Thema-audit

Informatiebeveiliging

Globaal rapport

Auditopdracht 1401 029

3 februari 2015

Vlaamse overheid

AUDIT VLAANDEREN

AUDIT
VLAANDEREN

Thema-audit informatiebeveiliging

Globaal rapport

Auditrapport:	**Thema-audit informatiebeveiliging - globaal rapport**
Datum:	3 februari 2015
Manager-auditor:	Jo Fransen
Auditteam:	Karel Bruneel, senior auditor Patricia Van de Capelle, senior auditor Tomas De Rycke, Manager, PwC Clément Herssens, Manager, PwC
Referentie:	1401 029

Deze opdracht is uitgevoerd in overeenstemming met de internationale standaarden van het Institute of Internal Auditors (IIA). Elke vijf jaar evalueert een externe instantie of Audit Vlaanderen deze standaarden naleeft.

Inhoudstafel en verzendlijst

Het rapport wordt verstuurd naar:

Voorzitter van het voorzitterscollege

De heer Martin Ruebens	Secretaris-generaal Departement Diensten voor het Algemeen Regeringsbeleid

Voorzitter van het coördinatiecomité bij de Vlaamse Dienstenintegrator (VDI)

De heer Frank Geets	Administrateur-generaal van het Agentschap Facilitair Bedrijf

De leidend ambtenaren van de entiteiten die gevat werden door deze thema-audit

De heer Frans Cornelis	Administrateur-generaal van het Agentschap voor Overheidspersoneel
De heer Helmer Rooze	Administrateur-generaal van het Agentschap Wonen-Vlaanderen
De heer David Van Herreweghe	Administrateur-generaal Vlaamse Belastingdienst
Mevrouw Katrien Verhegge	Administrateur-generaal van Kind en Gezin
De heer Fons Leroy	Gedelegeerd bestuurder van de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding
De heer Jef Roos	Voorzitter Raad van Bestuur en Auditcomité van de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding
Mevrouw Ann Verhaegen	Waarnemend administrateur-generaal van het Agentschap voor Hoger Onderwijs, Volwassenenonderwijs en Studietoelagen
De heer Luc Lathouwers	Secretaris-generaal van het Departement Bestuurszaken

De bevoegde ministers van de entiteiten die gevat werden door deze thema-audit

Mevrouw Hilde Crevits	Viceminister-president van de Vlaamse Regering en Vlaams minister van Onderwijs
Mevrouw Liesbeth Homans	Viceminister-president van de Vlaamse Regering en Vlaams minister van Binnenlands Bestuur, Inburgering, Wonen, Gelijke Kansen en Armoedebestrijding
De heer Philippe Muyters	Vlaams minister van Werk, Economie, Innovatie en Sport
Mevrouw Annemie Turtelboom	Viceminister-president van de Vlaamse Regering en Vlaams minister van Begroting, Financiën en Energie
De heer Jo Vandeurzen	Vlaams minister van Welzijn, Volksgezondheid en Gezin

De minister bevoegd voor interne audit:

De heer Geert Bourgeois	Minister-president van de Vlaamse Regering en Vlaams minister van Buitenlands Beleid en Onroerend Erfgoed

De leden van het Auditcomité van de Vlaamse Administratie:

De onafhankelijke leden

De heer Luc Discry	Voorzitter van het Auditcomité en onafhankelijk deskundige
De heer Jean-Pierre Bostoen	Onafhankelijke deskundige
Mevrouw Saskia Van Uffelen	Onafhankelijke deskundige
Mevrouw Diane Breesch	Onafhankelijke deskundige

De vertegenwoordigers van de Vlaamse Regering

Mevrouw Miet Vandersteegen	Raadgever van de minister-president van de Vlaamse Regering
De heer Johan Hanssens	Adjunct-kabinetschef algemeen beleid van de viceminister-president van de Vlaamse Regering en Vlaams minister van Begroting, Financiën en Energie
De heer Martin Ruebens	Secretaris-generaal Departement DAR

De secretaris van het Auditcomité

De heer Guido Collin	Beleidsadviseur algemeen beleid

Het Rekenhof:

De heer Ignace Desomer	Voorzitter van het Rekenhof

Conclusie

De Vlaamse overheid beheert en verwerkt tal van gegevens van burgers, ondernemingen en personeelsleden en draagt bijgevolg de verantwoordelijkheid om de gepaste beveiliging van deze informatie te garanderen. Gezien de toenemende digitalisering zal de omvang en het belang van digitaal opgeslagen en uitgewisselde informatie alleen maar toenemen. De Vlaamse overheid kiest immers resoluut de weg van de digitalisering (Radicaal Digitaal) en streeft ernaar om tegen 2020 alle administratieve transacties met burgers, ondernemingen of lokale besturen te digitaliseren. Tegelijkertijd groeien de complexiteit en het aantal mogelijkheden waarop opzettelijke en onopzettelijke bedreigingen de kwetsbaarheden van informatiesystemen kunnen benutten. Een adequate beveiliging van de gegevens in beheer bij de Vlaamse overheid wordt bijgevolg steeds belangrijker.

In het kader van deze thema-audit evalueerde Audit Vlaanderen in welke mate adequate beheersmaatregelen bij de Vlaamse overheid aanwezig zijn om het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen. De conclusie van dit rapport is gebaseerd op de auditwerkzaamheden uitgevoerd bij 6 entiteiten, aangevuld met bijkomende beveiligingstesten uitgevoerd op een aantal gemeenschappelijke platformen.

Gelet op de snel evoluerende veranderingen op het vlak van informatiebeveiliging vormen de resultaten van deze auditopdracht uiteraard slechts een momentopname en zijn informatiebeveiligingsrisico's nooit volledig uit te sluiten.

***

Hoewel de Vlaamse overheid initiatieven heeft genomen voor de beveiliging van haar informatie en tot nu grotendeels gespaard is gebleven van cybercriminaliteit, blijft ze te kwetsbaar voor huidige en toekomstige bedreigingen op het vlak van informatiebeveiliging.

Tijdens de auditwerkzaamheden kon Audit Vlaanderen zich op onregelmatige wijze toegang verschaffen tot verschillende interne netwerken van de Vlaamse overheid. Vanaf deze gebruikersnetwerken of vanaf het internet konden de auditoren sommige dossiers van burgers en gegevens van personeelsleden bemachtigen. Bovendien bleken diverse beheerinterfaces (bvb. voor het beheer van firewalls of servers) en test- en ontwikkelomgevingen bereikbaar voor niet bevoegde gebruikers.
Een test met een zgn. phishing e-mail op een steekproef wijst uit dat meer dan één op drie personeelsleden een hen toegestuurde malafide link aanklikt.
De thema-audit bracht daarenboven diverse technische kwetsbaarheden aan het licht die in het bestek van deze opdracht niet verder werden uitgebuit, maar wel mogelijkheden schiepen om bvb. de inhoud van websites aan te passen, rekeningnummers te wijzigen of informatiesystemen, met al dan niet kritieke informatie, onbeschikbaar te maken.

De geïdentificeerde tekortkomingen zijn te wijten aan kwetsbaarheden zowel op niveau van de Vlaamse overheid als op entiteitsniveau en leiden afzonderlijk, maar vooral in combinatie met elkaar, tot risico's voor de integriteit, vertrouwelijkheid en beschikbaarheid van informatie over burgers, personeelsleden en ondernemingen.

De belangrijkste organisatorische kwetsbaarheden hebben betrekking op:

1. Informatiebeveiligingsbeleid en -strategie (zie aanbeveling 1):
   Een beleid voor informatiebeveiliging en een bijhorende strategie op niveau van de Vlaamse overheid ontbreken. Het generiek ICT-Veiligheidsbeleid, goedgekeurd door de Vlaamse regering in 2003, werd niet geactualiseerd en is bijgevolg sterk verouderd. Van de destijds voorziene operationele doorvertaling naar entiteitsspecifieke voorschriften, procedures en standaarden kwam weinig terecht. Bovendien blijkt het merendeel van de geauditeerde entiteiten evenmin over een eigen informatiebeveiligingsbeleid en -strategie te beschikken. Hierdoor bestaat het risico dat de implementatie van informatiebeveiliging binnen de Vlaamse overheid adequate aansturing mist.

2. Veiligheidsorganisatie (zie aanbeveling 2 en 3):
   Op niveau van de Vlaamse overheid is er momenteel geen eenduidig organisatorisch kader om de implementatie van informatiebeveiliging te initiëren, te beheersen, op te volgen en bij te sturen. De initiatieven die hiertoe in het verleden werden opgezet, zijn stilgevallen. Door de oprichting van de Vlaamse Dienstenintegrator (VDI), het bijhorende coördinatiecomité en de onderliggende stuur- en werkgroepen krijgt de veiligheidsorganisatie binnen de Vlaamse overheid mogelijks wel een nieuwe impuls.

3. Bewustzijn en kennis met betrekking tot informatiebeveiliging (zie aanbeveling 4):
   Zwakke schakels in de beveiliging van informatie zijn vaak te relateren aan de organisatiecultuur, het gedrag of de bekwaamheid van medewerkers. Verschillende auditvaststellingen wijzen op een tekort aan bewustzijn rond informatiebeveiliging.
   Door de constante evolutie in en de toenemende complexiteit van cyberbedreigingen groeit bovendien de noodzaak aan de gespecialiseerde kennis, alsook aan kennisdeling over informatiebeveiliging binnen en tussen de entiteiten van de Vlaamse overheid.

Naast de organisatorische kwetsbaarheden werden tal van technische gebreken of zwakke plekken vastgesteld, die betrekking hebben op verschillende facetten zoals bvb. zwak wachtwoordbeheer, onvoldoende aandacht voor informatiebeveiliging bij de ontwikkeling of wijziging van informatiesystemen, ontbrekende of verouderde encryptie, onveilige configuratie van informatiesystemen.

Aan sommige technische kwetsbaarheden is eenvoudig te remediëren, andere zijn complexer en vergen specifieke investeringen. Op korte termijn voorziet het Facilitair Bedrijf een verbetering van de beveiligingsmaatregelen van het bekabelde, interne netwerk van de Vlaamse overheid en ontwikkelt de gemeenschappelijke ICT-dienstverlener een actieplan voor het verhelpen van de structurele tekortkomingen.

Vanaf 1 februari 2015 trad een nieuw raamcontract voor exploitatie-gebonden ICT-diensten in voege. Het is momenteel nog onvoldoende duidelijk hoe informatiebeveiliging onder dit nieuwe raamcontract concreet zal worden ingevuld.

***

Karel Bruneel,
Senior auditor

Patricia Van de Capelle,
Senior auditor

Jo Fransen,
Manager-auditor

Eddy Guilliams,
Administrateur-generaal

Aanbevelingen

Aanbeveling 1 – Informatiebeveiligingsbeleid- en strategie op niveau van de Vlaamse overheid

De Vlaamse overheid beheert en verwerkt tal van gevoelige gegevens van burgers, ondernemingen en **p**ersoneelsleden. Om het gewenste niveau van integriteit, beschikbaarheid en vertrouwelijkheid van deze gegevens te garanderen, is het aangewezen dat de Vlaamse overheid, rekening houdend met de autonomie van de entiteiten, haar beleid inzake informatiebeveiliging bepaalt en de strategie vastlegt, communiceert aan de belanghebbenden en met geplande tussenpozen beoordeelt of dit informatiebeveiligingsbeleid nog passend en doeltreffend is.

Toelichting:
Het vastleggen van een gemeenschappelijk referentiekader, zoals bvb. de ISO 27002[1], kan een eerste stap zijn in de richting van het uitwerken van een overkoepelend beleid. Dit referentiekader kan, ongeacht het al dan niet dwingende karakter ervan, dienen als uitgangspunt voor de beleids- en richtlijnen inzake informatiebeveiliging van de verschillende entiteiten van de Vlaamse overheid, in functie van hun specifieke risico's, strategieën en doelstellingen.

Aanbeveling 2 – Structuur voor security governance

Met het oog op de implementatie van een overkoepelend informatiebeveiligingsbeleid op het niveau van de Vlaamse overheid wordt een beheerskader voor informatiebeveiliging opgezet dat de processen[2] bepaalt en de rollen en verantwoordelijkheden duidelijk definieert en toewijst.

Toelichting:
Een security governance-structuur of beheerskader kan worden uitgerold door gebruik te maken van een combinatie van verscheidene structuren en processen waarbij de rollen en daarbij horende verantwoordelijkheden eenduidig worden toegewezen aan het aangewezen niveau.
Voor de hand liggende partijen die bij het uitvoeren van specifieke informatiebeveiligingsprocessen binnen de Vlaamse overheid worden betrokken, zijn:
- *het coördinatiecomité van de Vlaamse Dienstenintegrator (VDI) en de onderliggende werkgroepen;*
- *de informatie-eigenaars;*
- *de information security officers, veiligheidsconsulenten of data protection officers;*
- *het Facilitair Bedrijf (en de cel Netwerken en beveiliging);*
- *het agentschap Informatie Vlaanderen;*
- *de externe ICT-dienstverleners.*

Aanbeveling 3 – Opvolging en bijsturing van informatiebeveiliging

Om zich ervan te verzekeren dat informatiebeveiliging binnen de Vlaamse overheid wordt geïmplementeerd in overeenstemming met het desbetreffende beleid en de bijhorende strategie, behoort de aanpak van de verschillende entiteiten ten aanzien van het beheer van informatiebeveiliging te worden opgevolgd, beoordeeld en zo nodig bijgestuurd.

Toelichting:
Voor een doeltreffende regelmatige beoordeling valt te overwegen om een specifiek meet- en rapportage-instrument te ontwikkelen. Deze aangelegenheid kan bvb. opgenomen worden door het coördinatiecomité van de Vlaamse Dienstenintegrator (VDI) en de bijhorende werkgroepen.

[1] ISO/IEC 27002:2013 Informatietechnologie/Beveiligingstechnieken/Code voor informatiebeveiliging
[2] Strategische besluitvorming, kennisdeling, contacten met relevante overheidsinstanties en speciale belangengroepen, afstemming, ondersteuning, samenwerking, vorming,…

Aanbeveling 4 – Bewustzijns-, opleidings- en trainingsprogramma m.b.t. informatiebeveiliging

Faciliteer sensibiliserende en vormende initiatieven om ervoor te zorgen dat alle medewerkers zich bewust zijn van het belang van informatiebeveiliging en beschikken over de nodige kennis om zich van hun verantwoordelijkheden op het vlak van informatiebeveiliging te kwijten.

Toelichting:
Bij de opzet van bewustzijns-, opleidings- en trainingsprogramma's m.b.t. informatiebeveiliging voor het management, de medewerkers en externe dienstenleveranciers behoort rekening te worden gehouden met relevantie voor hun functie en waarbij aandacht uitgaat naar zowel digitale informatie als papieren documenten. Het management dient gesensibiliseerd te worden en heeft vervolgens de taak om ook anderen bewust te maken omtrent het belang van informatiebeveiliging.
Deze activiteiten worden bij voorkeur periodiek herhaald en geactualiseerd, zodat deze in overeenstemming blijven met het beleid en beheerskader voor informatiebeveiliging en voortbouwen op de lessen die zijn geleerd uit informatiebeveiligingsincidenten.

Beschrijving van de opdracht

1 Situering

1.1 Het belang van informatiebeveiliging

De Vlaamse overheid beheert en verwerkt tal van gevoelige gegevens van burgers, ondernemingen en personeelsleden en draagt bijgevolg de verantwoordelijkheid om het gewenste niveau van integriteit, vertrouwelijkheid en beschikbaarheid voor deze informatie te garanderen. Deze hoeveelheid aan gevoelige informatie zal nog toenemen ten gevolge van de zesde staatshervorming en de overdracht van bevoegdheden van het federale naar het Vlaamse bestuursniveau.

Ook het aantal personeelsleden met toegang tot gevoelige informatie stijgt en, door het toenemend aantal koppelingen tussen informatiesystemen en de groei in het gebruik van digitale informatie, groeit ook het risico op ongeautoriseerde toegang tot, wijziging of verspreiding van informatie.

Tegelijkertijd neemt de complexiteit en het aantal mogelijkheden toe waarop opzettelijke en onopzettelijke bedreigingen de kwetsbaarheden van informatiesystemen kunnen benutten.

Informatiebeveiliging is dan ook hoe langer, hoe meer een belangrijk aandachtspunt voor de Vlaamse overheid. Datalekken of andere inbreuken op de beveiliging van gegevens kunnen immers leiden tot imagoschade en hebben mogelijke financiële gevolgen.

1.2 Situering van de thema-audit

Een thema-audit licht een horizontale of transversale materie door binnen de volledige Vlaamse administratie, dit in tegenstelling tot andere soorten auditopdrachten die zich voornamelijk richten tot één bepaalde entiteit of proces.

Door Audit Vlaanderen werden achtereenvolgens de volgende thema-audits uitgevoerd:
- Thema-audit bedrijfscontinuïteitsmanagement (2007-2008);
- Thema-audit managementondersteunende dienstverlening (2008-2009);
- Thema-audit ICT-netwerken (2009-2010);
- Thema-audit debiteurenbeheer (2011);
- Thema-audit inspectie/handhaving (2013);
- Thema-audit ICT-contractbewaking (2013).

2 Auditdoelstellingen en relatie met doelstellingen interne controle

Deze thema-audit focust op de problematiek van de bescherming van kritieke en vertrouwelijke informatie. Concreet wordt geëvalueerd in welke mate de Vlaamse overheid over beheersmaatregelen beschikt om het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.

Artikel 33 van het kaderdecreet Bestuurlijk Beleid van 18 juli 2003 omvat het volgende:
"*De departementen, de intern verzelfstandigde agentschappen en de extern verzelfstandigde agentschappen staan in voor de interne controle van hun bedrijfsprocessen en activiteiten. De interne controle is in het bijzonder gericht op :*
1° het bereiken van de opgelegde doelstellingen en het effectief en efficiënt beheer van risico's;
2° de naleving van regelgeving en de procedures;
3° de betrouwbaarheid van de financiële en beheersrapportering;
4° de effectieve en efficiënte werking van de diensten en het efficiënt inzetten van de middelen;
5° de bescherming van haar activa en de voorkoming van fraude."

In de ondersteuning van het management draagt deze thema-audit, voor de vermelde reikwijdte, voornamelijk bij tot het realiseren van de volgende doelstellingen:
1° het bereiken van de opgelegde doelstellingen en het effectief en efficiënt beheer van risico's;
2° de naleving van regelgeving en de procedures;
5° de bescherming van haar activa en de voorkoming van fraude.

3 Auditaanpak en -reikwijdte

Op 18 juni 2013 keurde het Auditcomité van de Vlaamse administratie de uitvoering van de thema-audit m.b.t. informatiebeveiliging goed.

Audit Vlaanderen liet zich tijdens deze thema-audit, en meer specifiek voor de uitvoering van de technische veiligheidstesten, bijstaan door externen met de nodige gespecialiseerde kennis.

Eerste fase van de thema-audit informatiebeveiliging (periode augustus 2013 – januari 2014)

Tijdens de eerste fase werkte Audit Vlaanderen een auditprogramma uit dat gehanteerd werd als kader doorheen deze thema-audit. Dit auditprogramma is gebaseerd op het generiek ICT-Veiligheidsbeleid van de Vlaamse overheid, goedgekeurd door de Vlaamse Regering op 25 april 2003, en op de ISO/IEC 27002:2005 Informatietechnologie/Beveiligingstechnieken/Code voor informatiebeveiliging[3].

Dit auditprogramma werd toegepast tijdens twee pilootauditopdrachten, m.n.:
1. Agentschap Kind & Gezin (1301 010)
2. Agentschap Wonen-Vlaanderen (1301 011)

Op basis van deze auditopdrachten werd het controleprogramma geëvalueerd en bijgestuurd. Het definitieve auditprogramma is opgebouwd volgens de onderstaande thema's:
1. Informatiebeveiligingsbeleid en -organisatie
2. Architectuur
3. Informatieclassificatie
4. Outsourcing
5. Audit en logging
6. Bewustzijn *(awareness)*
7. Fysieke toegangsbeveiliging
8. Netwerkbeveiliging
9. Systeembeveiliging
10. Authenticatie en logische toegangsbeveiliging *(identity and access management)*
11. Incidentenbeheer
12. Wijzigingsbeheer
13. Back-up beheer
14. Configuratie- en operationeel beheer
15. Gebruik van mobiele informatiedragers

[3] Deze audit focust op de beveiliging van elektronische informatie. De problematiek van bedrijfscontinuïteitsbeheer en van naleving is buiten beschouwing gelaten.

Tweede fase van de thema-audit informatiebeveiliging (periode februari 2014 – oktober 2014)

In de tweede fase volgde de uitrol van de thema-audit naar 4 andere entiteiten:
1. Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (1401 003)
2. Agentschap voor Overheidspersoneel (1401 007)
3. Vlaamse Belastingdienst (1401 008)
4. Agentschap voor Hoger Onderwijs, Volwassenenonderwijs en Studietoelagen (1401 009)

Voor de selectie van de entiteiten die gevat werden door deze thema-audit, werden de volgende criteria gehanteerd:
- Risicofactoren:
  - Aanwezigheid van gevoelige/vertrouwelijke informatie;
  - Mogelijke imagoschade in het geval van een datalek;
- Spreiding over de verschillende beleidsdomeinen;
- Spreiding over types van entiteiten;
- Variatie in afname van de Gemeenschappelijke ICT-Dienstverlener;
- De planning van Audit Vlaanderen en van het Rekenhof.

Bij elke entiteit werden de volgende werkzaamheden uitgevoerd:
- Inzicht krijgen in het opzet van beheersmaatregelen via documentstudie en interviews;
- Het opstellen van het gedetailleerd kader voor de uitvoering van de veiligheidstesten;
- Het in de praktijk nagaan van de toepassing van de beheersmaatregelen via:
  - Veiligheidstesten (o.a. interne, externe en draadloze intrusietesten, systeemanalyses, webapplicatietesten);
  - Observaties;
  - Walkthroughs;
- Beoordelen van de risicoafdekking en formuleren van aanbevelingen.

De bevindingen van het onderzoek van de 6 voornoemde entiteiten kregen hun neerslag in 6 individuele rapporten die overgemaakt werden aan de betrokken bestemmelingen.

Derde fase van de thema-audit informatiebeveiliging (periode oktober 2014 – januari 2015)

De derde fase omvatte de opmaak van het voorliggend rapport betreffende de thema-audit informatiebeveiliging. Veiligheidstesten op een aantal gemeenschappelijke platformen werden uitgevoerd (zoals bvb. het platform voor toegangs- en gebruikersbeheer - ACM/IDM, het Vlaamse overheid Bedrijfsinformatieplatform - VOBIP en de datawarehouse van het departement Bestuurszaken – BDPIB) en kwetsbaarheidsanalyses op het interne netwerk van de Vlaamse overheid (ook het GID buroticanetwerk genoemd).

Dit globaal rapport is opgemaakt op basis van de bevindingen uit de individuele auditopdrachten, alsook vaststellingen op niveau van de Vlaamse overheid.

Vaststellingen

1 Inleiding

In het kader van deze thema-audit wordt onderzocht of gevoelige informatie in beheer bij de Vlaamse overheid op een afdoende wijze beschermd wordt.

Uit de resultaten van deze thema-audit blijkt dat er binnen de Vlaamse overheid momenteel verschillende kwetsbaarheden zijn op het vlak van informatiebeveiliging. Deze kwetsbaarheden leiden afzonderlijk, maar vooral in samenhang met elkaar tot risico's inzake misbruik en oneigenlijk gebruik van informatie over burgers en ondernemingen.

Het eerste deel van het syntheserapport bevat de *belangrijkste organisatorische en technische kwetsbaarheden* vastgesteld tijdens de uitvoering van deze thema-audit *(cfr. 2.1. & 2.2.)*. Het tweede deel gaat in op de *toekomstige uitdagingen* op het vlak van informatiebeveiliging en geeft weer of de Vlaamse overheid hierop voldoende voorbereid is.

2 Informatiebeveiliging binnen de Vlaamse overheid

2.1 Organisatorische opzet van informatiebeveiliging

2.1.1 Informatiebeveiligingsbeleid en –organisatie

Informatiebeveiligingsbeleid- en organisatie op niveau van de Vlaamse overheid
Binnen de Vlaamse overheid werd ruim 10 jaar geleden het generiek ICT-veiligheidsbeleid, gebaseerd op de ISO 17799:2000 standaard, als raamwerk op het vlak van informatiebeveiliging goedgekeurd[4]. De ISO-norm werd verschillende keren geactualiseerd, maar het generiek ICT-veiligheidsbeleid bleef ongewijzigd en is ondertussen sterk verouderd.
Ook het toepassingsgebied van het generiek ICT-veiligheidsbeleid is een knelpunt. Het beleid is immers niet van toepassing op de volledige Vlaamse overheid, maar geldt enkel voor de entiteiten zonder rechtspersoonlijkheid.

Er is momenteel dan ook geen overkoepelende strategie die de krijtlijnen uitzet op het vlak van informatiebeveiliging en waarin een gemeenschappelijk en actueel referentiekader, zoals bvb. de ISO 27002, bepaald wordt voor alle entiteiten van de Vlaamse overheid *(aanbeveling A1)*. Hierdoor bestaat het risico dat elke entiteit naar eigen goeddunken invulling geeft aan informatiebeveiliging.

Samen met het generiek ICT-veiligheidsbeleid werd destijds een organisatiemodel opgezet dat garant diende te staan voor de verdere implementatie en uitwerking ervan.
De stuurgroep Strategische ICT-Veiligheid stond hierin centraal en droeg tal van verantwoordelijkheden, gericht op het verder uitdragen en verduidelijken van het ICT-veiligheidsbeleid. De stuurgroep werd in 2007 als permanente werkgroep ondergebracht binnen het Strategische ICT-Overlegforum voor de Vlaamse overheid (SIOF)[5], dat in 2009[6] opgeheven werd, en werd vervolgens gepositioneerd als permanente architecturale werkgroep inzake ICT-Veiligheid onder de werkgroep Business-ICT-Alignment (BIA). De werking hiervan is ondertussen eveneens volledig stilgevallen.

[4] Nota aan de Vlaamse Regering op datum van 25/04/2003 betreffende het toekomstig ICT-Veiligheidsbeleid voor de beleidsdomeinen van de Vlaamse overheid.
[5] Het SIOF ressorteerde onder en formuleerde adviezen aan het vroegere Collega van ambtenaren-generaal (CAG).
[6] Beslissing van de Vlaamse Regering van 6 mei 2009 betreffende een gedragen globaal ICT-beleid voor de Vlaamse overheid: Samenwerking- en beslissingsstructuur voor garantie tot efficiënt en effectief business ICT-alignement onderbouwd door een geïntegreerde architectuur.

In 2008 werd de ambtelijke werkgroep Beveiliging/BCM opgericht, onder het voorzitterschap van het departement Bestuurszaken (dBZ) en bestaande uit vertegenwoordigers van de verschillende beleidsdomeinen en van de horizontale dienstverleners. Hoewel deze werkgroep in de benaming 'Beveiliging' draagt, ligt de focus hiervan voornamelijk op bedrijfscontinuïteitsmanagement.

Binnen het oorspronkelijk opgezette organisatiemodel werd eveneens de rol van ICT security officer voor de Vlaamse Overheid opgenomen. Deze werd initieel toegewezen aan het celhoofd Netwerken en Beveiliging van het vroegere e-IB en is, gegeven de fusie met het Agentschap voor Facilitair Management, mee verschoven naar de stafdienst van het Facilitair Bedrijf.
In het kader van de veiligheidsorganisatie, opgezet in het generiek ICT-Veiligheidsbeleid, werden aan de ICT security officer verschillende taken toegewezen op zowel strategisch als operationeel niveau. Door het wegvallen van de stuurgroep Strategische ICT-Veiligheid, verdween het overlegorgaan via dewelke de ICT security officer een draagvlak m.b.t. informatiebeveiliging kon genereren.

In 2012 werd de Vlaamse Dienstenintegrator (VDI)[7] opgericht. De VDI heeft als decretale taak om de elektronische dienstverlening en gegevensuitwisseling te organiseren met waarborgen op het vlak van informatiebeveiliging en de bescherming van de persoonlijke levenssfeer. De VDI zorgt bovendien voor de ontsluiting van authentieke gegevensbronnen, zoals bvb. het Rijksregister, naar de Vlaamse overheid en naar lokale overheden.
Het bijhorende coördinatiecomité dat de VDI ondersteunt bij de uitvoering van haar taken werd in 2013 opgericht. Onder het coördinatiecomité worden een aantal stuur- en werkgroepen opgestart waaronder de 'Informatieveiligheidsbeleid VDI' en 'Informatieveiligheidsbeleid Vlaamse overheid'. Deze laatste werkgroep initieerde eind 2014 een aantal initiatieven om informatiebeveiliging in de Vlaamse overheid terug op de agenda te zetten en werkt hiertoe een aantal voorstellen uit die ter goedkeuring voorgelegd zullen worden aan het coördinatiecomité. De oprichting van de Vlaamse Dienstenintegrator en de daarbij horende organen kunnen een structuur vormen die ten volle benut kan worden om invulling te geven aan een beleid en strategie inzake informatiebeveiliging *(aanbeveling A2*).

Informatiebeveiligingsbeleid- en organisatie op het niveau van de entiteiten
Met de goedkeuring van het generiek ICT-Veiligheidsbeleid werd aan de leidend ambtenaren de verantwoordelijkheid toegewezen zowel voor de toepassing, de opvolging en communicatie van het beveiligingsbeleid en de bijhorende voorschriften als voor het vastleggen van de kritieke beveiligingsvereisten en –maatregelen voor de eigen applicaties.

De resultaten van de thema-audit tonen evenwel aan dat er slechts een gebrekkige doorvertaling gebeurde vanuit het generiek ICT-Veiligheidsbeleid naar een entiteitsspecifiek informatiebeveiligingsbeleid. Het merendeel van de onderzochte entiteiten beschikt immers niet over een uitgewerkt beleid, waarin de beleidslijnen en principes op het vlak van informatiebeveiliging zijn opgenomen en afgestemd op risico's van de entiteit. Slechts 2 van de geauditeerde entiteiten werkten een informatiebeveiligingsbeleid uit of leveren inspanningen om te komen tot een beleid op zowel strategisch, tactisch en operationeel niveau. Bovendien blijkt dat de entiteiten vaak onvoldoende vertrouwd zijn met de principes van classificatie van informatie. Slechts een aantal entiteiten maken bewust een onderscheid tussen applicaties met persoonsgegevens enerzijds of niet-persoonsgevoelige data anderzijds en stemmen hun beveiligingsniveau hierop af (*zie verder 2.2. Technische kwetsbaarheden inzake informatiebeveiliging).*

Het ontbreken van een informatiebeveiligingsbeleid binnen de geauditeerde entiteiten gaat veelal samen met onduidelijke rollen en verantwoordelijkheden op het vlak van beveiliging. Zo blijkt dat:
- De bevoegdheden en de taken op het vlak van informatiebeveiliging binnen een organisatie vaak niet duidelijk afgebakend en toegewezen zijn;
- Er onvoldoende interne kennis en competenties zijn inzake informatiebeveiliging *(zie verder)*;
- Er veelal een beroep gedaan wordt op externe veiligheidsconsulenten zonder de nodige interne aansturing en opvolging;

[7] Decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator en besluit van de Vlaamse Regering van 29 november 2013 tot uitvoering van het decreet van 13 juli 2012 houdende de oprichting en organisatie van een Vlaamse dienstenintegrator

- Verschillende entiteiten inzake ICT en informatiebeveiliging beroep doen op externe dienstverleners. Door het gebrek aan interne kennis en competenties op het vlak van informatiebeveiliging is voor deze entiteiten moeilijk om een degelijke analyse en evaluatie te maken van de voorstellen van deze dienstverleners in functie van de risico's op het vlak van informatiebeveiliging.

2.1.2 Informatiebeveiliging en outsourcing

Het gemeenschappelijk ICT-raamcontract
Op 8 januari 2008 sloot de Vlaamse overheid een gemeenschappelijk ICT-contract voor een periode van 7 jaar met de tijdelijke handelsvennootschap EDS-Telindus (later HP-Belgacom). Dit gemeenschappelijk ICT-contract liep af op 1 februari 2015 en werd in de loop van 2014 gefaseerd vervangen door 4 ICT-raamcontracten voor respectievelijk: (1) *exploitatie-gebonden ICT-diensten*, (2) *ontwikkelingsprojecten*, (3) *technische ondersteuning door ICT-profielen* en (4) *aankoop van diverse ICT-producten*.

Elk raamcontract omvat minimaal een basiscontract met de algemene bepalingen, een glossarium en een Service Portfolio met een omschrijving van de concrete dienstverlening. In elk basiscontract zijn voor de ICT-dienstverlener en diens onderaannemers richtlijnen opgenomen over de omgang met persoonsgegevens, gegevens uit authentieke bronnen en andere vertrouwelijke informatie.

Het beveiligingsbeheer van het gemeenschappelijk ICT-contract 2008-2015 was gebaseerd op standaarden voor goede praktijken, aangevuld met de specifieke vereisten uit de Vlaamse Overheid Processen (VOPS) en het ICT-veiligheidsbeleid van de Vlaamse overheid. De concrete activiteiten werden vastgelegd in het basiscontract. In het kader van de ondersteuning, evaluatie en bijsturing van het beveiligingsbeheer vond er op een structurele basis afstemming plaats tussen HP-Belgacom en het vroegere e-IB:
- Wekelijks Security Debriefing;
- Wekelijks Overleg ICT-Architectuur en ICT-Veiligheid (OAV);
- Maandelijks Operationeel Security Overleg.

Bij het nieuwe ICT-raamcontract 2015 voor *exploitatie-gebonden ICT-diensten* is de aanpak van beveiligingsbeheer vermeld in een bijlage bij het basiscontract en dienen de specifieke beveiligingsaspecten te worden beschreven in de Service Portfolio. De VOPS-processen vervallen en er komt een nieuwe set beveiligingsprocessen. De ICT-dienstverlener zal het beveiligingsbeheer overkoepelend aanpakken op basis van een Security Information en Event Management benadering. Hoe dit concreet zal worden ingevuld en afgestemd met de afnemers, is momenteel nog onduidelijk.

Het raamcontract voor *exploitatie-gebonden ICT-diensten* biedt netwerk-, werkplek- en datacenterdiensten en bijbehorende projecten aan in een 'as a service'-businessmodel. Deze end-to-end aanpak beoogt meer flexibiliteit en gebruiksgemak te bieden voor de afnemers.

Afhankelijk van de reikwijdte gaat 'as a service'-dienstverlening gepaard met geleidelijk toenemende overdracht van de verantwoordelijkheid inzake informatiebeveiliging van de klant naar de ICT-dienstverlener. Om de vooropgestelde vereisten op het vlak van beschikbaarheid, integriteit en confidentialiteit te garanderen, zal de afnemer van het nieuwe ICT-raamcontract bijgevolg nog meer dan voorheen zijn aangewezen op weloverwogen en afdwingbare afspraken over rollen en verantwoordelijkheden met de outsourcer (*aanbeveling A2*).

Het nieuwe ICT-raamcontract 2015 voor *ontwikkelingsprojecten* stipuleert uitdrukkelijk dat de minimumvereisten inzake beveiliging dienen te worden vastgelegd in de exploitatie-, ontwikkel- en testdossiers. Er is nog niet bepaald op welke wijze dit in de praktijk verankerd gaat worden.

Informatiebeveiliging en outsourcing op het niveau van de entiteiten

Eind 2013 stelde Audit Vlaanderen n.a.v. de thema-audit van de bewaking van het gemeenschappelijk ICT-contract (auditopdracht 1201 004) vast dat de risico's voor de contractbewaking dikwijls te relateren zijn aan het niveau van ICT-expertise waarover de geauditeerde entiteiten beschikken voor de aansturing en opvolging van de ICT-dienstverlener.

Ook in het kader van de onderhavige thema-audit informatiebeveiliging vormt een beperkte ICT-expertise een belangrijk risico. Om weloverwogen en risico gebaseerde beslissingen inzake informatiebeveiliging te nemen, is naast een algemene ICT-kennis immers ook een actuele kennis van informatiebeveiliging vereist.

Tijdens de auditwerkzaamheden uitte deze problematiek zich bij de geauditeerde entiteiten in verschillende knelpunten:

- Bij de ontwikkeling van toepassingen gebeurt de evaluatie van de beveiligingsvereisten en -risico's veelal op ad hoc basis en niet volgens een vaste methodologie (bvb. OWASP top 10[8]);
- De risico-evaluatie en motivatie die ten grondslag liggen aan bepaalde beslissingen inzake informatiebeveiliging worden maar beperkt gedocumenteerd;
- Bij wijzigingen aan bestaande software of systemen wordt de inschatting van de beveiligingsrisico's vaak niet geactualiseerd;
- Er is geen of onvoldoende adequaat toezicht op geleverde dienstverlening inzake informatiebeveiliging;
- Onvoldoende vertrouwdheid met de bepalingen rond informatiebeveiliging in het gemeenschappelijk ICT-contract en de specifieke rollen en verantwoordelijkheden van de klant, de gemeenschappelijke ICT-dienstverlener (Security manager) en Het Facilitair Bedrijf (Information Security Officer) kon worden vastgesteld.

Gezien de constante evolutie en de toenemende complexiteit van de bedreigingen voor informatiebeveiliging geldt dat specifieke ICT-expertise hieromtrent, meer nog dan de meer algemene ICT-kennis, best wordt uitgebouwd op het niveau waar ze het meeste meerwaarde kan betekenen voor de Vlaamse overheid. De initiatieven die onder de koepel van het coördinatiecomité van de Vlaamse Dienstenintegrator werden en zullen worden genomen, kunnen in dat verband voor de individuele entiteiten een opportuniteit zijn om specifieke expertise te verwerven en ervaringen rond informatiebeveiliging te delen (*aanbeveling A4*).

2.1.3 Bewustzijn op het vlak van informatiebeveiliging

Bewustzijn inzake informatiebeveiliging op niveau van de Vlaamse overheid
Zwakke schakels in de beveiliging van vertrouwelijke informatie zitten vaak vervat in aspecten zoals de werkomgeving, het gedrag en de bekwaamheid van medewerkers. De resultaten van deze thema-audit tonen aan dat er binnen de Vlaamse overheid onvoldoende bewustzijn is omtrent het belang van beveiliging van gevoelige informatie. Een overkoepelend bewustzijnsprogramma ontbreekt dan ook. Specifieke initiatieven worden evenwel ondernomen, zoals bvb. de actualisatie van de ICT-gedragscode[9] betreffende het integer omgaan met ICT-middelen en de verspreiding van de ICT-nieuwsbrief waarin regelmatig veiligheidsproblemen aan bod komen. Deze gedragscode bevat een algemeen kader met waarden en principes die de personeelsleden van de Vlaamse overheid moeten respecteren bij het dagelijks gebruik van ICT.

Bewustzijn inzake informatiebeveiliging op entiteitsniveau
Het gebrek aan bewustzijn inzake informatiebeveiliging wordt eveneens bevestigd in de resultaten van de thema-audit. Hoewel een aantal entiteiten maatregelen (bvb. presentaties bij het directiecomité, een charter voor externen, een deontologische code voor gebruikers, een vertrouwelijkheidsclausule voor gebruikers van specifieke toepassingen of opleidingen rond privacy) nemen om de medewerkers bewust te maken omtrent het omgaan met gevoelige informatie, blijkt dat doordachte bewustzijnstrainingen, afgestemd op de risico's binnen de entiteit, veelal ontbreken.

[8] OWASP of Open Web Application Security Project. De OWASP top 10 bevat een overzicht van 10 van de meest voorkomende en serieuze kwetsbaarheden die zich voordoen in webapplicaties.
[9] Omzendbrief BZ 2014/2 ICT-code betreffende het integer omgaan met ICT-middelen op datum van 31 maart 2014 ter vervanging van de omzendbrief ICT/2004/02.

Dit gebrek aan bewustzijn blijkt uit o.a.:

- Het gebruik van zwakke wachtwoorden, alsook gebruikerswachtwoorden die weinig frequent gewijzigd worden;
- De aanwezigheid van gebruikersaccounts van personeelsleden die reeds uit dienst zijn;
- Een beperkte bekendheid met de meld- en contactpunten voor beveiligingsincidenten (bvb. servicedesk@vlaanderen.be , antispam@vlaanderen.be);
- Het relatief hoog aantal medewerkers dat ingaat op zgn. phishing-mail.
  Bij 5 van de 6 entiteiten werd, i.h.k.v. de uitvoering van de veiligheidstesten, een dergelijke e-mail met een malafide hyperlink uitgestuurd.
  Het aantal geadresseerden dat doorklikt op de meegestuurde link varieert sterk: bij één entiteit klikte slechts 10% de malafide hyperlink aan, terwijl bij een andere entiteit in totaal 63% van de bestemmelingen hierop ingingen.

Entiteit	Aantal bestemmelingen	Aantal hits	%
Entiteit 2	65	33	51%
Entiteit 3	51	32	63%
Entiteit 4	112	29	26%
Entiteit 5	58	6	10%
Entiteit 6	50	23	46%
	336	123	**37%**

  Eén reactie in een reële situatie is echter voldoende om een aanvaller de mogelijkheid te geven kwaadaardige software te installeren of zich toegang te verschaffen tot gevoelige informatie.
- Verbeteringsmogelijkheden op het vlak van de toepassing van een clear-screen beleid. De gebruikerssystemen worden soms onbeheerd achtergelaten waardoor een kwaadwillende persoon zich via dat systeem toegang kan verschaffen tot de applicaties en de informatie. In druk bezette kantoren kan de sociale controle enig misbruik voorkomen, in andere kantoren geldt deze regel niet.

Zwakke schakels in de beveiliging van informatie zitten niet alleen vervat in ICT-technische beheersmaatregelen, maar ook in het gedrag en de kennis van medewerkers inzake beveiliging van informatie. Bijgevolg is het aangewezen om via actieve sensibilisering bij te dragen tot het creëren van een werkomgeving waarin aandacht besteed wordt aan veilig gedrag van het personeel *(aanbeveling A4)*.

2.1.4 Opvolging en bijsturing inzake informatiebeveiliging

Opvolging en bijsturing inzake informatiebeveiliging op niveau van de Vlaamse overheid
Vanuit het vroegere e-IB werden, in samenwerking met de gemeenschappelijke ICT-dienstverlener, initiatieven ondernomen en overlegstructuren opgezet voor de opvolging van het beveiligingsmanagement in het kader van het overkoepelende outsourcingscontract (zie 2.1.2).

Het generiek ICT-veiligheidsbeleid, en meer specifiek de beleidslijn 'Naleving en controle' uit 2005, stelt dat de conformiteitsbewaking en de evaluatie van het veiligheidsniveau dient te worden uitgevoerd via conformiteitsrevisies, ICT-risicoanalyses (op niveau Vlaamse overheid en entiteit) en onafhankelijke audits. In de praktijk gebeurde de opvolging, tussen 2005 en 2008, voornamelijk via de jaarlijkse ICT-risicoanalyse die georganiseerd werd door de toenmalige Stuurgroep Strategische ICT-Veiligheid. Deze oefening werd, o.a. omwille van de te beperkte deelname van de entiteiten en het vertrek van de toenmalige ICT security officer, stopgezet. In 2008 stelde de stuurgroep Strategische ICT-Veiligheid ook een ontwerp voor een maturiteitsmodel op, maar dit voorstel werd nooit formeel goedgekeurd.

De werkgroep 'Informatieveiligheidsbeleid Vlaamse overheid' overweegt de ontwikkeling van een nieuw instrument om de informatiebeveiliging binnen de Vlaamse overheid in kaart te brengen (incl. rapporteringen over veiligheidsincidenten) en op te volgen (via bvb. maturiteit/benchmarking) (*zie aanbeveling 3*).

Opvolging en bijsturing inzake informatiebeveiliging op entiteitsniveau
Uit de individuele auditopdrachten blijkt bij verschillende entiteiten dat er geen duidelijk proces is voor de opvolging van veiligheidsincidenten. In sommige gevallen ontbreekt zelfs een contactpunt of escalatieprocedure. De service level agreements of SLA's met externe dienstverleners concentreren zich voornamelijk op het aspect "beschikbaarheid" maar besteden vaak nog onvoldoende aandacht aan afdwingbare afspraken op het vlak van integriteit en confidentialiteit.

2.2 Technische kwetsbaarheden inzake informatiebeveiliging

De resultaten van de thema-audit tonen aan dat er, naast de vastgestelde organisatorische kwetsbaarheden, eveneens tal van technische kwetsbaarheden zijn die ervoor zorgen dat de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens in beheer bij de Vlaamse overheid onvoldoende gewaarborgd worden.

De belangrijkste technische kwetsbaarheden zijn terug te brengen tot volgende categorieën:
- Wijzigingsbeheer
- Netwerkbeveiliging
- Versleuteling van informatie
- Systeembeveiliging
- Toegangs- en gebruikersbeheer
- Fysieke toegangsbeveiliging

2.2.1 Wijzigingsbeheer

In het kader van deze audit bleken belangrijke kwetsbaarheden vaak te wijten aan een onvoldoende richtlijnen rond het veilig ontwikkelen van informatiesystemen of aan de gebrekkige toepassing van dergelijke richtlijnen.

Bij het ontwikkelen van nieuwe informatiesystemen of het wijzigen van bestaande systemen gaat soms te weinig aandacht naar de analyse en specificatie van informatiebeveiligingseisen, wordt het beveiligingsaspect niet altijd meegenomen bij het testen van de applicaties en wordt de documentatie van de toepassingen (bvb. exploitatiedossiers, netwerk- en logische schema's) veelal niet up-to-date gehouden en bewaakt.

Dit uit zich o.a. in een gebrek aan controles op de ingevoerde gegevens (inputvalidatie) die door een toepassing worden verwerkt. Het verwerken van ongeldige en/of gemanipuleerde data kan een impact hebben op de integriteit, de beschikbaarheid en de confidentialiteit van de toepassing en de daarin opgenomen gegevens.
Zo kon tijdens de uitvoering van de veiligheidstesten via het internet op een ongeautoriseerde wijze toegang verkregen worden tot dossiers van burgers. Rekeningnummers konden gewijzigd worden en volmachten konden goedgekeurd worden in naam van andere personen. Een gebrek aan inputvalidatie kan er eveneens toe leiden dat samen met de ingevoerde data kwaadaardige software meegegeven wordt.

2.2.2 Netwerkbeveiliging

Ook op het vlak van netwerkbeveiliging konden verschillende kwetsbaarheden worden vastgesteld, m.n.:

1) *Het interne netwerk van de Vlaamse overheid is momenteel onvoldoende beveiligd.*
   De gemeenschappelijke ICT-dienstverlener biedt via het buroticanetwerk[10] zowel een interne bekabelde als draadloze netwerkinfrastructuur aan in de gebouwen van de Vlaamse overheid. Hierop worden mechanismen voorzien om te voorkomen dat niet-geautoriseerde systemen zich toegang kunnen verlenen tot het interne netwerk.
   Uit de veiligheidstesten, uitgevoerd in het Boudewijn-, Phoenix- en Ferrarisgebouw, blijkt evenwel dat de maatregelen voorzien op het bekabelde netwerk eenvoudig omzeild kunnen worden, waardoor een persoon met basiskennis van computernetwerken zich zonder veel moeite toegang kan verschaffen tot de interne netwerkomgeving. Om hier een antwoord op te bieden voorziet de gemeenschappelijke ICT-dienstverlener op termijn een verbetering van de beschermingsmaatregelen middels de toepassing van netwerkbeveiliging via Netwerk Acces Control (NAC), m.n. de implementatie van de 802.1x - standaard[11].

[10] Het GID-buroticanetwerk is een intern computernetwerk dat onder de gemeenschappelijke ICT-dienstverlening valt. Dit netwerk is beschikbaar over heel Vlaanderen en entiteiten kunnen aansluiting aanvragen en hun systemen eraan koppelen.
[11] 802.1X is een standaard voor geverifieerde toegang tot bekabelde Ethernet-netwerken en draadloze 802.11-netwerken. Deze standaard zorgt voor een betere beveiliging via o.a. gecentraliseerde gebruikersidentificatie en sleutelbeheer.

2) *Draadloos netwerk onvoldoende beschermd tegen toegang door onbevoegden.*
Eén entiteit, die zelf haar draadloos netwerk beheert, past geen *best practices* toe, waardoor onbevoegden zichzelf met vreemde toestellen toegang kunnen verschaffen zonder fysieke toegang tot de gebouwen van de respectievelijke entiteit.
Het draadloze buroticanetwerk, voorzien voor de interne gebruikers in beheer bij de gemeenschappelijke ICT-dienstverlener, bleek, op basis van de uitgevoerde testen, wel afdoende beveiligd om toegang door onbevoegden en niet-geautoriseerde systemen tegen te gaan. Voor het bezoekersnetwerk, dat enkel toegankelijk is door middel van een tijdelijke gebruiker, is er een strikte scheiding voorzien. Een bezoeker heeft via dit kanaal geen toegang tot het buroticanetwerk of andere interne systemen, wat de risico's van dit specifieke kanaal tot een minimum beperkt.

3) *Applicaties aangesloten op VONET zijn vaak onvoldoende beveiligd.*
De gemeenschappelijke ICT-dienstverlener voorziet een interne koppeling (VONET of het Vlaamse Overheidsnetwerk) tussen netwerken van verschillende entiteiten van de Vlaamse overheid en derden. Entiteiten zijn zich vaak onvoldoende bewust van het groot aantal toepassingen en personen die gebruik maken van deze koppeling. Hierdoor wordt vaak een lager niveau van beveiliging toegepast dan bij andere internet-gekoppelde systemen, zoals bvb. zwakke authenticatiemechanismen (geen of zwakke wachtwoorden) en het niet-versleutelen van gevoelige gegevens die over dit kanaal worden uitgewisseld (encryptie).

4) *Een degelijke scheiding tussen gebruikersnetwerken en de test- of productiesystemen vormt een aandachtspunt.*
De beveiligingstesten tonen aan dat verschillende entiteiten te weinig aandacht besteden aan een degelijke scheiding tussen gebruikersnetwerken en test- of productiesystemen. Zo blijkt bvb. dat bepaalde testinfrastructuur of beheerplatformen bereikbaar zijn voor een te grote groep gebruikers. Het is evenwel een goede praktijk om dergelijke serveromgevingen af te schermen, bvb. d.m.v. een firewall. Hiermee wordt het risico op ongeoorloofde toegang tot productiesystemen geminimaliseerd en wordt de blootstelling aan malware of aanvallen vanuit het gebruikersnetwerk ingeperkt.

2.2.3 Versleuteling van informatie

Om de vertrouwelijkheid van informatie over het informaticanetwerk te garanderen, bestaat de mogelijkheid om gegevens en communicatie tussen verschillende systemen te versleutelen. Een typisch voorbeeld van versleuteling is het gebruik van 'HTTPS' bij het bezoeken van een website.

De resultaten van deze thema-audit tonen evenwel aan dat slechts weinig entiteiten een duidelijke classificatie van informatie opstellen of dat, indien er een summiere classificatie opgesteld wordt, deze niet als richtinggevend gehanteerd wordt voor de implementatie van technische maatregelen, zoals bvb. versleuteling van data.
De veiligheidstesten bevestigen dan ook dat er vaak een gebrek is aan adequate versleuteling van informatie en uitwisseling ervan. Hierdoor bestaat het risico dat een kwaadwillende gebruiker de communicatie onderschept en zich toegang verschaft tot gevoelige informatie, zoals bvb. gebruikersnamen en wachtwoorden of dossiers van burgers, personeelsleden of ondernemingen. De onderschepte informatie kan een hacker vervolgens in staat stellen om de controle over te nemen van belangrijke systemen en componenten van de infrastructuur.

Concreet werd vastgesteld dat:
- De harde schijven in het persoonlijke informaticamateriaal van gebruikers, en in het bijzonder laptops, niet versleuteld zijn. Hierdoor kan een persoon met fysieke toegang tot dit informaticamateriaal alle gegevens raadplegen die op de harde schijf zijn opgeslagen.
  Hoewel veel entiteiten als richtlijn hanteren dat gevoelige gegevens niet op de lokale harde schijf mogen worden opgeslagen, werd in de praktijk vastgesteld dat deze richtlijn niet consequent wordt opgevolgd.

- Een aantal toepassingen geen gebruik maken van versleuteling, zelfs wanneer ze kritieke informatie verwerken en beheren. Tijdens de technische testen werd vastgesteld dat er intern onvoldoende tot geen gebruik gemaakt wordt van versleutelde protocollen. Dit zorgt ervoor dat data, inclusief gebruikersnaam en paswoord, op een onbeschermde manier verzonden worden van en naar de server. Een aanvaller die deze communicatie kan onderscheppen, kan bijgevolg in het bezit geraken van geldige authenticatiegegevens.
- Indien een versleuteling van communicatie wordt toegepast, dit in veel gevallen niet optimaal is ingesteld. Zo blijkt bvb. dat bepaalde certificaten niet erkend of vervallen zijn. Dit heeft als gevolg dat de communicatie mogelijks onvoldoende wordt versleuteld om de confidentialiteit te garanderen en onbevoegden de mogelijkheid biedt om bvb. webverkeer te onderscheppen.

2.2.4 Systeembeveiliging

Om een goede beveiliging van systemen te garanderen, is het belangrijk de aandacht te vestigen op:
- een regelmatige opvolging van veiligheidsupdates en –patches;
- een veilige configuratie van systemen en applicaties.

Opvolging van veiligheidsupdates en -patches
Uit de beveiligingstesten blijkt dat updates voor Windows-systemen en -servers over het algemeen systematisch worden bijgehouden; voor andere systemen en toepassingen gebeurt dit echter ad-hoc of helemaal niet. Een aantal systemen worden niet meer ondersteund door de leverancier en moeten dus inherent als onveilig worden beschouwd. Deze systemen vormen een zwakke schakel in de beveiliging van de infrastructuur, wat kan zorgen voor een aanzienlijke impact op de confidentialiteit, de integriteit en de beschikbaarheid van de systemen, de toepassingen en de bijhorende informatie.

Veilige configuratie van systemen en applicaties
M.b.t. de configuratie van de systemen en toepassingen kon worden vastgesteld dat richtlijnen gericht op een veilige basisconfiguratie vaak ontbreken. Het niet-wijzigen van standaardinstellingen, zoals bvb. standaard wachtwoorden, of het niet-uitschakelen van onnodige functionaliteiten verhogen de kwetsbaarheid van de IT-infrastructuur. Bij sommige entiteiten is tevens vastgesteld dat gebruikers antivirusoplossingen kunnen uitschakelen.

2.2.5 Toegangs- en gebruikersbeheer

Algemene bevindingen m.b.t. toegangs- en gebruikersbeheer
Een degelijke beheersing van processen voor het aanmaken, toekennen en afnemen van gebruikersrechten is onontbeerlijk voor een adequate afscherming van de toegang tot toepassingen en gegevens. Dergelijke processen vormen de basis voor de implementatie van technische maatregelen om de toegang tot informatie in te beperken.

Over het algemeen kon worden vastgesteld dat:

- De processen m.b.t. het toegangs- en gebruikersbeheer goed onder controle zijn wat betreft het tijdig en correct aanmaken van nieuwe gebruikers en het toekennen van rechten. Hierbij dient evenwel opgemerkt te worden dat vaak gebruik gemaakt van een referentiegebruiker, zijnde een gebruiker waarvan de rechten overgenomen worden voor een nieuw profiel. Als gevolg hiervan is het mogelijk dat aan een nieuwe gebruiker meer rechten toegekend worden dan strikt nodig voor de invulling van zijn functie, wat in strijd is met het principe van het toekennen van de minimale vereiste privileges.

- Er geregeld onvoldoende aandacht besteed wordt aan het tijdig intrekken van toegangen en rechten, bvb. bij het vertrek van een medewerker. Hierdoor zouden gebruikers toegang kunnen behouden tot de omgeving en mogelijks tot gevoelige informatie. Sommige organisaties beperken dit risico door op regelmatige tijdstippen inactieve accounts (d.w.z. gebruikers die een vast aantal dagen niet zijn aangemeld) automatisch te deactiveren. Dit lijkt een goede maatregel maar is niet doeltreffend als een gebruiker zijn/haar account na het vertrek oneigenlijk verder blijft gebruiken.

- Voor het beheer van systemen vaak gebruik gemaakt wordt van generieke accounts. Dit zijn accounts die niet gekoppeld zijn aan een unieke fysieke gebruiker, maar typisch gedeeld worden door verschillende personen, bvb. voor het beheren van een specifieke toepassing, systeem of een volledige IT-omgeving. Dit brengt een aantal mogelijke gevolgen met zich mee:
  - Het paswoord van een generiek gebruikersaccount wordt in klare tekst opgeslagen in broncode of scripts die door onbevoegden raadpleegbaar zijn;
  - Acties ondernomen met een generieke gebruiker kunnen zonder extra maatregelen niet herleid worden naar de fysieke persoon die deze heeft uitgevoerd (traceerbaarheid);
  - Het is moeilijk bij te houden welke personen in het bezit zijn van het gedeelde paswoord. Bovendien zouden dergelijke paswoorden moeten gewijzigd worden bij vertrek van een medewerker die er kennis van heeft, wat in de praktijk zelden gebeurt.

- Vaak zwakke wachtwoorden gehanteerd worden door zowel gebruikers als beheerders van toepassingen of productiesystemen. Hierbij dient te worden opgemerkt dat het centrale gebruikerssysteem geen regelmatige wijziging van wachtwoorden vereist.
  Bovendien blijkt dat bij de uitbesteding aan de gemeenschappelijke ICT-dienstverlener een groot aantal beheerders van die dienstverlener toegang heeft tot bepaalde productiesystemen en hierbij een identiek of sterk gelijkend zwak wachtwoord hanteert. Het merendeel van deze gebruikers heeft zich bovendien nooit op deze systemen aangemeld.

Authenticatie (ACM) en identificatie (IDM) .
Het ACM (Access Controle Management)-platform staat in voor het beheer van de toegangscontrole voor informatiebronnen en toepassingen. Het laat toe om via een centraal systeem de authenticatie van gebruikers te behandelen, waardoor personen voor de aangesloten toepassingen slechts over één gebruikersnaam en paswoord moeten beschikken. Naast ACM werd het IDM (Identity Management)-platform opgezet voor het gebruikersbeheer van toepassingen. Hiermee wordt bepaald wie er toegang heeft tot welke informatie en welke rechten deze personen krijgen. Via ACM/IDM is het mogelijk om wijzigingen aan gebruikersrechten (bvb. bij indiensttreding, vertrek of mutatie) centraal op te volgen en om een eenduidig beleid te hanteren m.b.t. bvb. wachtwoordbeheer.

Tot op heden zijn ongeveer één derde van de toepassingen van de Vlaamse Overheid gekoppeld aan deze centrale ACM/IDM-oplossing. Tijdens de veiligheidstesten werden geen kritieke kwetsbaarheden inzake informatiebeveiliging vastgesteld m.b.t. het ACM/IDM-platform. Op het IDM-platform waren evenwel een aantal kwetsbaarheden met mogelijks een hoog risico aanwezig.

2.2.6 Fysieke toegangsbeveiliging

De fysieke toegangsbeveiliging van de centrale gebouwen wordt centraal aangestuurd door het Facilitair Bedrijf. In de praktijk blijkt dat het relatief eenvoudig is om op een ongeautoriseerde wijze toegang te verkrijgen tot deze gebouwen. Door de samenhang met andere technische kwetsbaarheden is het risico op toegang tot en ontvreemding van informatie/documentatie door onbevoegden bijgevolg reëel.

Dankzij de evolutie naar het nieuwe werken groeit het draagvlak voor de toepassing van het clean desk-principe binnen de entiteiten van de Vlaamse overheid. Desalniettemin kon worden vastgesteld dat archiefkasten, met vertrouwelijke informatie, niet altijd slotvast afgesloten waren.

Op het vlak van een clear screen-beleid is eveneens nog verbetering mogelijk. De gebruikerssystemen worden soms onbeheerd achtergelaten waardoor een kwaadwillende persoon zich via dat systeem toegang kan verschaffen tot applicaties en/of informatie. In druk bezette kantoren kan de sociale controle misbruik te voorkomen, in andere kantoren speelt dit niet. Gebruikerssystemen worden evenwel vaak na enkele minuten automatisch afgesloten worden waardoor het risico op misbruik via deze weg beperkt is.

3 Toekomstige uitdagingen/trends

Het vorige hoofdstuk van dit rapport behandelde de belangrijkste organisatorische en technische kwetsbaarheden die vandaag de dag binnen de Vlaamse overheid vastgesteld worden. De wereld van digitalisering staat evenwel niet stil. Nieuwe trends worden immers dagelijks geïntroduceerd en geven aanleiding tot nieuwe uitdagingen en mogelijke bedreigingen op het vlak van informatiebeveiliging.

Het *Information Security Forum*[12] (ISF) stelt jaarlijks een rapport op waarin de verwachte trends en bedreigingen op het vlak van informatiebeveiliging samengevat worden. Een aantal van deze trends voor de komende jaren zijn:

1. Groeiend gebruik van cloud-toepassingen;
2. Tendens naar big data;
3. Toenemende privacy-regulering;
4. Hacktivisme;
5. Persoonlijk informaticamateriaal van gebruikers en mobiele applicaties (apps) als toegangspoort tot gevoelige informatie.

Audit Vlaanderen onderzocht in welke mate de Vlaamse overheid in staat is om in te spelen op en om te gaan met de toekomstige evoluties inzake digitale veiligheid. Vanuit de gedane vaststellingen i.h.k.v. deze thema-audit worden elk van de bovenvermelde trends nader bekeken.

1) Groeiend gebruik van cloud-toepassingen:

Populaire voorbeelden van cloud-toepassingen in de persoonlijke context zijn Dropbox of Google Docs. In de professionele context verwijst de cloud naar diensten waarbij een applicatie wordt aangeboden door leveranciers zonder dat de overheid zelf controle heeft over de software of hardware die gebruikt wordt. Via het internet wordt toegang verkregen tot een applicatie zoals bvb. een documentbeheersysteem.

In het kader van de uitvoering van deze thema-audit kon worden vastgesteld dat een aantal entiteiten het gebruik van cloud-toepassingen in overweging nemen of bezig zijn met de transitie van applicaties en gegevens naar een cloud-toepassing (zoals bvb. mail- en dataopslagplatformen van Google of HB-plus).
Een dergelijke transitie gaat op dit moment nog te weinig samen met een duidelijke classificatie van informatie die richtinggevend is voor de opname van data in de cloud, noch met een analyse van de risico's die gepaard gaan met het gebruik van de cloud en met contractuele afspraken die de residuele risico's voor de organisatie zo laag mogelijk houden. Hierdoor bestaat de kans dat te veel vertrouwen gegeven wordt aan de cloud-leverancier en dat zowel de controle over de hard- en software als over de data verloren gaat.
Bovendien bestaat er momenteel geen visie of zijn er geen richtlijnen m.b.t. de implementatie van cloud-toepassingen binnen de Vlaamse overheid.

2) Tendens naar big data:

"Big data" is een populaire term die refereert naar de technieken voor het beheren en exploiteren van grote hoeveelheden data. Op basis van statistische bewerkingen kunnen hieruit conclusies getrokken worden die kunnen bijdragen tot de beleidsvoorbereiding, -uitvoering of –evaluatie.

Hoewel "big data" ook voor de Vlaamse overheid mogelijke opportuniteiten biedt, brengt het ontsluiten en manipuleren van grote hoeveelheden data met deze technieken ook bijkomende risico's inzake confidentialiteit, integriteit en beschikbaarheid met zich mee. Gezien de vastgestelde onvolkomenheden inzake informatieclassificatie en toewijzing van het eigenaarschap van gegevens, blijkt de Vlaamse overheid hierop onvoldoende voorbereid.

[12] Het Information Security Forum is een onafhankelijke, non-profit vereniging van organisaties uit de hele wereld die zich toelegt op het onderzoeken, verduidelijken en oplossen van de belangrijkste problemen rond informatiebeveiliging.

3) *Toenemende privacy-regulering:*
Door de toenemende digitalisering wordt verwacht dat de regulering omtrent de bescherming van persoonlijke gegevens enkel nog zal toenemen. Het opvolgen en implementeren van deze toenemende regulering vormt ook voor de Vlaamse overheid een belangrijke uitdaging omwille van de onderstaande tekortkomingen, m.n.:
- Het gebrek aan bewustzijn, kennis en competenties omtrent informatiebeveiliging;
- De moeilijkheid van het vinden van een balans tussen informatiebeveiliging, operationele efficiëntie en werkbaarheid en budget.

4) *Hacktivisme:*
De term "hacktivisme" betreft een samenvoeging van hacken en activisme, waarbij als daad van protest of vanuit persoonlijk gewin ICT-systemen worden aangevallen of ongeautoriseerde toegang wordt bekomen tot gevoelige informatie. Voorbeelden hiervan zijn o.a. het aanpassen van websites om politieke boodschappen uit te dragen of het bemachtigen van persoonsgegevens om deze vervolgens over te dragen aan de media. Ook de toename van staatsgebonden aanvallen waarbij telecommunicatiebedrijven, financiële instellingen en overheden als doelwit gekozen worden, dienen in dit kader vermeld te worden.

De Vlaamse overheid, haar ICT-systemen, -applicaties en websites, dienen dan ook als mogelijk doelwit te worden aanzien. De vastgestelde organisatorische en technische kwetsbaarheden gecombineerd met het ontbreken van een aanspreekpunt voor de opvolging van en communicatie inzake cyberbeveiliging en het gebrek aan degelijke incidentmanagementprocessen tussen de verschillende entiteiten, incl. de gemeenschappelijke ICT-dienstverlener, wijzen erop dat de organisatie kwetsbaar is voor mogelijke aanvallen van hacktivisme.

5) *Persoonlijk informaticamateriaal van gebruikers en mobiele applicaties (apps) als toegangspoort tot gevoelige informatie:*
Het stijgend gebruik van smartphones, tablets en eigen gebruiksapparatuur (BYOD of Bring Your Own Device) wordt beschouwd als een mogelijke, toekomstige bedreiging op het vlak van informatiebeveiliging. Om de risico's gerelateerd aan eigen gebruiksapparatuur in te perken, houdt de gemeenschappelijke ICT-dienstverlener vast aan de richtlijn dat persoonlijk informaticamateriaal van gebruikers in principe niet toegelaten is op het netwerk. Smartphones en tablets worden ter beschikking gesteld door en geconfigureerd volgens de gemeenschappelijke ICT-dienstverlening.

In dit verband dient te worden gewezen op het risico m.b.t. het toenemend gebruik van specifieke mobiele applicaties (zgn. apps). Het vastgestelde gebrek aan richtlijnen voor de ontwikkeling van veilige software duidt erop dat informatiebeveiliging ook bij de ontwikkeling van deze mobiele applicaties niet uit het oog mag worden verloren.

Bijlage: Overzicht risicoafdekking

De onderstaande tabel geeft de risicoafdekking weer op basis van de uitgevoerde auditwerkzaamheden bij 6 entiteiten. De inschattingen zijn anoniem weergegeven. De tabel bevat de resultaten overeenkomstig de thema's uit het controleprogramma.

Legende:

kritiek	De vastgestelde beheersmaatregelen volstaan niet. Er werd minstens één aanbeveling geformuleerd.
hoog	De vastgestelde beheersmaatregelen zorgen voor gedeeltelijke afdekking van het beveiligingsrisico. Er werden aanbevelingen en/of verbetersuggesties geformuleerd.
midden	De vastgestelde beheersmaatregelen zijn voldoende effectief om een aanvaardbare risicoafdekking te garanderen. Er werden enkel verbetersuggesties geformuleerd.
laag	Er werden geen vaststellingen gedaan met betrekking tot controlelacunes. Er werden geen aanbevelingen of verbetersuggesties meegegeven.

	Entiteit 1	Entiteit 2	Entiteit 3	Entiteit 4	Entiteit 5	Entiteit 6
Informatiebeveiligingsbeleid- en organisatie	●	●	●	⬢	●	▲
Architectuur	▲	▲	⬢	■	▲	⬢
Informatieclassificatie	●	▲	■	■	●	▲
Outsourcing	■	▲	■	■	▲	▲
Audit en logging	■	▲	■	⬢	■	■
Bewustzijn	▲	▲	■	▲	▲	■
Fysieke toegangsbeveiliging	■	■	■	⬢	■	■
Netwerkbeveiliging	■	▲	▲	■	▲	▲
Systeembeveiliging	■	■	▲	■	▲	▲
Authenticatie en logische toegangsbeveiliging	▲	▲	▲	⬢	▲	■
Incidentenbeheer	■	▲	⬢	⬢	⬢	⬢
Wijzigingsbeheer	●	●	■	▲	▲	■
Back-up beheer	■	■	⬢	■	■	■
Configuratie- en operationeel beheer	■	▲	■	⬢	▲	▲
Gebruik van mobiele informatiedragers	■	■	⬢	⬢	■	⬢

AUDIT
VLAANDEREN

Colofon

VERANTWOORDELIJKE UITGEVER
Eddy Guilliams
administrateur-generaal
Audit Vlaanderen

CONTACT
Audit Vlaanderen
Boudewijnlaan 30, bus 24
1000 Brussel
T 02 553 45 55

Meer info over Audit Vlaanderen kunt u terugvinden op
www.auditvlaanderen.be.

DEPOTNUMMER
D/2015/3241/138