen (wat is er geregeld).
- (resulterend in) een beeld van de risico's die nog resteren.

Aan elk van de workshops hebben ook meerdere medewerkers van het team IAO deel genomen.

In elke workshop zijn alle 11 verschillende aandachtsgebieden uit de Code voor Informatiebeveiliging langsgelopen - niet alleen die voor het eigen specialisme - om een zo compleet mogelijk beeld te krijgen. Hierbij is er ruimte geboden om breder te kijken dan alleen het deelterrein van de workshop; wanneer er risico's gesignaleerd zijn buiten het eigen vakgebied of aanbevelingen werden gedaan zijn deze meegenomen, en indien van toepassing ook in volgende workshops ter sprake gebracht.

Een algemene opmerking die gemaakt kan worden is dat informatiebeveiliging bij de meeste betrokkenen als zodanig niet een direct herkenbaar begrip was. Met name de noties dat informatiebeveiliging meer is dan alleen ICT en dat bedrijfscontinuïteit één van de doelstellingen van informatiebeveiliging is was voor velen een nieuw inzicht. En zo men zich er al een duidelijk beeld van kon vormen was voor velen de eigen rol hierin toch in eerste instantie nog onduidelijk ("maar wat heb ik/wat heeft mijn team daarmee te maken?".)

Daarom zijn de workshops als instrument om ´bewustwording´ met betrekking tot informatiebeveiliging te bevorderen erg nuttig geweest.

Algemeen – teams BV / verantwoordelijkheid

Zoals uit de conclusies naar voren is gebracht, hanteert Deventer het principe van integraal management waarbij de verantwoordelijkheid voor alle bedrijfsvoeringsaspecten – inclusief informatiebeveiliging - laag in de organisatie bij de diverse teamleiders is neergelegd. Richtlijnen op het gebied van informatiebeveiliging ontbreken grotendeels of nemen de vorm aan van adviezen - met de bijbehorende keuzevrijheid.

Dit heeft er toe geleidt dat het niveau van informatiebeveiliging sterk afhangt van de mate waarin de individuele teamleiders en/of procesverantwoordelijken er aandacht aan besteden of zich bewust zijn van risico's die worden gelopen.

Er zijn grote verschillen te constateren tussen de verschillende teams binnen de organisatie en de mate waarin informatiebeveiliging ‘op de agenda’ staat. In de meeste gevallen is men zich onvoldoende bewust van het verschijnsel, en van de risico’s die gelopen worden. Er bestaat in de meeste gevallen onvoldoende inzicht in welke informatie aanwezig is en in hoeverre deze beveiligd dient te worden. Ook bestaande wettelijke voorschriften zijn in veel gevallen onbekend, en daarmee ook vaak de naleving van de voorschriften.

Binnen de teams van BV die aan de workshops en interviews hebben deelgenomen is dit zelfde verschil ook zeer duidelijk zichtbaar.

Binnen BV hebben de teams het onderwerp informatiebeveiliging binnen het eigen, relatief beperkte, verantwoordelijkheidsgebied op de meeste terreinen redelijk onder controle.

Echter, tussen de teams is een significant verschil in de mate waarin men zich verantwoordelijk acht voor dan wel betrokken acht voor informatiebeveiliging op het eigen specialisme binnen de rest van de organisatie; of zicht er op heeft/wil hebben. Binnen bepaalde teams leeft dit sterk, binnen andere is de opstelling meer een faciliterende: alleen bij een expliciete vraag wordt er geleverd; de verantwoordelijkheid ligt bij de decentrale teammanager/proceseigenaar.

Een punt van overeenkomt tussen alle teams is dat er over het algemeen weinig is gedocumenteerd. Zaken die geregeld zijn, maatregelen die zijn getroffen en werkwijzen die gevolgd worden, liggen niet vast en zijn veelal niet kenbaar voor anderen binnen het eigen team of de rest van de organisatie.

Het idee dat voorafgaand aan de workshops bestond dat met de workshops een goed beeld van de gehele organisatie gevormd kon worden, bleek slechts ten dele juist te zijn.

Documentair/archivering
Aan deze workshop hebben diverse medewerkers en de teamleider van het team DM deelgenomen.

Bij DM wordt een duidelijke bezorgdheid en betrokkenheid gevoeld voor de juiste, veilige omgang met informatie in en door de organisatie, die zich verder uitstrekt dan het eigen, formele (team-) verantwoordelijkheidsgebied.

De kennis binnen het team op documentair en archiefgebied binnen de organisatie is groot, en er zijn diverse risico’s binnen de organisatie gesignaleerd. Dit laatste zowel op het gebied van documentmanagement als ook op juridisch gebied, ten aanzien van ICT en met betrekking tot het inkoopproces.

De informatiebeveiliging onder verantwoordelijkheid van het *team* DM voldoet adequaat aan de vigerende regelgeving en de Code voor Informatiebeveiliging. Het niveau van informatiebeveiliging van het *aandachtgebied* documentair in de rest van de organisatie verschilt sterk, en is vaak te laag.

Fysieke beveiliging/facilitair
Aan deze workshop hebben diverse medewerkers van het team FZ deelgenomen.

Informatiebeveiliging is bij FZ geen onderwerp dat als zodanig geadresseerd wordt, en in de contacten van het team FZ met de organisatie wordt geen expliciete aandacht besteed aan aspecten van informatiebeveiliging.

FZ heeft diverse voorzieningen getroffen op het gebied van fysieke en/of toegangsbeveiliging. FZ heeft hier de rol van leverancier en uitvoerder, en voert het gemeentelijke beleid uit en biedt standaard faciliteiten aan. Wanneer er nadrukkelijk wordt gevraagd om een voorziening, dan zal deze (binnen de bestaande mogelijkheden) worden geleverd, en op aanvraag kunnen extra beveiligingsvoorzieningen worden getroffen.

FZ benadrukt het duidelijkst het standpunt van de verantwoordelijkheid van de decentrale teamleider en/of procesverantwoordelijke; FZ draagt/voelt hiervoor geen verantwoordelijkheid. Ook wat betreft informatie omtrent FZ zaken/mogelijkheden benadrukt FZ de eigen verantwoordelijkheid van medewerkers om informatie te *halen*, en ziet het niet als taak van FZ om deze te *brengen*. “Iedereen wordt geacht te wet te kennen, en ook de regels binnen de organisatie.”

De kennis binnen FZ van wat er op het gebied van fysieke beveiliging voor voorzieningen is getroffen binnen de organisatie is groot, en op deze wijze konden vele risico’s in kaart worden gebracht.

Op het gebied van het eigen team is het onderwerp informatiebeveiliging redelijk onder controle, vooral op het terrein van bedrijfscontinuïteit.

Financieel/administratief
Aan deze workshop hebben diverse medewerkers van de teams PC en GA deelgenomen, waaronder de teammanager.

Bij de deelnemers aan de workshop was veel kennis aanwezig over de financieel/administratieve processen binnen de organisatie als geheel alsmede zicht op de risico's die aanwezig zijn. De betrokkenheid bij het onderwerp informatiebeveiliging was relatief groot. Er kwamen behalve suggesties voor verbetering op het eigen vakgebied ook aandachtspunten op de terreinen ICT en P&O naar voren.

De financieel/administratieve processen binnen de organisatie zijn grotendeels geformaliseerd en vastgelegd. De processen zijn voorzien van autorisaties, functiescheidingen en controles. Hiermee zijn ook diverse aspecten van informatiebeveiliging afgedekt.

Op het gebied van de eigen teams is het onderwerp informatiebeveiliging adequaat geregeld.

Juridisch/inkoop

Voor dit onderwerp is gesproken met een medewerker en de teammanager van het team JZ, alsmede met een juridisch medewerker uit de eenheid StadThuis.

Vanuit het team JZ wordt de eigen verantwoordelijkheid binnen de organisatie benadrukt; JZ neemt geen verantwoordelijkheid voor juridische aspecten buiten het eigen team, heeft geen zicht op wat er bij de overige organisatieonderdelen gebeurt en ziet hier ook het belang niet van in, gezien de taakopdracht van het team.

Desgevraagd komt het team met juridische adviezen en ondersteuning voor de teams.. Het onderwerp informatiebeveiliging speelt hier bij in de praktijk geen rol en in de contacten van het team JZ(&I) met de organisatie wordt geen aandacht besteed aan aspecten van informatiebeveiliging.

Binnen het team JZ zelf krijgt het onderwerp informatiebeveiliging hoegenaamd geen aandacht.

Personeel & organisatie

Vanwege tijdgebrek en prioriteitsstelling bij het team P&O heeft deze workshop plaatsgevonden met twee medewerkers van het team P&O.

P&O benadrukt eveneens de decentrale verantwoordelijkheid voor zowel P&O-aspecten in het algemeen als ook voor het onderdeel informatiebeveiliging.

In de contacten van het team P&O met de organisatie wordt geen expliciete aandacht besteed aan aspecten van informatiebeveiliging en het zicht binnen het team P&O op aspecten van informatiebeveiliging binnen de organisatie is beperkt.

Vanuit P&O is weinig op het gebied van informatiebeveiliging geformaliseerd of vastgelegd, zowel wat betreft intern team P&O-gebruik of als handreiking naar de organisatie. Er zijn binnen het team zelf enkele zaken met betrekking tot informatiebeveiliging geregeld.

ICT

Voor het specifieke onderdeel centraal technisch ICT-beheer (team ICT-beheer) is vooruitlopend op deze algemene, gemeentgebrede baseline een onderzoek verricht door (Getronics) PinkRoccade Local Goverment B.V. Hierbij is in opdracht van de gemeente gebruik gemaakt van de systematiek van de Code voor Informatiebeveiliging, zoals deze ook in dit rapport en in de workshops is gebruikt. Voor dit onderzoek zijn diverse mensen vanuit de teams ICT-beheer en IAO geïnterviewd.

Voor zover de bevindingen uit dit onderzoek uitstijgen boven alleen het specifieke teamniveau van ICT-beheer zijn deze integraal opgenomen in de gemeentelijke baseline.

Uit dit onderzoek en uit de gehouden workshops komt naar voren dat binnen het team ICT-beheer veel kennis, betrokkenheid en verantwoordelijkheid wordt ervaren met betrekking tot informatiebeveiliging binnen het eigen vakgebied / verantwoordelijkheidsgebied. Ook is er redelijk zicht op ICT-informatiebeveiligingsaspecten binnen de rest van de organisatie. De zorg hiervoor wordt in lijn net de gemeentelijke decentrale verantwoordelijkheid niet als verantwoordelijkheid van het ICT-beheer team gezien, maar wel als een punt van zorg en aandacht.

De informatiebeveiliging onder verantwoordelijkheid van het *team* ICT-beheer voldoet adequaat aan de vigerende regelgeving en de Code voor Informatiebeveiliging. Het niveau van informatiebeveiliging van het *aandachtgebied* ICT in de rest van de organisatie verschilt sterk, en is vaak te laag.