Thema-audit Informatiebeveiliging

Globaal rapport | 18 september 2018

Vlaamse overheid

AUDIT VLAANDEREN

De auditopdrachten die de onderliggende basis voor dit globaal rapport vormen, zijn 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.

Thema-audit Informatiebeveiliging

Globaal rapport | 18 september 2018

Vlaamse overheid

AUDIT VLAANDEREN

INHOUDSOPGAVE

SAMENVATTING

Lokale besturen beveiligen vertrouwelijke en (persoons)gevoelige informatie onvoldoende.

Audit Vlaanderen evalueerde in de thema-audit Informatiebeveiliging bij 28 lokale besturen (zie bijlage 1) de mate waarin ze de integriteit, de vertrouwelijkheid en de beschikbaarheid kunnen garanderen van de vertrouwelijke en (persoons)gevoelige informatie waarover zij beschikken of die zij verwerken.

De lokale besturen nemen wel initiatieven rond informatiebeveiliging, maar ze dekken hiermee de risico's nog onvoldoende af. Burgers, bedrijven en andere overheden hebben bijgevolg onvoldoende garanties dat hun gegevens veilig zijn bij hun lokale bestuur. Hoewel hieraan niet veel ruchtbaarheid wordt gegeven, heeft dit nu en dan wel degelijk gevolgen (zie bijlage 4).

Bij de geauditeerde besturen testte Audit Vlaanderen in samenwerking met extern ingehuurde experten welke impact iemand met kwade bedoelingen kan hebben wanneer die daar fysiek langsgaat. Bij 24 van de 28 besturen konden de ingehuurde ethische hackers controle krijgen over de volledige IT-omgeving of de belangrijkste delen ervan. Dergelijke controle laat toe de werking stil te leggen, kennis te nemen van alle gegevens en deze te manipuleren. De betrokken IT-verantwoordelijken kregen telkens informatie over de openstaande deuren die ze moesten sluiten. Waar relevant, mogelijk ook voor gelijkaardige situaties bij andere klanten, werden ook de betrokken software- en IT-dienstenleveranciers ingelicht. Besturen en hun leveranciers leverden vervolgens inspanningen om deze kwetsbaarheden te beheersen. Toch tonen opvolgtests aan dat een belangrijk deel van de gesignaleerde deuren verschillende maanden later nog steeds openstaat.

Er is dus werk aan de winkel.

Elk individueel bestuur is er voor verantwoordelijk om de vertrouwelijke en (persoons)gevoelige informatie waarover ze beschikt of die ze verwerkt, te beschermen in de mate dat de maatschappij dit verwacht. Die verwachtingen evolueren mee met de digitalisering. Denken we maar aan de opkomst van sociale media of aan de Algemene Verordening Gegevensbescherming (AVG). Problemen met informatiebeveiliging ondergraven tegenwoordig geregeld ook het vertrouwen in het bestuur en in de dienstverlening.

Een structurele aanpak en periodieke opvolging zijn aangewezen pistes om vooruitgang te boeken. Verschillende van de geauditeerde besturen verbeterden op die manier de afgelopen jaren reeds stapsgewijs hun informatiebeveiliging. Veel van de vastgestelde problemen kunnen bovendien met gezonde reflexen en een goede discipline in grote mate worden vermeden. Verschillende haalbare beschermingsmaatregelen worden echter nog te weinig benut (zie verder).

Om alle inspanningen ter verbetering van de informatiebeveiliging goed te borgen, is naast de structurele aanpak van het informatiebeveiligingsbeleid ook een goed invulling van rollen en verantwoordelijkheden belangrijk. Daarbij is de organisatie van de IT-functie een belangrijk aandachtspunt. Vaak is de opzet en invulling daarvan historisch gegroeid eerder dan het gevolg van weloverwogen keuzes. Besturen die wel duidelijke keuzes hebben gemaakt en bewust inzetten op informatiebeveiliging slagen er beter in de nodige garanties voor de informatiebeveiliging te voorzien.

Verschillende van de uitdagingen rond informatiebeveiliging zijn zo groot en complex dat geen enkel geauditeerd lokaal bestuur alle risico's daaromtrent zelfstandig kan beheersen. Naast de individuele inspanningen is daarom ook meer samenwerking een belangrijk element om als bestuur voldoende garanties te kunnen bieden omtrent informatiebeveiliging.

Enerzijds is er nood aan meer horizontale/overkoepelende samenwerking tussen besturen.
Immers is het voor een individueel bestuur vaak niet mogelijk om alle vereiste expertises zelf in huis te hebben. Door samenwerking kan de expertise die aanwezig is bij één bestuur gedeeld worden met andere besturen (die aanvullend hun expertises kunnen delen). Ook kunnen door samenwerking efficiënter gedragen oplossingen worden uitgewerkt voor de uitdagingen waar elk bestuur voor staat.
Zo kunnen gezamenlijk meer en betere garanties worden uitgewerkt voor de informatiebeveiliging.

Anderzijds is er ook ruimte voor meer verticale samenwerking met de verschillende actoren.
Hoewel leveranciers en besturen elkaar continu tegenkomen en elkaars informatiebeveiliging beïnvloeden, valt op hoe weinig daar onderling over gesproken wordt. Concrete afspraken kunnen misverstanden voorkomen door duidelijker te maken wat de noden en verwachtingen zijn, welke garanties worden geboden en waar kwetsbaarheden kunnen ontstaan door niet of onvoldoende afgedekte verwachtingen.
Ook tussen bestuursniveaus en tussen besturen en ondersteunende organisaties is de communicatie nog voor verbetering vatbaar.

Een structurele aanpak en periodieke opvolging zijn aangewezen pistes om vooruitgang te boeken.

Verschillende van de geauditeerde besturen verbeterden de afgelopen jaren reeds stapsgewijs hun informatiebeveiliging. Net zoals bij de ruimere organisatiebeheersing bleek hierbij een structurele aanpak met periodieke opvolging zinvol om vooruitgang te boeken.

Een uitgebreid informatiebeveiligingsbeleid kan hiervoor een solide basis bieden. Veel informatieveiligheidsconsulenten bieden sjablonen om dergelijk beleid op papier te zetten. Om succesvol te zijn, is het nodig om deze te concretiseren door ze aan te vullen met onder meer gedragen keuzes en maatregelen op maat van het eigen bestuur.
Om van de actuele situatie te evolueren naar de gewenste, is een informatieveiligheidsplan vaak een goed instrument. De voortgang van de acties moet dan wel voldoende worden opgevolgd.

De verschillende rollen en verantwoordelijkheden rond informatiebeveiliging kunnen nog worden geoptimaliseerd.

De meeste geauditeerde besturen organiseren een informatieveiligheidscel waarin ze enkele betrokkenen periodiek samenbrengen. De frequentie waarmee deze cel samenkomt en de wijze waarop ze contact houdt met de rest van de organisatie kunnen vaak nog worden verbeterd.

Alle geauditeerde besturen stelden een informatieveiligheidsconsulent aan. De dienstverlening van deze informatieveiligheidsconsulenten varieert evenwel sterk en dekt vaak niet alle aspecten van de informatiebeveiliging. Ondanks hun inspanningen om medewerkers te sensibiliseren en informatieveiligheidsplannen op te stellen, werden tijdens deze thema-audit talrijke kwetsbaarheden en verbeterpunten vastgesteld. Over het takenpakket van de informatieveiligheidsconsulenten (+ de functionarissen voor gegevensbescherming) en de verwachte wisselwerking met de besturen, kunnen dan ook betere afspraken worden gemaakt.

In de praktijk zijn het vooral de (interne en externe) IT-verantwoordelijken die de informatiebeveiliging technisch moeten realiseren. Lokale besturen organiseren hun IT veelal in functie van de praktische noden en op basis van een historisch gegroeide individuele invulling. De diversiteit van de vereiste expertises, de daarmee samenhangende noden en de daartoe benodigde inzet van middelen worden vaak onderschat.
De uitbouw van informatiebeveiliging vereist weloverwogen keuzes: bv. rond uitbesteding, samenwerking, technologieën, IT-verwachtingen en uitgaven. Zo moet IT meer worden georganiseerd in overeenstemming met de behoeften en de doelstellingen van de organisatie, ook deze op het vlak van informatiebeveiliging.

Alle besturen vertrouwen in zekere mate op externe software- en IT-dienstenleveranciers. Het is echter onduidelijk in hoeverre deze leveranciers de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens garanderen. Zelfs al stellen ze zich in de praktijk klantvriendelijk en welwillend op, toch blijken de leveranciers hun rol vaak beperkter te zien dan waar het bestuur denkt op te mogen vertrouwen.
Slechts een minderheid van de geauditeerde besturen heeft afspraken met zijn leveranciers over wie welke verantwoordelijkheden draagt, wie welke taken uitvoert en hoe deze minimaal ingevuld moeten worden.

Talrijke uitdagingen lenen zich bij uitstek tot samenwerking.

Elk lokaal bestuur dient zijn informatiebeveiliging te garanderen. Hoe kleiner het bestuur, hoe moeilijker dat vaak blijkt. De uitzonderingen maken vaak meer doordachte keuzes, onder meer qua uitbesteding. Kleine besturen beperken soms ook hun inzet van IT. Meer samenwerking, enerzijds tussen lokale besturen onderling, anderzijds met alle actoren kan helpen om de nodige garanties te kunnen realiseren. Bepaalde uitdagingen en activiteiten lenen zich bijzonder tot een overkoepelende aanpak:

- de vertaling van de relevante regelgeving naar vlot inzetbare oplossingen zoals richtsnoeren, procedures, werkdocumenten en sjablonen;
- de identificatie van en actieve kennisdeling over nieuwe bedreigingen;
- de voorlichting over en promotie van onderbenutte mogelijkheden voor informatiebeveiliging;
- de opvolging van de feitelijke informatiebeveiliging via technische testen.

Voor de meeste besturen is het moeilijk om goed zicht te krijgen op hun noden en om te bepalen welke keuzes aangewezen zijn. Aangezien de geauditeerde besturen zelf geen IT-systemen of -oplossingen ontwikkelen, zijn ze bovendien in grote mate aangewezen op de keuzes en het aanbod van hun IT-leveranciers. Ook daarvoor is samenwerking aangewezen: enerzijds horizontaal om de nodige expertise te verzamelen om de noden en keuzes te kunnen bepalen, anderzijds verticaal met alle partijen om te komen tot oplossingen die afgestemd zijn op enerzijds de noden en keuzes van de besturen en anderzijds de mogelijkheden van de leveranciers.

Audit Vlaanderen laat in het midden welke samenwerkingsverbanden hiertoe het beste geschikt zijn. Voorlopig neemt echter geen enkele partij deze handschoen voldoende op.

Veel haalbare beschermingsmaatregelen blijven onderbenut.

Om de data van burgers en bedrijven afdoende te beschermen, zijn niet altijd geavanceerde technische systemen nodig. Lokale besturen kunnen een groot aantal vastgestelde risico's vermijden met gezonde reflexen en een goede discipline. Veel van de vastgestelde risico's zijn het gevolg van onvervulde verwachtingen en/of een onderschatting van de IT-risico's. De beheersing van de risico's kan dan ook al sterk worden verbeterd wanneer de lokale besturen en hun leveranciers onderling goed afspreken voor het:

- tijdig bijwerken van zowel besturingssystemen, toepassingen als ondersteunende IT-systemen;
- sluitend beheren van toegangen en rechten;
- gebruiken en afdwingen van sterke wachtwoorden voor alle gebruikers;
- gepast omgaan met versleutelingsmechanismen;
- doordacht segmenteren of monitoren van het netwerk van het bestuur zodat achterliggende systemen minder kwetsbaar zijn voor infecties op eindgebruikersapparatuur;
- periodiek testen van de continuïteitsmaatregelen;
- communiceren, registreren, behandelen en rapporteren van incidenten;
- opvolgen van de kwetsbaarheden en van de levenscyclus van hard- en software.

Goede afspraken hierover, met gepaste verantwoording en/of monitoring, zijn vooral nodig om de technische beveiliging van de IT-omgevingen te verbeteren en zo de gegevens die de besturen verwerken en opslaan te beschermen tegen computercriminelen en de schade bij incidenten te beperken.

Onderstaande figuur is geïnspireerd op indelingen die ook worden gebruikt in het ISO-raamwerk omtrent informatiebeveiliging. De kleurvlakken in deze figuur tonen het gemiddelde resultaat voor de 28 geauditeerde besturen weer (De legende van de gehanteerde kleuren staat onder de figuur). De (geanonimiseerde) resultaten per bestuur staan in bijlage 2.

Onderstaande legende verklaart de kleuren van de figuren in dit rapport:

0 **Onbestaand**
Er bestaan geen of zeer weinig beheersmaatregelen. Het controlebewustzijn is eerder laag en er worden weinig acties ondernomen om te komen tot een adequaat systeem van organisatiebeheersing (intern controlesysteem).

1 **Ad-hocbasis**
Op ad-hocbasis zijn er beheersmaatregelen uitgewerkt. Het bewustzijn van de nood aan adequate beheersmaatregelen (interne controlemaatregelen) groeit, maar er is nog geen gestructureerde of gestandaardiseerde aanpak. Het systeem van organisatiebeheersing (intern controlesysteem) draait meer rond personen dan rond systemen.

2 **Gestructureerde aanzet**
Er is een gestructureerde aanzet tot de ontwikkeling van beheersmaatregelen. De beheersinstrumenten zijn dus in ontwikkeling, maar worden nog niet toegepast ('Plan').

3 **Gedefinieerd**
Beheersmaatregelen zijn aanwezig. Zij zijn gestandaardiseerd, gedocumenteerd, gecommuniceerd en worden toegepast ('Do').

4 **Beheerst systeem (= niveau 3 +)**
De beheersmaatregelen zijn periodiek intern geëvalueerd en bijgestuurd ('Check' & 'Act'). Er is een 'levend' adequaat en doeltreffend systeem van organisatiebeheersing.

Lies Van Cauter (Signature)
Digitaal ondertekend door Lies Van Cauter (Signature)
Datum: 2018.09.17 11:22:17 +02'00'

Lies Van Cauter,
Auditor

Karel Bruneel (Signature)
Digitaal ondertekend door Karel Bruneel (Signature)
Datum: 2018.09.17 11:00:10 +02'00'

Karel Bruneel,
Senior-auditor

Gunter Schryvers (Signature)
Digitaal ondertekend door Gunter Schryvers (Signature)
Datum: 2018.09.17 12:23:24 +02'00'

Gunter Schryvers,
Manager-auditor

Mark Vandersmissen (Signature)
Digitaal ondertekend door Mark Vandersmissen (Signature)
Datum: 2018.09.17 13:06:35 +02'00'

Mark Vandersmissen,
Administrateur-generaal

LEESWIJZER

Dit rapport gaat in op de globale resultaten van de thema-audit Informatiebeveiliging bij de lokale besturen. Het is als volgt gestructureerd:

- De inleiding omschrijft de opzet van de thema-audit.
- Deel 1 beschrijft de elementen van informatiebeveiliging waarvoor de belangrijkste risico's onvoldoende beheerst zijn.
- Deel 2 licht verbeterpunten bij kleine en middelgrote risico's toe die de geauditeerde besturen onvoldoende beheersen.
- Deel 3 gaat in op hoe besturen kunnen werken aan informatiebeveiliging. Daarbij worden mogelijke acties richting verbetering aangebracht.

Een overzicht van de geauditeerde besturen is opgenomen in bijlage 1.
Een geanonimiseerd overzicht van de resultaten per audit is terug te vinden in bijlage 2.
De resultaten van de parallelle phishing-test zijn opgenomen in bijlage 3.
In bijlage 4 zijn enkele voorbeelden van informatiebeveiligingsincidenten opgenomen ter illustratie van de risico's.
In bijlage 5 zijn ter inspiratie enkele bestaande voorbeelden van vlot inzetbare oplossingen terug te vinden.
In bijlage 6 zijn enkele vaststellingen in cijfers uitgedrukt.

DANKWOORD

Audit Vlaanderen dankt de geauditeerde besturen voor de constructieve samenwerking. Dit globaal rapport kwam tot stand dankzij hun waardevolle inbreng.

Audit Vlaanderen waardeert de bereidheid van de betrokken IT-verantwoordelijken en van de diverse software- en IT-dienstenleveranciers wiens producten en/of diensten bij deze thema-audit betrokken waren om onze bevindingen te bespreken en constructief te bekijken hoe de situatie kan worden verbeterd. De vaststellingen tonen aan dat dit al tot verbeteringen geleid heeft, hoewel op andere vlakken bij de afronding van het terreinwerk van deze thema-audit ook duidelijk is dat nog inspanningen nodig zijn.

Audit Vlaanderen wil alle deelnemers aan de klankbordgroep danken voor hun constructieve houding en feedback. De klankbordgroep was voor ons nuttig bij de ontwikkeling van deze thema-audit en ook bij de aftoetsing van de bevindingen. De ruime aanwezigheid vanuit verschillende belanghebbenden op de klankbordgroep van 28 februari 2018 en de respectvolle actieve inbreng van alle zijden, toont het belang aan dat al deze organisaties hechten aan informatiebeveiliging.

INLEIDING

SITUERING AGENTSCHAP

Het agentschap Audit Vlaanderen heeft als opdracht het systeem van organisatiebeheersing van de lokale besturen en de Vlaamse administratie te evalueren. Die evaluatie doet Audit Vlaanderen door audits uit te voeren. Twee auditcomités sturen Audit Vlaanderen aan: een auditcomité van de lokale besturen en een auditcomité van de Vlaamse administratie. De auditcomités staan in voor de strategische keuzes van en het toezicht op het agentschap.

Wat is organisatiebeheersing?

Organisatiebeheersing gaat over het in de hand hebben en de nodige sturing en opvolging geven aan een organisatie.
Elke organisatie is dus, al dan niet bewust, dagelijks bezig met organisatiebeheersing.
Hierdoor kan een organisatie de juiste dingen doen en deze dingen ook op de juiste manier doen. Organisatiebeheersing situeert zich zowel op organisatieniveau, op dienstniveau als op procesniveau.

CONTEXT THEMA-AUDIT

Informatiebeveiligingsrisico's zijn groot en reëel. En de noodzaak om ze aan te pakken neemt snel toe. Naarmate de dienstverlening meer digitaal verloopt en ook de werking meer steunt op IT-systemen, vergroot ook de potentiële impact van kwetsbaarheden (zie bijlage 4 voor enkele voorbeelden).

Stilstaan is geen optie op lange termijn omdat de digitalisering sneller werken, een ruimere bereikbaarheid en een betere dienstverlening mogelijk maakt. Een sluitende informatiebeveiliging is bovendien een essentiële voorwaarde om het vertrouwen in een bestuur ook in de digitale wereld te behouden.

Informatiebeveiliging is in belangrijke mate verbonden aan ICT, maar gaat over meer dan elektronische beveiliging alleen. Ook ruimten met gevoelige IT-systemen en vertrouwelijke documenten moeten beveiligd zijn. We zetten massaal informatie op papier of op digitale informatiedragers zoals usb-sleutels of smartphones maar staan zelden stil bij de risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie die daaraan verbonden zijn. Dat je sommige informatie beter niet laat rondslingeren, weten we eigenlijk al lang. Wanneer dit toch gebeurt, maken moderne technologieën en assertievere slachtoffers steeds vaker duidelijk wat de samenleving daarvan denkt.

De Europese Algemene Verordening Gegevensbescherming (AVG)[1] maakt de nood aan een gedegen informatiebeveiliging nog prangender. Doordat de voorbereidingen voor deze thema-audit gestart zijn vóór de goedkeuring van de verordening, werd niet specifiek gefocust op de vereisten opgelegd door deze verordening. Verschillende van de onderzochte aspecten zijn wel een belangrijke basis om aan de AVG te voldoen.

[1] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679&from=NL

DE AUDITAANPAK EN -DOELSTELLING

Audit Vlaanderen stelde een controleprogramma op om de informatiebeveiliging van lokale besturen op een consequente manier te onderzoeken. Dit controleprogramma omvat specifieke doelen, potentiële risico's en mogelijke beheersmaatregelen rond informatiebeveiliging. Het is gebaseerd op richtlijnen als de ISO/IEC 27000-serie voor het beheersen van informatiebeveiliging[2] en op de richtsnoeren informatiebeveiliging voor lokale besturen[3], die een gelijkaardige indeling volgen.

Het ontwerp-controleprogramma werd met verschillende experten afgetoetst en uitgetest bij drie lokale besturen. Voor de aanvang van de audits en tussentijds gaf een klankbordgroep met vertegenwoordigers van onder andere de verschillende overheidsniveaus en veiligheidsconsulentenorganisaties input voor en feedback over de inhoud, de werkwijze en de praktijkrelevantie van de audit. Later sloten softwareleveranciers aan bij deze groep.

Via het controleprogramma evalueerde Audit Vlaanderen in welke mate lokale besturen adequate beheersmaatregelen nemen om de gewenste beschikbaarheid, integriteit[4] en vertrouwelijkheid van de informatie te garanderen.

Een onvoldoende beheersing van deze drie concepten heeft immers potentieel grote gevolgen:

- Wanneer de beschikbaarheid van informatie, eventueel na een calamiteit, niet kan worden gegarandeerd, komt de continuïteit van de dienstverlening in het gedrang met hinder bij korte onderbrekingen en schade bij langdurende problemen (bv. voor burgers die de documenten die ze nodig hebben niet kunnen bekomen).
- Wanneer (de integriteit van de) informatie kan worden gemanipuleerd, is het niet zeker dat de juiste beslissingen worden genomen. In extremis kan het nemen en uitvoeren van beslissingen zelfs onmogelijk worden (bv. wanneer essentiële informatie via malware gewijzigd of versleuteld wordt).
- Wanneer de vertrouwelijkheid onvoldoende kan worden verzekerd, kunnen burgers en bedrijven hinder of zelfs schade ondervinden (bv. wanneer inbrekers kunnen zien wie aangeeft een tijdje niet thuis te zullen zijn).

Problemen hiermee ondergraven tegenwoordig geregeld ook het vertrouwen in het bestuur en in de dienstverlening. Wie zal bijvoorbeeld steun aanvragen via een e-loket of gebruikmaken van andere e-dienstverlening wanneer duidelijk is dat andere kanalen veiliger zijn?

[2] Meer bepaald de internationale normen ISO 27001 en ISO 27002 alsook de Nederlandse 'ISO/IEC 27001:2013 Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging'.

[3] Of voluit:
richtsnoeren m.b.t. de informatiebeveiliging van persoonsgegevens in steden en gemeenten, in instellingen die deel uitmaken van het netwerk dat beheerd wordt door de Kruispuntbank van de Sociale Zekerheid en bij de integratie OCMW-gemeente, versie 3 (https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Steden%20en%20gemeenten_v%203.0_0.pdf).

[4] Integriteit heeft betrekking op de accuraatheid en de volledigheid van de informatie en zijn validiteit, met andere woorden, de mate waarin besturen er kunnen op betrouwen dat de gegevens die ze gebruiken juist zijn en dus niet – bewust of onbewust – gewijzigd.

Een gedegen informatiebeveiliging speelt in op diverse facetten. Het controleprogramma focuste op 16 aspecten die onderverdeeld zijn in zes domeinen:

1. **Beleid en organisatie**

   Het management initieert en beheerst de informatiebeveiliging met zijn beleid en bepaalt rollen en verantwoordelijkheden voor alle interne en externe betrokkenen.

2. **Bewustzijn**

   Informatiebeveiliging is in sterke mate afhankelijk van gedrag. Het bewustzijn van medewerkers, mandatarissen, software- en IT-dienstenleveranciers rond informatiebeveiligingsrisico's is cruciaal. Lokale besturen kunnen hen op verschillende manieren sensibiliseren.

3. **Technisch beheer**

   Een goed technisch beheer vermijdt het misbruik van zwaktes in de beveiliging van IT-systemen, -netwerken of -middelen. Ook de fysieke beveiliging van ruimten met gevoelige IT-infrastructuur of vertrouwelijke informatie valt hieronder.

4. **Logisch toegangsbeheer**

   Aandacht voor de toegangsbeveiliging van computers en applicaties verkleint het risico op onrechtmatige toegang tot informatie. Niet alle informatie is even vertrouwelijk. Elke soort informatie kan een gepaste bescherming krijgen door de gegevens volgens hun gevoeligheid op te delen in klassen.

5. **Continuïteit**

   Weloverwogen en uitgeteste continuïteitsmaatregelen helpen de onderbreking van de dienstverlening wegens calamiteiten te beperken.

6. **Incidentenbeheer**

   Informatiebeveiligingsincidenten identificeren, classificeren, behandelen en beoordelen helpt om herhaling van deze incidenten te voorkomen of de impact ervan te begrenzen.

Per domein van het controleprogramma is onderzocht in welke mate de geauditeerde organisaties de belangrijkste risico's beheersen. De inschatting gebeurde op basis van interviews, documentanalyse en een vijftal technische testen[5]. Om na te gaan in welke mate besturen de gesignaleerde verbeterpunten remediëren, zijn een aantal technische testen na een redelijke termijn gedeeltelijk opnieuw uitgevoerd.

Audit Vlaanderen kende aan elk bestuur en per domein uiteindelijk een maturiteit toe met een bijhorende kleur (zie legende p. 8-9). De figuur op pagina 8 geeft het gemiddelde van elk domein voor de 28 geauditeerde organisaties weer (waarbij elke audit als 1 inschatting werd geteld, ongeacht de betrokken besturen). De (geanonimiseerde) resultaten per bestuur zijn terug te vinden in bijlage 2.

[5] Deze testen omvatten:
1. Een beperkt nazicht van de toegangs- en gebruikersrechten bij enkele geselecteerde systemen.
2. Een analyse van de netwerkarchitectuur.
3. Een inventarisatie van de aanwezige draadloze netwerken en de beveiliging daarvan.
4. Een scan op verdacht in- en uitgaand netwerkverkeer.
5. Een kwetsbaarheidsscan en manueel bevestigde penetratietesten.
Deze testen werden uitgevoerd in samenwerking met externe experten die Audit Vlaanderen inhuurde via raamovereenkomst Audit Vlaanderen 2015-02 .

Telkens werd naast de inschatting van de maturiteit van de 16 deelaspecten van informatiebeveiliging in een 17de aspect ook nagegaan in welke de mate het bestuur voldeed aan de decretale vereisten omtrent de ruimere organisatiebeheersing.

Dit rapport bundelt de bevindingen voor de zes domeinen in een aantal vaststellingen (vanaf p. 16) en een aantal mogelijke acties richting verbetering (p. 32 en volgende).

AUDITREIKWIJDTE

Audit Vlaanderen auditeerde 27 OCMW's en/of[6] gemeenten en één provincie rond informatiebeveiliging (zie bijlage 1).

Daarnaast organiseerde Audit Vlaanderen in maart 2017 ook een phishing-test[7]. Alle gemeenten, OCMW's en provinciebesturen van Vlaanderen werden uitgenodigd om kosteloos aan deze test deel te nemen. Uiteindelijk participeerden 221 gemeenten en 197 OCMW's. Dat stemt overeen met 72% van de gemeenten en 64% van de OCMW's. Ook de 5 Vlaamse provinciebesturen deden mee. Audit Vlaanderen stuurde naar de 40.612 ingeschreven e-mailadressen twee phishing-mails. Een derde phishing-mail richtte zich enkel tot de secretarissen van de deelnemende besturen. De resultaten van de phishing-test bij de Vlaamse lokale besturen zijn opgenomen in bijlage 3.

[6] Wanneer gemeente en OCMW een secretaris deelden én de IT-functie gezamenlijk was opgezet, werden gemeente én OCMW geauditeerd.

[7] Met een phishing-mail trachten computercriminelen op listige wijze aan persoonlijke informatie of bankgegevens te komen of de computers van hun doelwit te besmetten met kwaadaardige software (zoals een virus, ransomware of keylogger).

1

DE BELANGRIJKSTE ONBEHEERSTE RISICO'S VOOR INFORMATIEBEVEILIGING

Dit hoofdstuk bundelt de belangrijkste risico's en vaststellingen van de thema-audit. Deze gaan over:

1.1 DUIDELIJKE AFSPRAKEN MAKEN EN VERANTWOORDELIJKHEDEN TOEWIJZEN

REFERENTIEKADER

Goede afspraken met de interne en externe betrokkenen van gemeenten en OCMW's zijn essentieel voor een sterke informatiebeveiliging. Daarom is het belangrijk dat elk bestuur:

- duidelijke rollen en verantwoordelijkheden vastlegt voor sleutelactoren zoals het management, de informatieveiligheidsconsulent, de IT-dienst, de software- en IT-dienstenleveranciers en de eventuele informatieveiligheidscel, alsook voor de rest van de organisatie;
- de voorwaarden vastlegt voor de verwerking, opslag en communicatie van informatie door derden;
- de door derden geleverde dienstverlening opvolgt en deze partijen aanspreekt bij problemen of incidenten;
- regelmatig de naleving van interne afspraken en wettelijke vereisten beoordeelt.

BELANGRIJKSTE VASTSTELLINGEN

De lokale besturen vullen de rollen en verantwoordelijkheden op het gebied van informatiebeveiliging onvoldoende concreet in. Daardoor bestaat het risico dat taken niet, onvolledig of dubbel opgenomen worden.

De verwachtingen tegenover de IT-verantwoordelijken zijn onrealistisch. Bij veel organisaties leeft de ijdele hoop dat ze door de aanstelling van één of meerdere IT-verantwoordelijken het hoofd bieden aan het gros van de uitdagingen rond informatiebeveiliging. In de praktijk blijkt dat de IT-verantwoordelijken vaak nauwelijks alle vereiste expertises kunnen bolwerken voor (alle aspecten van) het operationele IT-beheer van de organisatie. Daardoor rest er dikwijls weinig ruimte om het informatiebeveiligingsbeleid te vertalen naar de IT-werking. Acties die op detectie en preventie gericht zijn, raken daardoor meestal op het achterplan. Soms worden nuttige maatregelen niet voorzien omdat de betrokken IT-verantwoordelijken de nodige expertise en tijd missen, hetzij om het belang ervan correct af te wegen tegen de vereiste inspanning, hetzij om de maatregelen op gepast wijze te realiseren en te onderhouden.

Het personeel, de tijd en de middelen die de lokale besturen inzetten voor IT verschillen aanzienlijk. Grosso modo doen zich de volgende situaties voor:

- De organisatie stelt voor het IT-beheer een Chinese vrijwilliger aan.
- Het lokaal bestuur heeft geen eigen IT-verantwoordelijke maar huurt een externe IT-beheerder in.
- Het bestuur stelt één, soms deeltijdse, IT-verantwoordelijke tewerk.
- Het lokaal bestuur beschikt over een IT-dienst met meerdere IT-verantwoordelijken.

Lokale besturen bewandelen verschillende paden om hun capaciteitsbeperkingen te verhelpen en interne IT-expertise te versterken:

- uitwisseling van ervaringen en kennis via beroepsorganisaties;
- instappen in kostendelende modellen of verenigingen;
- een beroep doen op IT-dienstenleveranciers via outsourcing.

Software- en IT-dienstenleveranciers krijgen te veel carte blanche. Alle lokale besturen maken in mindere of meerdere mate gebruik van externe software- en IT-dienstenleveranciers. De meeste besturen halen hiermee specialistische expertise in huis die ze zelf onvoldoende voorhanden hebben. Ook de ontwikkeling van nieuwe systemen of functionaliteiten en de bijsturing van de bestaande systemen wordt bij de geauditeerde besturen systematisch aan deze firma's overgelaten. [Noot: Berichten in de media bevestigen dat verschillende centrumsteden wel betrokken zijn bij de ontwikkeling van specifieke oplossingen, maar deze werden niet geauditeerd in het kader van deze thema-audit.]

Besturen vertrouwen op deze leveranciers voor de verwerking, opslag en/of communicatie van al dan niet vertrouwelijke en/of (persoons)gevoelige gegevens. Toch werden met deze leveranciers weinig afspraken gemaakt over verantwoordelijkheden, rollen/taakverdelingen en de verwachte invulling daarvan.
Veel van de geauditeerde besturen hebben niet de nodige expertise in huis om te weten hoe ze deze externe inhuring moeten aanpakken en welke vereisten ze daarbij moeten formuleren. Ook het toezicht op de naleving van het informatiebeveiligingsbeleid en op de naleving van eventuele afspraken over informatiebeveiliging of de ruimere werking, laat vaak te wensen over.

Sinds 25 mei 2018 wordt bij het maken van afspraken over verantwoordelijkheden over vertrouwelijke en/of (persoons)gevoelige gegevens al snel gedacht aan verwerkingsovereenkomsten. Tijdens deze thema-audit, die liep in de periode tussen de goedkeuring van de algemene verordening gegevensbescherming (AVG) en de volledige afdwingbaarheid ervan, was nog maar een beperkt deel van de geauditeerde besturen begonnen met het voorbereiden of afsluiten van verwerkingsovereenkomsten met leveranciers. Het is voor individuele besturen ook niet evident om de tekst van dergelijke verwerkingsovereenkomst vast te leggen of om leveranciers bereid te vinden dergelijke teksten te ondertekenen. Langs de kant van de leveranciers is het evenmin evident om met alle klanten individuele verwerkingsovereenkomsten af te sluiten. Overkoepelende samenwerking en sectoroverleg kunnen deze situatie faciliteren. De Vereniging van Vlaamse Steden en Gemeenten (VVSG) werkte op basis van het model van de juridische werkgroep GDPR/AVG van de Vlaamse overheid een model van verwerkingsovereenkomst voor alle lokale besturen uit en besprak dit met diverse software en IT-dienstenleveranciers van de lokale besturen. VVSG verspreidde dit model op 2 september onder de Vlaamse lokale besturen. Als via dergelijke initiatieven geen oplossing kan worden gevonden, kan eventueel worden gedacht aan sectorafspraken en/of certificeringen onder toezicht van de gegevensbeschermingsautoriteiten en/of de Europese Commissie (een optie die expliciet mogelijk is gemaakt in de AVG). Bij dit alles mogen de verantwoordelijkheden voor vertrouwelijke gegevens die geen persoonsgegevens zijn niet uit het oog verloren worden.

Al te vaak blijkt de aanwezigheid van kwetsbaarheden binnen de IT-omgeving van een bestuur het gevolg te zijn van onvoldoende afspraken tussen de betrokken partijen. Vaak veronderstellen bestuur en leverancier dat de andere partij bepaalde taken opneemt, waardoor die taken uiteindelijk (bijvoorbeeld het doorvoeren van kritische beveiligingsupdates) niet of niet tijdig worden uitgevoerd. Naast afspraken over algemene verantwoordelijkheden zijn dan ook concrete afspraken over taakverdelingen nodig. Zo moet bijvoorbeeld voor elk IT-systeem duidelijk zijn:

- wie instaat voor het toepassen van updates;
- bij wie incidenten moeten worden gemeld;
- wie instaat voor de onmiddellijke probleemoplossing;
- wie instaat voor de nazorg van de afgehandelde incidenten (o.a. de periodieke evaluatie om te leren uit incidenten).

Naast toepassingen en besturingssystemen mogen hierbij ook de ondersteunende systemen niet vergeten worden.
Om dergelijke afspraken gemakkelijk opvolgbaar te maken, kan het nuttig zijn ze te integreren in netwerkschema's, inventarissen en/of verwerkingsregisters.

Na de toewijzing van verantwoordelijkheden en de verdeling van alle noodzakelijke taken, is het ook belangrijk de verwachtingen van het bestuur - met andere woorden de risicoappetijt - te concretiseren. Ook wanneer bijvoorbeeld de verantwoordelijkheid voor het uitvoeren van updates op een specifiek centraal systeem concreet is toegewezen, kunnen verschillende partijen nog een ander idee hebben over de invulling van die taak. De persoon die de taak moet uitvoeren zal het makkelijk vinden daarvoor een vaste periodiciteit te voorzien, zeker wanneer het nodig is om fysiek ter plaatse te gaan. In de praktijk komt dat bij verschillende besturen neer op het één keer per kwartaal doorvoeren van updates.

Dergelijke frequenties staan vaak ook los van de frequentie waarmee de fabrikant (bv. Microsoft, Oracle, Drupal, …) updates beschikbaar stelt. Deze aanpak maakt ook geen onderscheid tussen kritische beveiligingsupdates en andere aanpassingen. Voor het bestuur betekent dit dat de systemen in de tussenperiode een gekende kwetsbaarheid kunnen bevatten, een risico waaraan het bestuur zich misschien niet verwacht.

Bovenvermelde aandachtspunten voor de samenwerking tussen besturen en leveranciers hebben er in deze thema-audit toe geleid dat alle geauditeerde besturen een aanbeveling hebben gekregen voor het verbeteren van hun leveranciersrelaties. Zo o.a.

Om de risico's die verbonden zijn aan de verwerking, opslag of communicatie van informatie door externe software- en IT-dienstenleveranciers te beperken, is het belangrijk dat de organisatie:

- **De informatiebeveiligingsvereisten bepaalt in overeenstemming met de toegang die de leveranciers hebben tot de IT-systemen en de informatie daarin;**
- **Duidelijk afspreekt wie waarvoor verantwoordelijkheid opneemt, hoe die verantwoordelijkheid minimaal moet worden ingevuld (bv. SLA's, verwerkingsovereenkomst, updatebeheer, incidentbeheer, …) en hoe daarover moet gerapporteerd worden;**
- **Toeziet op de naleving van deze informatiebeveiligingsvereisten en afspraken door de leveranciers.**

De meeste besturen gaven hierbij aan deze aanbeveling moeilijk te kunnen invullen als individueel bestuur.

Alle betrokken partijen kampen met een aantal overkoepelende uitdagingen. Audit Vlaanderen stelde bij alle geauditeerde besturen kwetsbaarheden vast die risico's inhouden voor de informatiebeveiliging. Het blijkt zowel voor de lokale besturen als voor hun software- en IT-dienstenleveranciers moeilijk om alle uitdagingen rond informatiebeveiliging autonoom aan te pakken. Daarom kan het zinvol zijn om met de verschillende actoren samen acties te ondernemen. Sommige activiteiten lenen zich bij uitstek tot een overkoepelende aanpak:

- de vertaling van de juridische vereisten naar de dagelijkse praktijk;
- de opmaak van procedures, werkdocumenten en sjablonen;
- de bepaling van normerende richtsnoeren voor het ontwerp en onderhoud van veilige software;
- de installatie van een generiek communicatiekanaal om kwetsbaarheden aan de lokale besturen te signaleren.

Audit Vlaanderen laat in het midden welke samenwerkingsverbanden of bestuursniveaus hiertoe het beste geschikt zijn.

De dienstverlening van de informatieveiligheidsconsulenten varieert sterk. Uit de audits blijkt dat alle geauditeerde besturen minstens op papier een informatieveiligheidsconsulent hebben. Driekwart van de besturen doet daarvoor een beroep op externe ondersteuning. Er zijn grote verschillen in de samenwerking met en de dienstverlening van de informatieveiligheidsconsulenten. Verschillende oorzaken dragen daartoe bij:

- Niet alle lokale besturen weten wat ze van hun informatieveiligheidsconsulent mogen verwachten. Dit bemoeilijkt de opvolging en de bijsturing van de werkzaamheden. Een enkele keer blijkt een informatieveiligheidsconsulent zelfs te factureren zonder dat daar diensten tegenover staan.
- Veel organisaties die informatieveiligheidsconsulenten leveren aan lokale besturen zijn overbevraagd. Ze trachten meerdere besturen tegelijk te helpen, zodat hun tijdsbesteding per individueel bestuur vaak (te) beperkt is. Dat leidt vaak tot een verminderde betrokkenheid bij hun klanten en het verlies van maatwerk.
- De lokale besturen betrekken hun informatieveiligheidsconsulent niet consequent bij initiatieven die een impact hebben op de informatiebeveiliging. De veiligheidscel waar de informatieveiligheidsconsulent deel van uitmaakt, komt bij meer dan een derde van de lokale besturen hoogstens jaarlijks samen.

De medewerkers en mandatarissen bepalen deels zelf wat (on)veilig gedrag is. In het arbeidsreglement of de deontologische code informeren de lokale besturen hun werknemers over (enkele van) hun verantwoordelijkheden rond informatiebeveiliging. Deze documenten worden echter zelden echt geduid. Stagiairs, mandatarissen en leveranciers ontvangen bij het leeuwendeel van de besturen geen richtlijnen. Ook de sensibilisering van medewerkers om het bewustzijn rond informatiebeveiliging levend te houden en hen (bij herhaling) te wijzen op specifieke risico's wordt in meer dan de helft van de geauditeerde besturen niet structureel aangepakt. Naast eigen incidenten en persaandacht voor incidenten elders blijkt ook het einde van de inwerkingtredingsperiode van de AVG een goede aanleiding om ad-hoc-infosessies te organiseren.

In de volgende besturen zijn goede praktijken omtrent afspraken en verantwoordelijkheden vastgesteld:	
De diverse rollen en verantwoordelijkheden rond informatiebeveiliging concreet uitschrijven en expliciet toewijzen.	Gemeente Wevelgem
Systematisch de geplande acties in het kader van de informatiebeveiliging opvolgen.	Gemeente en OCMW Balen
De medewerkers motiveren om veilig om te gaan met de IT-middelen door de potentiële risico's te duiden in een gedragscode.	OCMW Lokeren
Gebruiksvriendelijk documenteren en ontsluiten van de taakverdeling en -inhoud van de IT-dienst.	Gemeente Schoten
De medewerkers en raadsleden sensibiliseren voor informatiebeveiliging via opleiding en training.	OCMW Kalmthout
Personeelsleden bewust maken van hun verantwoordelijkheden rond informatiebeveiliging via een gedragscode met concrete instructies.	Gemeente en OCMW Erpe-Mere

1.2 DE TECHNISCHE BEVEILIGING VAN DE IT-OMGEVING VERSTERKEN

REFERENTIEKADER

Een goed technisch beheer schermt de IT-omgeving af tegen computercriminelen. Het helpt om de schade bij incidenten te beperken. Technische beveiliging betekent onder meer:

- maatregelen om een veilige IT-omgeving te bouwen en te onderhouden;
- versleuteling van gegevens om vertrouwelijke informatie af te schermen voor onbevoegden;
- netwerkbeveiliging en -scheiding om incidenten te voorkomen en de impact ervan te beperken.

BELANGRIJKSTE VASTSTELLINGEN

De technische beveiliging van de IT-omgeving is ontoereikend. De lokale besturen lopen aanzienlijke veiligheidsrisico's. Bij alle geauditeerde besturen kunnen malafide personen aanzienlijke schade aanrichten door technische kwetsbaarheden te misbruiken.

Er is werk aan de winkel om de technische beveiliging van de IT-omgeving op te krikken. Bijna alle organisaties nemen initiatieven om de servers en de gebruikerstoestellen te beschermen tegen malware en om het interne netwerk te beveiligen tegen externe aanvallen. Deze beveiligingsmaatregelen zijn echter het elementaire minimum. Veel potentiële beschermingsmaatregelen blijven onderbenut. De lokale besturen missen de expertise om zelf een meer sluitende technische beveiliging te implementeren en geven op dit vlak geen prioriteit aan externe ondersteuning.

Bij de geauditeerde besturen testte Audit Vlaanderen in samenwerking met extern ingehuurde experten welke impact iemand met kwade bedoelingen kan hebben. Daarbij werd voornamelijk de situatie gesimuleerd waarbij dergelijk persoon reeds toegang had tot het interne netwerk van het bestuur. Dergelijke toegang kan worden bekomen door fysiek bij het bestuur langs te gaan, via social engineering of door het overnemen van een systeem van het bestuur na besmetting ervan.

Bij 22 van de 28 besturen bleek het mogelijk controle te krijgen over de volledige IT-omgeving. Bij 2 andere besturen kregen de ethical hackers controle over een belangrijk deel van de IT-omgeving. Dergelijke controle laat toe de werking stil te leggen, kennis te nemen van gegevens en deze te manipuleren.

De betrokken IT-verantwoordelijken kregen telkens informatie over de openstaande deuren die ze moesten sluiten. Waar relevant, mogelijk ook voor gelijkaardige situaties bij andere klanten, werden ook de leveranciers ingelicht. Besturen en hun leveranciers leverden vervolgens inspanningen om deze kwetsbaarheden te beheersen.

Toch tonen opvolgtests aan dat een belangrijk deel van de gesignaleerde deuren verschillende maanden later nog steeds openstaat.

De besturen actualiseren hun systeemsoftware onvoldoende. De meeste lokale besturen werken besturingssystemen en ondersteunende systemen van centrale IT-infrastructuur onvoldoende bij met kritische beveiligingsupdates. Herhaaldelijk bleken bestuur en leveranciers te verwachten dat de andere partij dit wel zou doen. Meermaals was het interval waarmee updates werden uitgevoerd te groot. Enkele keren bleken oudere systemen reeds een hele tijd niet meer bijgewerkt te zijn.

Ook bleken sommige besturen voor hun servers nog gebruik te maken van een verouderd besturingssysteem, zelfs nadat deze door een IT-leverancier gemigreerd waren naar nieuwe hardware. Door verouderde besturingssystemen te blijven gebruiken en kritische beveiligingsupdates niet door te voeren, blijven gekende kwetsbaarheden bestaan waarvan personen met malafide bedoelingen misbruik kunnen maken.

Volledigheidshalve wijzen we er op dat in het kader van deze thema-audit geen evaluatie werd uitgevoerd van de wijze waarop bedrijfstoepassingen geüpgraded worden.

De besturen zetten te weinig in op het gebruik van sterke wachtwoorden. Goede wachtwoorden zijn voldoende lang en complex. Ze wijzigen idealiter periodiek. Hoewel ongeveer twee derde van de geauditeerde organisaties een sterk wachtwoordenbeleid hanteert, bleken slechts 6 besturen voor alle geteste gebruikersprofielen een voldoende sterk wachtwoord te hebben. In de 22 andere besturen gebruiken een aantal medewerkers, IT-systemen en/of leveranciers zeer eenvoudige of voorspelbare wachtwoorden. Eén leverancier blijkt voor het opzetten van sommige systemen bij verschillende besturen een wachtwoord te gebruiken dat slechts beperkt – en voorspelbaar – verschilt.

De besturen zijn zich te weinig bewust van de mogelijkheden tot versleuteling. Versleuteling verhindert net zoals wachtwoorden dat onbevoegden kennis nemen van gevoelige informatie. Dit is nuttig voor draagbare toestellen zoals laptops of usb-sleutels met gevoelige gegevens. Bij verlies van draagbare toestellen kan versleuteling veel problemen voorkomen. Lokale besturen maken er echter zelden gebruik van. Versleuteling is ook een must wanneer gevoelige gegevens zoals wachtwoorden worden verstuurd over een computernetwerk. Uit de technische testen blijkt dat de lokale besturen deze verbindingen wel versleutelen. Ze hanteren daarbij echter vaak verouderde en dus onveilige versleutelingsmethodes.

Netwerksegmentatie is onbekend en onbemind. De lokale besturen schermen de verschillende delen van hun interne netwerk onvoldoende af. Wanneer het interne netwerk al opgedeeld is in netwerksegmenten, is de opdeling meestal te weinig risicogericht en zijn er vaak (bijna) geen beperkingen op de communicatie tussen netwerksegmenten. Van de mogelijke opdelingen is vooral de opdeling tussen eindgebruikersapparatuur en de servers een belangrijk element voor het beperken van de risico's. Daarbij moeten leveranciers aangeven welke ip-adressen, protocols en poorten toegankelijk moeten zijn voor eindgebruikers en beheerders.

Zonder een afdoende segmentering van het netwerk kan een besmetting – bijvoorbeeld met kwaadaardige software zoals bijvoorbeeld Wannacry ransomware (zie bijlage 4) – op één systeem zich vlot verspreiden naar alle andere systemen. Een ongeautoriseerde gebruiker die zichzelf toegang verschaft tot het interne netwerk – al dan niet door een eindgebruikerscomputer over te nemen of door zich aan te melden met gebruikersgegevens van een willekeurige eindgebruiker – kan in dat geval meteen alle netwerk- en systeembeheerinterfaces aanvallen.

Voor technologie die de sterkte van de informatiebeveiliging test, heerst koudwatervrees. Speciale software kan gekende kwetsbaarheden in de IT-omgeving proactief opsporen. Slechts enkele lokale besturen maken hiervan gebruik. Dit is onder meer een gevolg van de beperkte IT-capaciteit en een gebrek aan specialistische kennis. Zo een analyse is nochtans een goede manier om te evalueren of beveiligingsmaatregelen afdoende zijn. Zonder dergelijke periodieke evaluatie, is het voor besturen moeilijk om de gevolgen van de impliciet en expliciet gemaakte keuzes m.b.t. het ICT-gebeuren in beeld te krijgen en te beoordelen.

Audit Vlaanderen huurde voor dergelijke testen in het kader van deze thema-audit specialisten in via de raamovereenkomst "Audit Vlaanderen 2015-02". Ook de lokale besturen kunnen gebruik maken van deze raamovereenkomst.

In de volgende besturen zijn goede praktijken voor technische beveiliging vastgesteld	
Gevoelige informatie op harde schijven en usb-sticks beschermen via versleuteling.	Gemeente Wevelgem
Via versleuteling van documenten gevoelige informatie veilig delen met derden.	Gemeente Niel
Gevoelige informatie op usb-sticks beschermen door het gebruiken van versleutelde USB-sticks.	Gemeente en OCMW Erpe-Mere
Een duidelijk overzicht bijhouden van al het IT-materiaal zodat de IT-dienst de nodige beheerstaken en de gepaste bescherming kan uitvoeren.	Gemeente Niel
Met periodieke kwetsbaarheidsscans proactief de gaten in de beveiliging van IT-systemen en software opsporen.	Provincie West-Vlaanderen

1.3 TOEGANGS- EN GEBRUIKERSRECHTEN OP PUNT ZETTEN EN HOUDEN

REFERENTIEKADER

Een degelijke toegangsbeveiliging is cruciaal om onrechtmatige toegang tot (gevoelige) informatie te voorkomen. De logische toegangs- en gebruikersrechten moeten steeds in overeenstemming zijn met de beleidsregels en met andere beheersmaatregelen zoals functiescheiding. Informatie moet afhankelijk van de gevoeligheid een passende bescherming krijgen. Dat geldt ook voor de bedrijfsmiddelen waarop deze informatie staat. Wanneer gebruikers vertrekken of van functie veranderen, moeten hun toegangs- en gebruikersrechten aangepast worden.

BELANGRIJKSTE VASTSTELLINGEN

Het beheer van de toegangs- en gebruikersrechten verloopt niet optimaal. Zo kunnen onbevoegden (zowel personeelsleden met een andere functie, ex-gebruikers als andere externen) zich soms toegang verschaffen tot vertrouwelijke informatie. De besturen beschermen hun informatie niet in functie van de gevoeligheid. Hierdoor beschikken de medewerkers en mandatarissen vaak over ruimere gebruikersrechten dan wenselijk is vanuit een informatiebeveiligingsoogpunt.

Ex-medewerkers en ex-mandatarissen hebben soms nog toegangsrechten. Een sluitende procedure voor het toewijzen of intrekken van deze rechten ontbreekt meestal. Waar er afspraken over het beheer van de rechten zijn, focussen deze vaak onvoldoende op alle types gebruikers en alle IT-systemen en diensten. Door het ontbreken van zo'n gestandaardiseerde aanpak schiet de organisatie niet of te laat in actie wanneer gebruikers het lokale bestuur verlaten. Slechts een handvol besturen volgt proactief de verleende rechten op en past die periodiek aan. Deze bevinding sluit aan bij de bevindingen uit eerdere thema-audits. Dit probleem blijft met andere woorden de kop op steken.

Verschillende medewerkers hebben ruimere rechten dan noodzakelijk is voor hun functie.

- De toekenning, wijziging en intrekking van rechten wordt uitgevoerd door applicatiebeheerders en IT-verantwoordelijken. Applicatiebeheerders weten vaak zelf onvoldoende hoe het rechtenbeheer van de toepassing die ze beheren functioneert. Informatie over het vertrek van personeelsleden en over wijzigingen van functies stroomt vaak ook te laat of niet door naar alle personen die rechten moeten wijzigen of schrappen.
- Wanneer besturen aan nieuwe gebruikers rechten verlenen, kopiëren ze geregeld een bestaande set gebruikersrechten van een andere medewerker. Ze gaan hierbij niet na of die rechten overeenstemmen met de feitelijke noden van de nieuwe gebruiker. Gemakshalve te ruime gebruikersrechten toekennen, hypothekeert de bescherming van vertrouwelijke en/of (persoons)gevoelige informatie.
- Meermaals bleken gebruikersprofielen die werden aangemaakt op vraag van software- en IT-dienstenleveranciers te ruime toegangs- en gebruikersrechten te hebben. Ook de opslaglocaties waar toepassingen automatisch bestanden opslaan waren meermaals te ruim toegankelijk. Ook hier hypothekeert het gemakshalve te ruim instellen van rechten de bescherming van vertrouwelijke en/of (persoons)gevoelige informatie.
- Meerdere besturen maken nog sporadisch gebruik van gedeelde gebruikersprofielen die niet gekoppeld zijn aan één unieke gebruiker. Hierbij bestaat het risico dat bij misbruik niet te achterhalen valt wie daarvoor verantwoordelijk is. Wanneer na het schrappen van het centrale gebruikersprofiel nog toegangsrechten actief blijven voor specifieke applicaties, kan zo een gedeeld gebruikersprofiel het soms ook mogelijk maken om alsnog de specifieke applicaties te misbruiken.

Besturen beschermen sommige data te veel en andere te weinig. Informatie moet beschermd worden in functie van haar gevoeligheid. Organisaties kunnen ervoor zorgen dat al hun informatie een passend beschermingsniveau krijgt door een classificatie toe te passen en daarna de gepaste beschermingsmaatregelen te voorzien bij de verschillende soorten informatie. Er zijn verschillende types van classificatie mogelijk. Zo onderscheiden de richtsnoeren van de Vlaamse Toezichtscommissie (VTC) en de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL, thans de Gegevensbeschermingsautoriteit) voor gemeenten en OCMW's minstens vier gegevenstypes. Het informatieclassificatiemodel dat recenter werd goedgekeurd door het Stuurorgaan Vlaams Informatie- en ICT-beleid werkt met 5 klassen. Zelfs wanneer besturen al een classificatiemodel hebben aangenomen (bijvoorbeeld door de goedkeuring van een sjabloondocument aangeleverd door de informatieveiligheidsconsulent), blijken zij dit niet voldoende te concretiseren en in de praktijk te brengen. Bij gebrek aan een organisatiebrede aanpak voor de classificatie van gegevens, wordt de inschatting van wat hoe moet worden afgeschermd overgelaten aan de individuele beoordeling van elke betrokkene. In de praktijk leidt dit ertoe dat sommige gegevens te veel en andere te weinig worden afgeschermd.

1.4 CONTINUÏTEIT GARANDEREN EN GEPAST OMGAAN MET INCIDENTEN

REFERENTIEKADER

Bij calamiteiten wordt de gewone werking onderbroken. Vaak is een beperkte onderbreking eerder storend en geen echt probleem. Hoe langer de onderbreking duurt, hoe problematischer dit wordt voor een bestuur en voor diegenen die van dat bestuur afhankelijk zijn (mogelijke gevolgen: imagoschade, extra kosten, technische werkloosheid, ontevreden burgers, enz.). Ook rijst de vraag of alle gegevens nog beschikbaar zijn en of een deel van de gegevens mogelijk verloren is gegaan.

De organisatie treft continuïteitsmaatregelen om de onbeschikbaarheid van tijdskritische diensten en van informatie door een uitval van IT-systemen, huisvesting en/of logistieke ondersteuning te beperken. Dat kan in de vorm van bijvoorbeeld een bedrijfscontinuïteitsstrategie met concrete continuïteitsplannen. Om te verzekeren dat de uitgewerkte maatregelen werken, test de organisatie ze periodiek en stuurt ze bij waar nodig.

Voor een goed begrip van de toegekende maturiteitsinschattingen omtrent het aspect continuïteit moet worden gewezen op volgende bijsturing van het traditionele normenkader hieromtrent: Rekening houdend met de flexibiliteit waarmee besturen veelal reageren op logistieke uitdagingen, werd in het kader van deze thema-audit de maturiteit van de beheersing rond continuïteit reeds ingeschat op niveau 3 wanneer de continuïteit van de centrale IT-systemen kon worden gegarandeerd. Van het volwaardig garanderen van de continuïteit, ook logistiek, is bijgevolg slechts sprake op niveau 4.

Het is logisch dat organisaties occasioneel geconfronteerd worden met informatiebeveiligingsincidenten. Sinds de invoering van de AVG kunnen de gegevensbeschermingsautoriteiten straffen toepassen wanneer belangrijke informatiebeveiligingsincidenten niet voldoende gerapporteerd worden. Door incidenten te registreren en periodiek de geregistreerde incidenten te evalueren, kunnen organisaties bijsturen om incidenten in de toekomst te vermijden of om de impact ervan te verminderen. Alles begint evenwel bij de identificatie van incidenten. Personeelsleden moeten voldoende geïnformeerd en blijvend gesensibiliseerd worden om alle informatiebeveiligingsincidenten te herkennen en te weten hoe/waar ze deze incidenten moeten melden. Wanneer gereageerd wordt op informatiebeveiligingsincidenten moeten de afspraken over de onmiddellijke probleemaanpak voor alle betrokkenen duidelijk zijn. Zij moeten ook weten wanneer en naar wie geëscaleerd of gerapporteerd moet worden.

BELANGRIJKSTE VASTSTELLINGEN

Lokale besturen beschikken meestal wel over een back-up waarop ze na een calamiteit kunnen terugvallen. Doordat ze zich niet voorbereiden, lopen de meeste besturen het risico dat de heropstart na een incident moeizaam verloopt. Dit kan in de nasleep van een calamiteit voor vermijdbare bijkomende problemen zorgen.

Lokale besturen zijn vaak onvoldoende gewapend om snel gepast te reageren op incidenten (bv. een gebruiker of beheerder die doorklikt op een phishingmail, zie bijlage 3). Dit kan bijvoorbeeld in het kader van de AVG tot problemen leiden. Ook leren besturen meestal te weinig uit incidenten om incidenten in de toekomst te vermijden of om de gevolgen ervan te beperken.

De IT-dienst verzekert de basiscontinuïteit maar de besturen vertrouwen er te veel op dat alles na een calamiteit wel goed komt.
Alle geauditeerde besturen treffen technische maatregelen om de beschikbaarheid van de digitale gegevens minstens dagelijks te garanderen. Zij nemen back-ups, de servers zijn meestal beschermd tegen een plotse stroomonderbreking en de kritieke IT-systemen zijn vaak ontdubbeld. Sommige lokale besturen installeerden een generator die de servers bij een langdurige stroomuitval van stroom kan voorzien. De toenemende samenwerking tussen OCMW's en gemeenten biedt vaak opportuniteiten om de kosten van de continuïteitsmaatregelen te drukken. Zo kunnen ze bijvoorbeeld elkaars computerlokaal als uitwijklocatie of back-uplokaal gebruiken.

De lokale besturen rekenen evenwel te veel op een goede afloop bij calamiteiten:
- Hoewel de meeste besturen een back-up nemen, doen maar weinig van hen de moeite om de integriteit en bruikbaarheid daarvan periodiek te testen. Verrassingen zijn dan ook mogelijk op het moment dat de back-ups nodig zijn. Wanneer gebeurlijk individuele bestanden werden teruggehaald uit back-ups, werden daarbij door de geauditeerde besturen evenwel geen problemen vastgesteld.
- Wat - bij onbeschikbaarheid van de primaire serverruimte - in welke volgorde moet gebeuren om terug een werkende ICT-omgeving te creëren, is meestal niet concreet uitgewerkt, laat staan getest. Hoeveel tijd nodig is om de werking te kunnen voortzetten is bijgevolg ook niet duidelijk.
- Slechts één geauditeerd bestuur heeft aan de hand van een bedrijfsimpactanalyse vastgelegd welke processen het meest kritiek zijn en welke processen minder prioritair zijn wanneer er bij het herstellen van de werking keuzes moeten worden gemaakt.
- Over logistieke aspecten van continuïteit is vaak nog niet nagedacht (bv. op welke locatie kunnen loketten worden ingericht, hoe kan in stoelen, tafels en computers worden voorzien, hoe kunnen elektriciteit en netwerkverbindingen worden opgezet en hoe kan nieuwe hardware voor de centrale IT-voorzieningen worden verkregen). Ook crisiscommunicatie en back-upregelingen over kritische functies zijn meestal weinig ingesteld op IT-continuïteit.

Informatiebeveiligingsincidenten blijven onder de radar.
- Doordat de geauditeerde besturen hun personeelsleden nauwelijks houvast bieden voor het identificeren van informatiebeveiligingsincidenten, is het niet voor iedereen binnen die besturen duidelijk wat ze als dusdanig moeten beschouwen. Daardoor worden sommige (niet-IT-)incidenten niet of onvoldoende gesignaleerd.
- De medewerkers melden IT-problemen en dus ook IT-gerelateerde informatiebeveiligingsincidenten doorgaans aan een IT-verantwoordelijke of een helpdesk. Deze staan in voor de onmiddellijke probleemoplossing. Er zijn met hen echter geen afspraken gemaakt over eventuele escalaties. Bijvoorbeeld over de vraag wie ze via welk kanaal bij welke problemen kunnen/moeten informeren?
- Om te leren uit incidenten is het belangrijk om die incidenten te registreren. Meer dan de helft van de geauditeerde besturen heeft geen register van informatiebeveiligingsincidenten. Zelfs waar er wel een register is, worden maar weinig van de incidenten geregistreerd.

De meeste besturen veronderstellen dat technische IT-problemen die een impact hebben op informatiebeveiliging een rariteit zijn. Als er zich een technisch probleem voordoet dat een impact kan hebben op informatiebeveiliging, doen slechts enkele van de geauditeerde besturen de moeite om daarvan een echte analyse te maken. Vaak is de logging ook beperkt tot datgene wat standaard geactiveerd is, wat bij veel systemen maar weinig analyse van informatiebeveiligingsincidenten toelaat. Uit deze thema-audit blijkt dat de geauditeerde besturen:
- de automatische registratie van relevante gebeurtenissen in logbestanden niet altijd activeren;
- hun logbestanden enkel lokaal opslaan, waardoor ze bij zware incidenten mogelijk niet meer raadpleegbaar zijn;
- soms verschillende gebruikers op eenzelfde gebruikersprofiel toelaten, wat de gebruikersidentificatie bij incidenten bemoeilijkt;
- het moeilijk hebben de informatie uit de logbestanden te interpreteren.

In de volgende besturen zijn goede praktijken voor continuïteitsbeheer vastgesteld:	
Een goede aanpak uitwerken voor het nemen en bijhouden van back-ups.	Gemeente en OCMW Erpe-Mere
De ICT-systemen, back-ups en bijhorende infrastructuur ontdubbelen zodat de beschikbaarheid van de dienstverlening is gegarandeerd.	Gemeente en OCMW Lanaken
Een uitwijklocatie ter beschikking houden waar het bestuur de prioritaire dienstverlening kan verderzetten wanneer een gebouw niet meer beschikbaar is.	OCMW Essen
Een bedrijfscontinuïteitsplan ontwikkelen dat de prioritair te zetten stappen beschrijft om de dienstverlening na een calamiteit te herstarten.	OCMW Wemmel

2

KLEINE EN MIDDELGROTE ONBEHEERSTE RISICO'S VOOR INFORMATIEBEVEILIGING

Informatiebeveiliging is een zaak van iedereen en behelst meer dan louter technische elementen. Dit hoofdstuk behandelt de bevindingen over bewustzijn en sensibilisering en over fysieke beveiliging. Deze gaan over:

2.1 BLIJVEN WERKEN AAN HET BEWUSTZIJN EN AAN DE SENSIBILISERING

REFERENTIEKADER

Informatiebeveiliging is sterk afhankelijk van gedrag. Het bewustzijn over informatiebeveiligingsrisico's bij medewerkers, mandatarissen, software- en IT-dienstenleveranciers is daarbij cruciaal. Sensibiliseringsacties kunnen het bewustzijn aanwakkeren. Periodieke controles op de naleving van afspraken dragen hiertoe bij.

BELANGRIJKSTE VASTSTELLINGEN

Hoewel lokale besturen inspanningen leveren om hun personeel te sensibiliseren over informatiebeveiliging, wordt dit meestal weinig planmatig aangepakt. Ook kan nog worden gewerkt aan de vertaling van de algemene principes en risico's naar de dagelijkse praktijk van de verschillende functies. Tot slot kan het bewustzijn over het omgaan met informatiedragers bij veel besturen nog worden verbeterd.

Bij werving en indiensttreding wordt meestal wel aandacht geschonken aan informatiebeveiliging, maar vaak gebeurt dit slechts oppervlakkig. Doordat elementen zoals betrouwbaarheid en discretie in veel functiebeschrijvingen zijn opgenomen, wordt daaraan bij twee derde van de besturen tijdens de werving aandacht geschonken. Mogelijkheden om daar diepgaander naar te polsen, zoals het bespreken van dilemma's of concrete praktijksituaties, worden evenwel weinig gebruikt. Bij indiensttreding worden vaak wel het arbeidsreglement en de deontologische code bezorgd, soms aangevuld met een document over de omgang met ICT-materiaal, maar deze documenten worden niet zo vaak echt doorgepraat en toegelicht.

Bij gebrek aan organisatiebrede ondersteuning, varieert het bewustzijn over informatiebeveiliging vaak per dienst. Waar kaders en ondersteuning op organisatieniveau ontbreken, hangt de aandacht voor informatiebeveiliging vooral af van de persoonlijke aandacht die hieraan gegeven wordt binnen de diensten. In de concrete vertaling van dat bewustzijn naar de praktijk blijkt er geen aantoonbaar verschil te zijn tussen diensten in OCMW's en in gemeenten. Waar diensthoofden hun medewerkers duidelijke richtlijnen meegeven, handelt men bewuster en durft men elkaar makkelijker aan te spreken op niet-conform gedrag.

De concretisering van het bewustzijn naar de omgang met informatiedragers is bij de meeste besturen voor verbetering vatbaar. Hoewel er gebruiksvriendelijke manieren zijn om digitale informatiedragers te beveiligen, gebruikt men deze vaak niet, met alle risico's vandien bij verlies of diefstal. Voor papieren informatiedragers werken veel besturen met eenvoudige maatregelen zoals afsluitbare kasten of lokalen. Toch is men vaak nog te slordig met papieren gegevensdragers. Ook bleek meermaals dat archieven onvoldoende afgeschermd werden.

Omtrent sensibilisering is de volgende goede praktijk vastgesteld:	
Het bewustzijn over de gevaren voor phishing bij de medewerkers actief stimuleren.	Gemeente en OCMW Lanaken

2.2 VERWAARLOOS FYSIEKE BEVEILIGING NIET

REFERENTIEKADER

Een lokaal bestuur heeft veel dossiers met vertrouwelijke informatie. Het is niet de bedoeling dat eender wie die kan inkijken. Het is ook niet wenselijk dat onbevoegden vlot bij de kritieke IT-infrastructuur geraken. Met fysieke beveiligingsmaatregelen kunnen organisaties de ongewenste toegang tot informatie voorkomen.

BELANGRIJKSTE VASTSTELLINGEN

Terwijl sommige geavanceerde beveiligingssystemen op IT-vlak bijna gemeengoed zijn, laten de meeste organisaties kansen liggen om met eenvoudige maatregelen hun fysieke beveiliging aanzienlijk te verbeteren.

De recuperatie van sleutels en badges loopt soms spaak. Besturen weten ook onvoldoende wie deze in handen hebben. De meeste besturen hebben geen sluitend overzicht van wie over een sleutel en/of badge beschikt. Een kleine helft van de besturen hanteert een vaste procedure voor de teruggave van sleutels of badges bij de uitdiensttreding. Dergelijke toegangsmiddelen blijven vaak bij oud-medewerkers omdat er geen verantwoordelijke voor de recuperatie is of omdat die verantwoordelijke niet (tijdig) van de uitdiensttreding verwittigd wordt. Op sommige locaties kunnen oud-medewerkers het systeem voor inbraakdetectie uitschakelen omdat hun codes nog functioneren.

De beveiliging van fysieke documenten is een aandachtspunt. Een cleandesk- of cleardeskbeleid[8] en het effectief afsluiten van kasten en afgeschermde archieven zijn onvoldoende ingeburgerd. Soms wordt er ook van uitgegaan dat dit wringt met de wens om 'een open huis' te zijn. Het is echter niet omdat iedereen welkom is, dat diensten geen beschermingsmaatregelen moeten nemen voor het afschermen van sommige informatie. Bezoekers kunnen vaak het hele bestuursgebouw rondzwerven. Omdat gevoelige papieren dossiers meestal niet standaard in afgesloten kasten opgeborgen worden, is het relatief gemakkelijk om ze in te kijken. Sommige besturen nemen echter beheersmaatregelen om dit te voorkomen, zoals het gebouw in verschillende afgeschermde zones indelen of het archief en de technische ruimtes afschermen.

De helft van de besturen beschermt zijn serverruimte afdoende. De andere helft kan nog bijkomende maatregelen treffen. Zo worden sommige serverruimtes als opslaglocatie van kantoormateriaal gebruikt of kan de brandbeveiliging beter. In enkele gevallen was de serverruimte niet afgeschermd. Nochtans kan schade aan de kritieke IT-infrastructuur lokale besturen veel problemen bezorgen.

De volgende goede praktijken rond fysieke beveiliging is vastgesteld:	
De fysieke toegang tot zones met gevoelige informatie voor onbevoegden verhinderen aan de hand van programmeerbare badges.	Gemeente en OCMW Erpe-Mere

[8] Een 'cleandeskbeleid' is er op gericht dat alles op het bureau wordt opgeruimd en op een veilige plaats wordt bewaard. Volgens een 'cleardeskbeleid' is het niet nodig om zo ver te gaan en is het enkel verboden vertrouwelijke en/of (persoons)gevoelige informatie onbewaakt achter te laten op het bureau.

3

HOE BESTUREN KUNNEN WERKEN AAN INFORMATIEBEVEILIGING

Audit Vlaanderen formuleert op basis van de structurele vaststellingen een aantal mogelijke acties richting verbetering. Hierbij is het niet onze intentie om ons uit te spreken over wie precies welke actie moet ondernemen.

Mogelijke actie 1: Kies bewust voor de gewenste IT- en informatiebeveiligingsgaranties

Mogelijke actie 2: Zet als bestuur samen met je software- en IT-dienstenleverancier de puntjes op de i

Mogelijke actie 3: Meer samenwerking tussen besturen

Mogelijke actie 4: Meer samenwerking met alle actoren

3.1 MOGELIJKE ACTIE 1: KIES BEWUST VOOR DE GEWENSTE IT EN INFORMATIEBEVEILIGINGSGARANTIES

Organiseer IT in overeenstemming met de behoeften en de doelstellingen van de organisatie, ook deze op het vlak van informatiebeveiliging.

Structurele vaststellingen

Het takenpakket van een IT-functie bij de lokale besturen is omvangrijk, divers en vergt veel specialistische expertise. Het personeel, de tijd en de middelen die de besturen daarvoor inzetten verschillen aanzienlijk. Alle lokale besturen doen een beroep op externe software- en IT-dienstenleveranciers, vaak maar niet altijd aangevuld met één of meer interne IT-verantwoordelijken. De praktische organisatie van de IT-functie bepaalt de mate waarin de IT-dienst tegemoet kan komen aan de verwachting van de organisatie, onder meer rond informatiebeveiliging. Die concrete invulling van de IT-functie gebeurt nog te veel in functie van de praktische noden en de historisch gegroeide invulling.

Mogelijke piste

De lokale besturen moeten bepalen hoe ze hun IT-functie concreet gestalte willen geven. Voor de invulling van hun noden en verwachtingen moeten ze weloverwogen keuzes maken over de wijze waarop ze de IT-diensten en -producten verwerven, over het opzetten van het IT-beheer en -beleid en over het samensmeden van dat alles tot een goed beheerde IT-omgeving. Besturen moeten met andere woorden een sourcingstrategie vastleggen gekoppeld aan een IT-beleid en -budget in functie van de organisatie en de maatschappij. Keuzes die hierbij aan bod kunnen komen zijn:

- de ontwikkeling van een eigen dan wel uitbestede IT-dienst;
- de inschakeling en de opvolging van externe software- en IT-dienstenleveranciers;
- het instappen in kostendelende modellen of verenigingen;
- de bij aankopen te hanteren vragenlijsten en evaluatiecriteria;
- het zelf opzetten of het afnemen van anderen van contracten, applicaties, infrastructuur, helpdeskfuncties, monitoring en managementprocessen;
- de afstemming tussen de IT-verwachtingen en de IT-uitgaven.

Een weloverwogen sourcingsstrategie vermindert het risico dat de IT-dienst onvoldoende tegemoet komt aan de behoeften en doelstellingen van de organisatie, ook deze op het vlak van informatiebeveiliging.

3.2 MOGELIJKE ACTIE 2: ZET ALS BESTUUR SAMEN MET JE SOFTWARE- EN IT-DIENSTENLEVERANCIERS DE PUNTJES OP DE i

Leg de taakverdeling voor het IT-beheer en de verwachte invulling daarvan eenduidig vast tussen het lokale bestuur en zijn leveranciers.

Structurele vaststellingen

Vele externe software- en IT-dienstenleveranciers ondersteunen de lokale besturen voor de verwerking, de opslag en de communicatie van informatie en gegevens. De aard van die samenwerkingen en de geleverde producten en diensten is zeer divers.

Slechts een minderheid van de geauditeerde besturen maakte echter duidelijke afspraken met zijn externe leveranciers over wie welke taken dient uit te voeren en hoe deze minimaal ingevuld moeten worden. De besturen zien ook zelden toe op de door deze leveranciers geleverde dienstverlening.

Veel van de vastgestelde problemen op het vlak van informatiebeveiliging kunnen met gezonde reflexen en een goede discipline in grote mate worden vermeden. In het samenspel tussen besturen en externe leveranciers is het daarbij belangrijk dat deze elementen gezamenlijk worden opgenomen onder een sluitende coördinatie.
De door Audit Vlaanderen uitgevoerde technische testen tonen bijvoorbeeld aan dat bij bijna alle geauditeerde besturen verouderde of niet langer ondersteunde systeemsoftware gebruiken. De vage toewijzing van de verantwoordelijkheden voor de bijwerking van deze systeemsoftware draagt daartoe bij.

De externe software- en IT-dienstenleveranciers hebben omwille van hun werkzaamheden vaak toegang tot heel wat gevoelige of vertrouwelijke gegevens. Het is onduidelijk in hoeverre deze leveranciers de beschikbaarheid, de integriteit en de vertrouwelijkheid van die gegevens garanderen. De informatiebeveiligingsvereisten waaraan de externe leveranciers moeten voldoen zijn zelden geconcretiseerd.

De relatief grote afhankelijkheid van externe leveranciers, het ontbreken van een eenduidig vastgelegde taakverdeling en verwachte invulling daarvan, de weinig concrete informatiebeveiligingsvereisten en het gebrek aan monitoring van de door de leveranciers geleverde dienstverlening, brengt risico's mee voor de bescherming van gevoelige informatie(systemen).

Mogelijke piste

De lokale besturen en hun externe software- en IT-dienstenleveranciers brengen voor het respectieve bestuur in onderling overleg eenduidig in kaart wie voor het IT-beheer precies welke taken opneemt en welke verwachtingen daarbij minimaal moeten worden ingevuld.

Daarbij gaat aandacht uit naar het:
- tijdig bijwerken van zowel besturingssystemen, toepassingen als ondersteunende IT-systemen;
- sluitend beheren van toegangen en rechten;
- gebruiken en afdwingen van sterke wachtwoorden voor alle gebruikers;
- gepast omgaan met versleutelingsmechanismen;
- doordacht segmenteren of opvolgen van het netwerk van het bestuur zodat achterliggende systemen minder kwetsbaar zijn voor infecties op eindgebruikersapparatuur;
- periodiek testen van de continuïteitsmaatregelen;
- communiceren, registreren, behandelen en rapporteren van incidenten;
- opvolgen van de kwetsbaarheden en van de levenscyclus van hard- en software.

Duidelijke afspraken tussen individuele lokale besturen en hun externe software- en IT-dienstenleveranciers verkleinen het risico dat informatiebeveiligingsrisico's niet, onvolledig of dubbel worden afgedekt.

De hier beoogde afspraken over taakverdeling en minimale invulling moeten per bestuur worden afgesproken, afgestemd op de eigen verwachtingen en de concrete situatie van het specifieke bestuur. Eventueel kan wel gezamenlijk werk worden gemaakt van sjablonen, handleidingen en eventueel zelfs basisrichtlijnen of het maken van deze afspraken te faciliteren en om te vermijden dat belangrijke afspraken over het hoofd worden gezien. Deze afspraken mogen niet worden verward met de in het kader van de Algemene Verordening Gegevensbescherming vereiste verwerkingsovereenkomsten.

3.3 MOGELIJKE ACTIE 3: MEER SAMENWERKING TUSSEN BESTUREN

Vertaal de relevante regelgeving naar vlot inzetbare oplossingen met duidelijke voorwaarden, instructies en garanties.

Structurele vaststellingen

Elk lokaal bestuur moet zijn informatiebeveiliging te garanderen.
Voor een individueel bestuur is het vaak niet mogelijk om alle vereiste expertises zelf in huis te hebben. In de praktijk is elk bestuur sterk in sommige expertises en vormen andere expertises vaak de zwakke plekken.
Bovendien moeten besturen momenteel al te vaak het warm water opnieuw uitvinden. Zo brengen veel organisaties momenteel de maatregelen in kaart in het kader van de AVG. Veel besturen werken daarvoor op eigen houtje aan modellen voor de opmaak van een verwerkingsovereenkomst, een register van verwerkingsactiviteiten of een gegevensbeschermingseffectbeoordeling. Zo'n vertaalslag van regelgeving naar praktische acties is echter geen sinecure.

Mogelijke piste

Organiseer samenwerking en kennisdeling tussen lokale besturen om alle vereiste expertises toegankelijk te maken en parallelle inspanningen te vermijden.

Deel kennis en expertise om gezamenlijk op een haalbare wijze op alle gebieden voldoende gewapend te zijn.

Bekijk samen de gezamenlijke uitdagingen en verspreidt de kennis die daar uit voortvloeit zodat elk bestuur de nodige informatie heeft om onderbouwde keuzes te kunnen maken.

Werk gezamenlijk vlot inzetbare oplossingen uit zodat niet elk lokaal bestuur het warm water uitvindt.

Dit laat de lokale besturen toe op een effectieve en efficiënte wijze zowel individueel als gezamenlijk de gewenste informatiebeveiliging te garanderen.

3.4 MOGELIJKE ACTIE 4: MEER SAMENWERKING MET ALLE ACTOREN

Breng een sectoroverleg tot stand voor informatiebeveiliging bij lokale besturen.

Structurele vaststellingen

Verschillende factoren bemoeilijken de bescherming van de vertrouwelijke informatie waarmee de lokale besturen werken, zoals:
- de toenemende digitalisering en de daarmee gepaard gaande kwetsbaarheden;
- de beperkte capaciteit en IT-expertise binnen de lokale besturen;
- het gebrek aan duidelijke rollen en verantwoordelijkheden rond informatiebeveiliging;
- de wijzigende regelgeving;
- het diverse landschap van toezichthoudende instanties.

Diverse actoren leveren inspanningen om die uitdagingen het hoofd te bieden. Verscheidene overheidsinstanties werken, vaak in gespreide slagorde, aan informatiebeveiliging binnen de lokale besturen. Denk onder meer aan:
- het Centrum voor Cybersecurity België (CCB) van de federale overheid;
- de Programmatorische Overheidsdienst Maatschappelijke Integratie (POD MI);
- de Gegevensbeschermingsautoriteit, voorheen de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) of de Privacycommissie;
- de Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer (VTC);
- de werkgroep Informatieveiligheid van het stuurorgaan Vlaams Informatie- en ICT-beleid.

De lokale besturen doen zelf aan kennisdeling over informatiebeveiliging in enkele fora zoals:
- de werkgroep informatieveiligheid voor informatieveiligheidsconsulenten van de Vereniging van Vlaamse Steden en Gemeenten (VVSG);
- de kenniskringen van de Vlaamse ICT Organisatie (V-ICT-OR);
- INFOLOK, een LinkedIn-groep over informatieveiligheid in lokale besturen.

Daarnaast bieden veel commerciële en non-profitorganisaties de lokale besturen ondersteuning en diensten op het vlak van informatiebeveiliging.

Geen enkele betrokkene is echter in staat alle risico's voor informatiebeveiliging autonoom aan te pakken. Daarom is het zinvol om met verschillende actoren samen acties te ondernemen.

Mogelijke piste

Organiseer een sectoroverleg voor informatiebeveiliging bij de lokale besturen om met alle betrokken partijen samen de overkoepelende uitdagingen het hoofd te bieden.

Een sectoroverleg voor informatiebeveiliging bij de lokale besturen kan oplossingen bieden voor problematieken die in gespreide slagorde moeilijk effectief en efficiënt op te lossen zijn.

BIJLAGE 1: DE GEAUDITEERDE BESTUREN

Deze thema-audit gebeurde bij besturen waar Audit Vlaanderen nog geen audit uitvoerde. De geauditeerde besturen werden geselecteerd op basis van:

- **Een algemene risicoanalyse**

  Audit Vlaanderen stelde een algemene risicoanalyse op met factoren als de relatieve materialiteit (bv. uitgaven per inwoner), de financiële situatie en de kwaliteit van de interne beheersing.

- **De representativiteit van deze thema-audit voor alle lokale besturen**

  Audit Vlaanderen koos bij de selectie voor een maximale spreiding op zes dimensies:
  - het aantal inwoners;
  - de geografische ligging;
  - de aangestelde informatieveiligheidsveiligheidsconsulent;
  - de leverancier van de boekhoudsoftware (softwarepakket gebruikt door zowel OCMW's als gemeenten);
  - de maturiteit van het bestuur volgens de I-monitor[9];
  - het type van lokaal bestuur.

In totaal werden 28 besturen geselecteerd op basis van deze criteria:

Gemeente Assenede	Gemeente & OCMW Wachtebeke
Gemeente Balen	OCMW Alken
Gemeente Herne	OCMW Essen
Gemeente Heusden-Zolder	OCMW Houthulst
Gemeente Niel	OCMW Kalmthout
Gemeente Oud-Turnhout	OCMW Lokeren
Gemeente Wevelgem	OCMW Riemst
Gemeente Zedelgem	OCMW Rotselaar
Gemeente & OCMW Erpe-Mere	OCMW Wellen
Gemeente & OCMW Herenthout	OCMW Wemmel
Gemeente & OCMW Hoegaarden	Provincie West-Vlaanderen
Gemeente & OCMW Hoeilaart	Stad Gistel
Gemeente & OCMW Lanaken	Stad Lommel
Gemeente & OCMW Liedekerke	Stad Schoten

Wanneer bij een bestuur de ICT-organisatie gemeenschappelijk is opgezet voor gemeente en OCMW, zijn veel van de vaststellingen vaak voor beide van toepassing. Wanneer reeds dezelfde secretaris was aangeduid voor gemeente en OCMW, werd dan ook een auditrapport opgemaakt voor beide. De 28 geauditeerde organisaties waar van sprake in dit rapport omvatten dus eigenlijk 35 lokale besturen.

[9] De I-monitor is een initiatief van Informatie Vlaanderen in samenwerking met o.a.de VVSG. De I-monitor geeft de zelf ingeschatte maturiteit weer van lokale besturen in Vlaanderen op het vlak van informatiehuishouding en IT.

BIJLAGE 2: DE GEANONIMISEERDE RESULTATEN

	+ 19.000 inwoners									aantal inwoners < 19.000 en > 12.000									< 12.000 inwoners									gemiddelde
ORGANISATIEBEHEERSING																												
Organisatiebeheersing	3	3	2	2	3	0	3	0	2	3	0	3	3	2	2	2	2	0	2	0	3	0	0	0	0	2	3	1,67
BELEID EN ORGANISATIE	**3**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1**	**1**	**1,78**
informatiebeveiligingsbeleid	3	3	2	1	1	2	1	1	2	3	3	1	1	2	2	2	2	2	2	1	2	2	2	2	2	1	2	1,85
rollen en verantwoordelijkheden	3	3	2	1	2	2	2	1	2	3	3	2	2	2	2	2	1	2	2	2	1	2	1	3	2	1	1	1,93
leveranciersrelaties	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,07
naleving	3	2	2	2	2	1	2	1	1	1	4	3	3	1	1	1	1	2	2	2	2	1	1	1	2	1	1	1,70
BEWUSTZIJN	**2**	**2**	**2**	**1**	**2**	**1**	**1**	**1**	**1**	**3**	**3**	**3**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1,78**
veilig personeel (bij en na indiensttreding)	2	3	3	2	1	1	2	1	1	2	3	3	2	3	2	1	1	1	2	2	2	2	2	1	1	1	2	1,81
omgang met digitale en papieren informatiedragers	3	2	2	1	2	2	1	2	1	3	3	3	1	2	1	1	1	2	1	3	2	2	1	1	1	2	2	1,78
TECHNISCH BEHEER	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,44**
cryptografie	3	2	2	1	1	1	2	1	1	1	1	1	2	0	1	1	2	0	1	1	1	1	1	1	1	1	0	1,15
fysieke beveiliging	2	2	3	3	2	2	nvt	2	1	3	3	2	3	2	2	2	2	2	2	2	3	2	1	2	1	3	1	2,04
beveiliging van de IT-omgeving	2	2	2	2	1	1	2	1	1	2	1	1	2	1	2	2	2	1	2	2	2	1	2	1	1	1	1	1,52
netwerkbeveiliging	2	2	2	2	2	2	2	1	1	2	1	1	2	1	2	1	2	1	2	2	2	2	1	2	1	2	1	1,63
acquisitie, ontwikkeling en onderhoud van informatiesystemen	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,04
LOGISCH TOEGANGSBEHEER	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**3**	**2**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,56**
veilig personeel (bij en na uitdiensttreding)	1	2	2	2	2	1	1	1	0	3	2	3	1	2	3	1	1	1	2	2	1	2	1	1	0	2	1	1,52
beheer van bedrijfsmiddelen en classificatie van informatie	2	2	2	2	2	1	1	2	1	3	2	2	1	2	1	1	1	2	1	2	2	1	1	1	1	1	2	1,56
toegangsbeveiliging	2	1	2	2	2	2	1	1	2	2	3	2	1	2	1	2	1	1	3	2	2	2	2	1	1	1	1	1,67
CONTINUÏTEIT	**2**	**3**	**3**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**3**	**1**	**1**	**1**	**2**	**1**	**3**	**1**	**1**	**2,22**
INCIDENTENBEHEER	**3**	**1**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**	**1,26**
gemiddelde maturiteit informatiebeveiliging (op de 16 aspecten)	2,25	2,00	2,00	1,75	1,69	1,50	1,47	1,31	1,19	2,19	2,06	1,94	1,75	1,63	1,63	1,44	1,38	1,31	1,75	1,69	1,69	1,50	1,31	1,31	1,31	1,31	1,19	1,61
	1,68									1,70									1,45									

	+ 19.000 inwoners									aantal inwoners < 19.000 en > 12.000									< 12.000 inwoners									gemiddelde
Organisatiebeheersing	3	3	2	2	3	0	3	0	2	3	0	3	3	2	2	2	2	0	2	0	3	0	0	0	0	2	3	1,67
BELEID EN ORGANISATIE	**3**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1**	**1**	**1,78**
BEWUSTZIJN	**2**	**2**	**2**	**1**	**2**	**1**	**1**	**1**	**1**	**3**	**3**	**3**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1,78**
TECHNISCH BEHEER	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,44**
LOGISCH TOEGANGSBEHEER	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**3**	**2**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,56**
CONTINUÏTEIT	**2**	**3**	**3**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**3**	**1**	**1**	**1**	**2**	**1**	**3**	**1**	**1**	**2,22**
INCIDENTENBEHEER	**3**	**1**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**	**1,26**

De gemiddelde maturiteit informatiebeveiliging (op de 16 aspecten) bedraagt voor de OCMW's 1,71 , voor de organisaties waar gemeente en OCMW samen werden geëvalueerd 1,59 en voor de gemeenten 1,55. Het verschil is voornamelijk te verklaren door het domein bewustzijn.
De inschattingen voor de provincie werden in deze tabellen niet meegenomen gelet op de beperktere vergelijkbaarheid ervan.
De legende is te vinden op p. 8.

BIJLAGE 3: DE RESULTATEN VAN DE PHISHINGTEST BIJ DE LOKALE BESTUREN

In de marge van de thema-audit Informatiebeveiliging organiseerde Audit Vlaanderen een phishingtest voor alle gemeenten, OCMW's en provincies om het bewustzijn voor internetfraude via phishing[7] te testen. Deze bijlage beschrijft beknopt de aanpak en de overkoepelende resultaten. Alle deelnemende lokale besturen ontvingen een individueel rapport met hun resultaten.

Audit Vlaanderen verstuurde onschadelijke phishingmails naar de e-mailadressen die door de ingeschreven besturen werden bezorgd. Via drie scenario's ging Audit Vlaanderen na hoeveel personen potentieel onveilige handelingen stelden:

- De eerste phishingmail was een verzorgde e-mail die opriep om meer te bewegen op het werk en die doorverwees naar een betrouwbaar ogende wedstrijd. Enkel een oplettende gebruiker kon de verdachte aard van deze actie identificeren.
- De tweede phishingmail was een slordig bericht met een hyperlink naar een website met een ongeloofwaardig commercieel aanbod. De verdachte aard van deze actie was overduidelijk. De communicatie oogde opzettelijk onbetrouwbaar en amateuristisch.
- Als derde phishingmail stuurde Audit Vlaanderen een dringende klacht van een fictieve persoon naar het e-mailadres van de secretaris. Voor concrete details verwees het bericht naar een html-bestand dat als bijlage werd meegestuurd.

De eerste twee scenario's maten het bewustzijn omtrent het:

- klikken op een mogelijk malafide link waardoor de computer van de gebruiker kan worden besmet met een computervirus;
- ingeven van gebruikersgegevens op een onbekende en onveilige website waardoor computercriminelen deze informatie kunnen misbruiken.

Het derde scenario ging na of er voldoende aandacht is voor bijlagen die kwaadaardige codes kunnen bevatten.

Uit de phishingtest blijken de volgende conclusies:

- **Verschillende gemeenten en OCMW's hanteren goede technische beheersmaatregelen om het risico op phishing te beperken.**

  16% van de gemeenten en 25% van de OCMW's slaagden erin de phishingmails uit de mailboxen van hun medewerkers te houden door automatische en/of manuele filtering. Dit was bij geen enkele provincie het geval. Audit Vlaanderen kon 1 op de 4 deelnemende besturen niet bereiken met de eerste, goed verzorgde phishingmail. De tweede phishingmail was opzettelijk veel doorzichtiger en raakte bij net iets meer dan 1 op 2 besturen niet in de mailbox van de medewerkers.

  De bijlage bij de phishingmail die zich specifiek richtte naar de secretarissen werd in 68% van de gevallen binnen de twee dagen geopend. Enkele van de aangeschreven secretarissen antwoordden dat de bijlage bij het bericht omwille van afspraken in het kader van het informatieveiligheidsplan niet kon worden geopend en vroegen de afzender om de boodschap op een andere wijze te bezorgen.

- **De medewerkers van de lokale besturen zijn in zekere mate risicobewust, maar een deel is nog te nieuwsgierig en klikt door naar mogelijk besmette websites.**

  Naar aanleiding van de phishingmails 1 en 2 klikten respectievelijk 7% en 12% van de medewerkers van de gemeenten en de OCMW's via een hyperlink door naar de achterliggende websites. Bij de provincies was dit 9% voor phishingmail 1 en 15% voor phishingmail 2. Deze personen stelden hierdoor handelingen die voor hun besturen een risico vormen.
  De medewerkers die doorklikken behoren voor phishingmail 1 tot 75% van de deelnemende besturen. Voor phishingmail 2 gaat het om 63% van de deelnemende besturen. In beide gevallen klikten medewerkers van alle 5 de provincies door.

  De phishingtest werd niet aangevuld met een verdere evaluatie van de mate waarin deze besturen technische maatregelen voorzien voor het beperken van de veiligheidsrisico's. Mogelijke maatregelen daarvoor zijn regelmatige updates van de IT-systemen en beschermingssoftware, netwerksegmentatie, bedrijfscontinuïteitsmaatregelen en een toereikend incidentbeheer. De thema-audit informatiebeveiliging toont aan dat de 28 geauditeerde besturen alvast niet afdoende beschermd zijn tegen dergelijke risico's.

- **Door de onveilige handelingen van sommige medewerkers lopen een ruime meerderheid van gemeenten en OCMW's en alle provincies aanzienlijke veiligheidsrisico's.**

  Sommige kwaadaardige software heeft maar één onvoorzichtige gebruiker nodig om voor een verregaande besmetting te zorgen. Een deel van de medewerkers die in de eerste of tweede phishingmail via de hyperlink doorklikten, gaven daarna vrijwillig hun gebruikersnaam en wachtwoord prijs. Dit gebeurde bij 280 van de 418 deelnemende gemeenten en OCMW's. Dit betekent dat bij 67% van de ingeschreven gemeenten en OCMW's gebruikersgegevens werden prijsgegeven. Dit gebeurde ook bij 100% van de provincies.

Een beschrijving van deze phishingtest en van de overkoepelende resultaten is online beschikbaar:

De beschrijving van de phishingtest

De overkoepelende resultaten van de gemeenten en OCMW's

De overkoepelende resultaten van de provincies

BIJLAGE 4: ENKELE VOORBEELDEN VAN INFORMATIEBEVEILIGINGSINCIDENTEN

In 2017 leerde de wereld (nogmaals) ransomware kennen: kwaadwillige software (zogenaamde 'malware') die de gegevens op computers versleutelt (en dus onleesbaar maakt voor de gebruiker), waarna een boodschap verschijnt die vraagt losgeld te betalen voor de versleutelde gegevens.

Een eerste breed bekend geworden ransomware, die de naam "Wannacry" meekreeg, zorgde in mei 2017 wereldwijd voor grote problemen. Wannacry verspreidde zich via geïnfecteerde bestanden in phishing-mails. Eens een computer geïnfecteerd was, probeerde deze ransomware zich bovendien te kopiëren naar alle andere computers in hetzelfde netwerk. De poging om zichzelf te kopiëren lukte alleen wanneer binnen het netwerk gebruik werd gemaakt van een verouderd netwerkprotocol. Tijdens de thema-audit bleek dat verschillende lokale besturen nog steeds gebruik maken van dat protocol.

In juni 2017 volgde een andere ransomware met enkele duidelijke verschillen, onder andere:
- de initiële verspreiding gebeurde via een besmette update van een veel gebruikte toepassing (een illustratie van het samenspel en de onderlinge afhankelijkheid tussen organisaties en hun leveranciers);
- de code van deze ransomware was speciaal vormgegeven om antivirusbescherming te misleiden en werd door veel virusscanners destijds niet herkend;
- hoewel wel losgeld werd gevraagd, was de toegebrachte schade eigenlijk onherroepelijk.

Er zijn geruchten dat deze andere ransomware vooral bedoeld was als aanval op een aantal Oekraïnse overheidsinstanties. Veel internationale bedrijven geraakten geïnfecteerd. Zo onder meer koeriersbedrijf TNT dat het een tijdlang moeilijk had om verzendingen af te handelen en aangaf ook een deel van de verzendgegevens van pakketten onherstelbaar verloren te hebben. Een ander gekend slachtoffer was transportbedrijf Maersk, wereldwijd het grootste bedrijf op het gebied van containertransport over water. Dit incident ontwrichtte dan ook internationaal de werking van een hele reeks havens en veroorzaakte honderden miljoenen euro's schade. Maersk maakte achteraf zelf bekend dat ze – zelfs met de immense inspanning die ze hadden geleverd – tien dagen nodig hadden gehad om alle servers, computers en toepassingen te herinstalleren.

Nog in 2017 bleek (nogmaals) dat bij online bewakingscamera's, net zoals veel andere hard- en software, gebruikers (naast privépersonen ook commerciële firma's en besturen) vaak nalaten het standaardwachtwoord te veranderen. De federale staatssecretaris voor o.a. privacy riep in augustus 2017 betrokkenen op om klacht in te dienen tegen een Russische website die verschillende beelden online beschikbaar maakte.

Een ander fenomeen dat vorig jaar onder de aandacht werd gebracht, was de kwetsbaarheid van wachtwoorden die gebruikers voor verschillende websites gebruiken. Concreet werd door ethische hackers een website opgezet waar je kan zien of er de afgelopen jaren wachtwoorden gehackt zijn van websites waar jij destijds ook op inlogde.

In de eerste helft van 2018 verspreidde Drupal, een systeem waar veel websites gebruik van maken, tot tweemaal toe een kritieke beveiligingsupdate voor een kwetsbaarheid waar reeds grootschalige aanvallen op waren vastgesteld. Drupal gaf daarbij telkens quasi simultaan informatie over de kwetsbaarheid én de update vrij. Omdat niet iedereen even snel de updates kon doorvoeren, volgden heel wat aanvallen op systemen die niet snel genoeg bijgewerkt waren. Dit droeg er onder meer toe bij dat honderden websites besmet werden, waarna een deel van de performantie van de computers waarmee deze websites werden bezocht, ongevraagd 'gestolen' werd om cryptogeld (een variant op bitcoin) aan te maken.

Er waren de voorbije jaren ook geregeld grootschalige datalekken bij overheden. Zo zorgde een onzorgvuldigheid bij het Zweedse transportagentschap er in 2015 voor dat onbevoegden toegang kregen tot vertrouwelijke informatie en persoonsgegevens van miljoenen Zweden. In 2016 bleken 200.000 patiëntengegevens (onderzoeksresultaten) van twee Belgische ziekenhuizen een maand lang publiek toegankelijk op het internet te staan. In datzelfde jaar werd in Nederland door een arts een usb-stick verloren met honderden patiëntengegeven die niet versleuteld waren en dus door de vinder (of dief?) vrij konden bekeken worden. Reeds in 2012 werden persoonsgegevens van 700.000 reizigers van NMBS Europe enkele maanden opgeslagen op een locatie die vrij toegankelijk is via het internet.

Ook Vlaamse lokale besturen ontspringen de dans niet en worden door informatiebeveiligingsincidenten getroffen. Zo ontvingen verschillende financieel beheerders (thans financieel directeurs) de afgelopen jaren phishing-mails waarin hen zogezegd door de secretaris (thans algemeen directeur) gevraagd werd dringend geld over te schrijven. In 2017 ging veel aandacht naar de afwezigheid van veilige verbindingen bij ongeveer 1 op 5 Vlaamse gemeentelijke websites. Verschillende Vlaamse gemeenten hebben in het verleden al hun dienstverlening aan de burger moeten verminderen en zelfs tijdelijk stopzetten ten gevolge van informatiebeveiligingsincidenten. In één geval duurde het na een cyberaanval vorig jaar drie weken alvorens de betrokken gemeente het normale niveau van dienstverlening kon hervatten.

Ook enkele geauditeerde besturen ervaarden in het verleden al de gevolgen van virussen en malware op computers en servers, onbeschikbaarheid van loketruimtes, diefstal van documenten of IT-apparatuur en andere reële probleemsituaties.

Dat informatiebeveiliging veel ruimer gaat dan enkel ICT, is eveneens in Vlaanderen duidelijk: Een Vlaamse stad liep al schade op doordat een ontevreden burger ongezien naar de kelder kon wandelen en er vernielingen aanrichtte. Vorig jaar nog maar kwam een Vlaams OCMW in opspraak omdat dozen vol papier met vertrouwelijke en (persoons)gevoelige informatie waren buitengezet voor ophaling als oud papier en vervolgens in de tuinen van de buren waaiden.

BIJLAGE 5: ENKELE VOORBEELDEN VAN VLOT INZETBARE OPLOSSINGEN

Diverse actoren op alle bestuursniveaus spannen zich in voor de bescherming van de gegevens waarover de lokale besturen beschikken. Ook vele commerciële en non-profitorganisaties bieden daarbij ondersteuning. Het hoeft dan niet te verbazen dat zelfs zonder bewuste en gecoördineerde samenwerking hieromtrent nu reeds enkele pragmatische oplossingen bestaan of in ontwikkeling zijn. Om dit te illustreren, maar zonder exhaustief te willen zijn, verwijzen we hier naar een aantal van deze oplossingen. De aangehaalde voorbeelden werden niet geauditeerd en worden dan ook vermeld zonder garanties.

Beleid en organisatie

Om een goed informatiebeveiligingsbeleid te kunnen uitbouwen, is het nuttig om eerst zicht te hebben op de risico's waar je bestuur mee geconfronteerd wordt en op de al bestaande beheersmaatregelen. De informatieveiligheidstool aangeboden door de Vlaamse ICT-organisatie vzw (V-ICT-OR) biedt een vlot inzetbare oplossing voor een reeks van uitdagingen. Via deze tool kunnen organisaties onder andere een risicoanalyse en maturiteitsmeting uitvoeren om verbeteracties op te lijsten in een actie- of veiligheidsplan; een verwerkingsregister opstellen of aanvullen; de verwerkingsovereenkomsten centraal beheren; goede voorbeelden consulteren en sjablonen gebruiken.

Om het informatiebeveiligingsbeleid te concretiseren in een informatieveiligheidsplan met bijhorende procedures en afsprakenkaders is de informatieveiligheidsconsulent vaak een drijvende kracht in samenwerking met de informatieveiligheidscel. Verschillende veiligheidsconsulentenorganisaties bieden sjablonen voor het opstellen van een informatieveiligheidsbeleid, van een informatieveiligheidsplan en van tal van andere plannen, procedures en afsprakenkaders. Dergelijke sjablonen zijn nuttig om niet van nul te moeten beginnen.

Ook de VVSG biedt op zijn website verschillende sjablonen en linken naar nuttige documenten als inspiratie om mee te nemen bij het uitwerken van diverse elementen van het informatiebeveiligingsbeleid (http://www.vvsg.be/Werking_Organisatie/informatieveiligheid/Paginas/default.aspx).
De Cyberguide van het Centrum voor Cybersecurity Belgium (afgekort CCB, https://ccb.belgium.be/nl) geeft dan weer op zeer bevattelijke wijze duiding bij diverse informatiebeveiligingsrisico's en bij nuttige mogelijke beheersmaatregelen (https://cyberguide.ccb.belgium.be/nl).
En met de nodige aanpassingen, kunnen ook verschillende sjablonen die beschikbaar zijn bij de Nederlandse buren een insteek bieden.

Bewustzijn

De Vlaamse overheid stelt al enkele jaren via e-learning een gratis bewustmakingsopleiding beschikbaar. Lokale besturen die dit willen aanbieden aan hun personeelsleden kunnen dit (aan)vragen via www.facilipunt.be of 3200@vlaanderen.be .

Informatie over de bewustmakingscampagnes van de Vlaamse overheid staat online ter inspiratie van anderen (https://overheid.vlaanderen.be/ict/informatieveiligheid/bewustmaking).

Safe on web (https://www.safeonweb.be/nl), een initiatief van het CCB, probeert ook ondersteuning te bieden voor de sensibilisering van gebruikers rond de gevaren van de digitale wereld.

Technisch beheer

Om alle aspecten van het technisch beheer af te dekken, is veel kennis en energie vereist. Informatie Vlaanderen faciliteert al langer e-government en digitalisering door het aanbieden van diverse basisdiensten. Steeds meer zijn de oplossingen waar Informatie Vlaanderen aan werkt ook gericht op het verminderen van de zorgen van lokale besturen en andere afnemers. Zo is bijvoorbeeld in het gegevensdelingsplatform Magda al jaren logging voorzien die kan helpen invulling te geven aan de verhoogde aandacht voor gegevensbescherming sinds de AVG. Verschillende oplossingen bieden ook een betrouwbare en veilige ontsluiting van authentieke bronnen en andere gegevensregisters. Eén voorbeeld daarvan is de ontsluiting van allerlei geografische data via het Geopunt (http://www.geopunt.be), niet enkel via diensten waar besturen kunnen op aansluiten, maar deels ook rechtstreeks in publiek toegankelijke viewers. Een ander voorbeeld is Magdaonline (https://overheid.vlaanderen.be/magda) waar personeelsleden van besturen na een beperkte registratie en in het kader van gerechtvaardigde doeleinden via de beveiligde website Magda-diensten kunnen bevragen, bijvoorbeeld om adresgegevens op te zoeken. Ook de in ontwikkeling zijnde opvolger van Magda, de Vlaamse Kruispuntbank, zal verschillende zorgen kunnen opvangen.

Uit de hertesting bleek hoe moeilijk besturen het hebben om kwetsbaarheden te identificeren en aan te pakken. Toch bestaan er verschillende hulpmiddelen op dat vlak, zelfs enkele gratis tools om een reeks gekende kwetsbaarheden te detecteren, bijvoorbeeld de Baseline Security Analyzer voor windows-systemen. Ook is de informatie over de meeste gekende kwetsbaarheden op het internet te vinden, bijvoorbeeld op www.CVEdetails.com .

Logisch toegangsbeheer

Een goed beheer van toegangen en rechten blijft een uitdaging. Een belangrijke factor daarbij is dat het moeilijk is zicht te houden op de actualiteit van de toegekende rechten. Ook verschilt de toekenning van rechten al eens per toepassing of minstens per leverancier, wat het niet altijd makkelijk maakt om een goed overzicht te houden. De door Het Facilitair Bedrijf aangeboden dienstverlening in de vorm van het Gebruikersbeheer Vlaanderen https://overheid.vlaanderen.be/ict/ict-diensten/gebruikersbeheer biedt een aantal functionaliteiten die het beheer kunnen ondersteunen. Zo is het bijvoorbeeld mogelijk om per persoon een overzicht te trekken van alle via het gebruikersbeheer toegekende rechten. Dat rapportje is niet enkel nuttig voor individuele toepassingsbeheerders, maar kan ook organisatiebreed worden opgevolgd. Ook is de interface voor het toekennen, wijzigen en intrekken van de rechten identiek voor alle aangesloten toepassingen. Voorwaarde voor dit alles is natuurlijk wel dat de toepassingen worden aangesloten op het gebruikersbeheer, wat een beperkte ontwikkeling kan vergen.

Continuïteit

Een noodplanning voor ICT gaat veel verder dan louter een back-up voorzien. Verschillende organisaties die IT-projecten bij lokale besturen begeleiden, bieden daarom sjablonen en handleidingen aan voor het opstellen van continuïteitsplannen. Zo heeft ook VERA, het steunpunt e-government van de provincie Vlaams-Brabant, een praktische leidraad opgesteld die je vrij kan gebruiken. Je vindt deze op https://www.vera.be/ICTnoodplanning. De leidraad helpt organisaties om in kaart te brengen hoelang elk proces mag uitvallen, hoeveel gegevens in extremis kunnen verloren gaan, welke systemen met welke prioriteit terug moeten worden opgestart en wie welke rol moet opnemen.

Incidentenbeheer

Voor dit aspect van informatiebeveiliging werden helaas nog maar weinig oplossingen uitgewerkt. Wel kan worden verwezen naar het Belgische Computer Emergency Response Team (www.cert.be) .

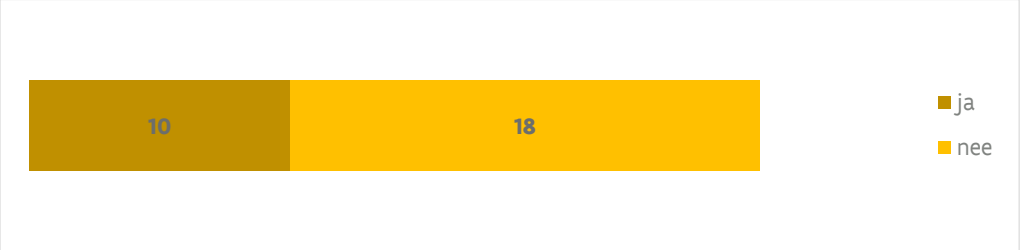
BIJLAGE 6: VASTSTELLINGEN IN CIJFERS

In deze bijlage worden enkele vaststellingen cijfermatig weergegeven. Deze cijfers hebben enkel betrekking op de geauditeerde organisaties (zie bijlage 2). Elke audit werd hierbij als 1 organisatie geteld, ongeacht de betrokken besturen.

Organisatiebeheersing

Hebben de geauditeerde lokale besturen een door de raad goedgekeurd kader om te werken aan hun organisatiebeheersing?

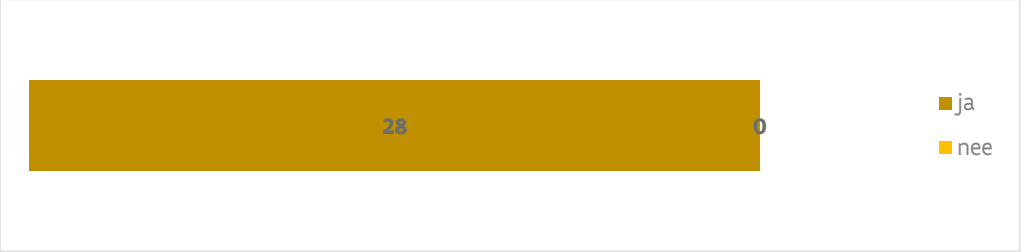
Rapporteren de geauditeerde besturen minstens jaarlijks aan de raad over de organisatiebeheersing?



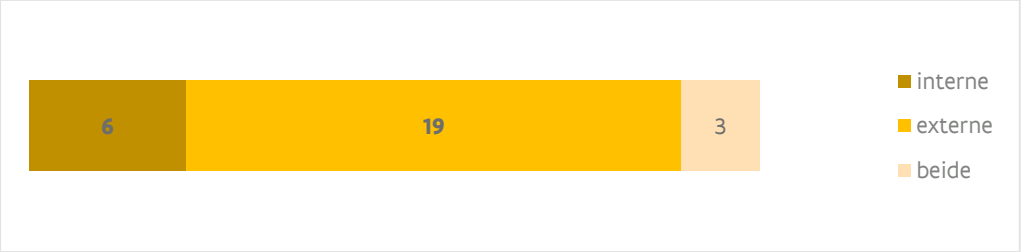
Voerden de geauditeerde besturen reeds een zelfevaluatie uit van hun organisatiebeheersing?

Beleid en organisatie

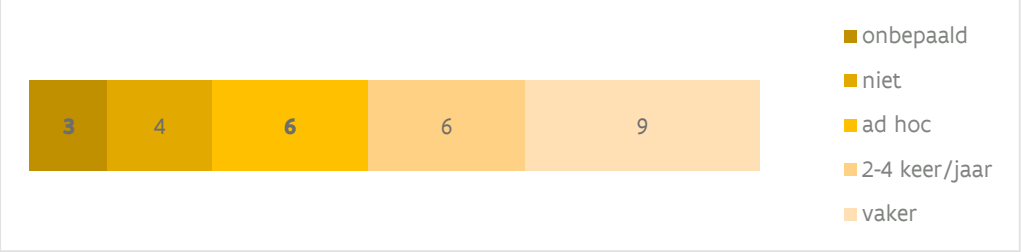
Hebben de geauditeerde besturen een informatieveiligheidsconsulent aangesteld?



Kiezen de geauditeerde besturen voor een interne of een externe informatieveiligheidsconsulent?



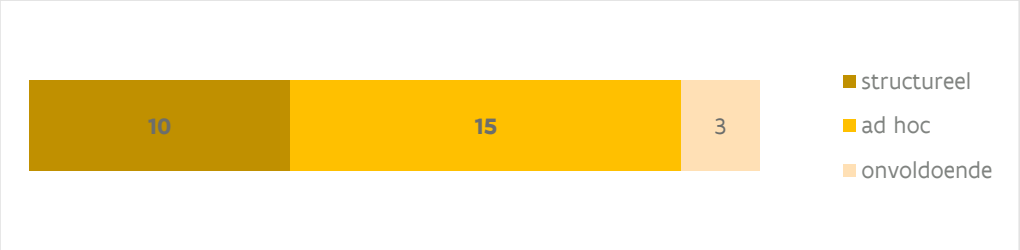
Hoe frequent komt de informatieveiligheidscel bij de respectievelijke geauditeerde besturen samen?



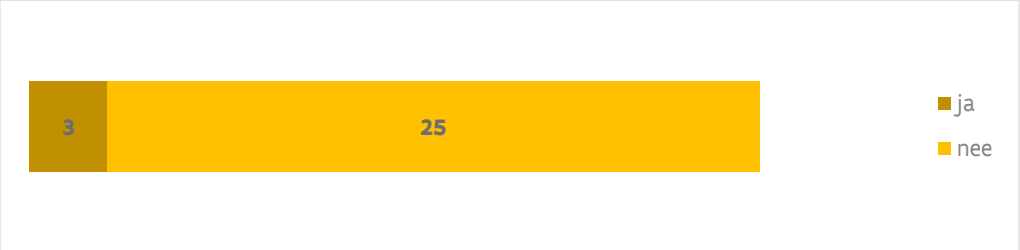
Bewustzijn

Besteden de geauditeerde besturen aandacht aan informatiebeveiliging bij werving en selectie?

Sensibiliseren de geauditeerde besturen periodiek hun personeelsleden?



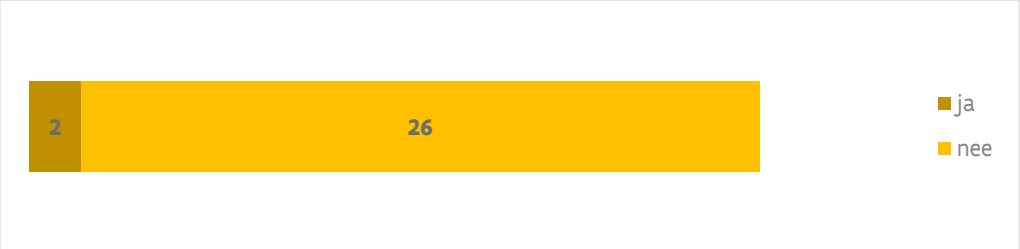
Sensibiliseren de geauditeerde besturen personeelsleden bij uitdiensttreding over hun beroepsgeheim?



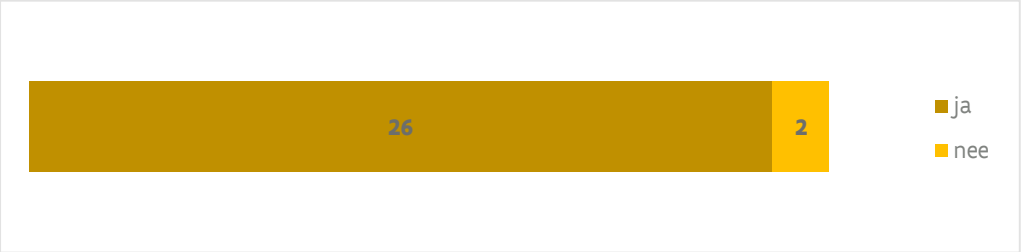
Technisch beheer

In welke mate passen de geauditeerde besturen reeds cryptografische maatregelen toe?

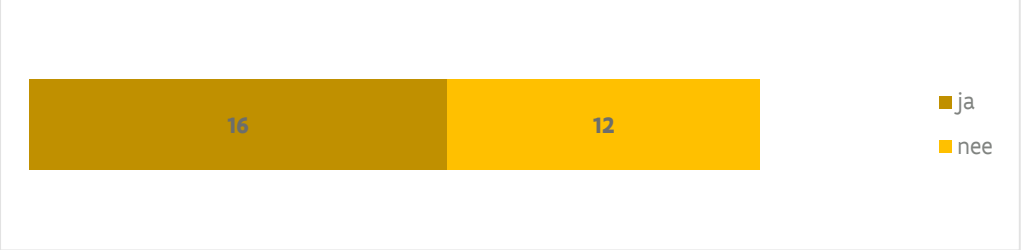
Hadden de geauditeerde besturen bij aanvang van de audit al een goede aanpak om afscherming door versleuteling te voorzien wanneer vertrouwelijke en/of gevoelige informatie wordt opgeslagen op USB-sticks?



Gebruiken de geauditeerde besturen een inbraakdetectiesysteem voor ruimtes met vertrouwelijke en/of (persoons)gevoelige informatie?

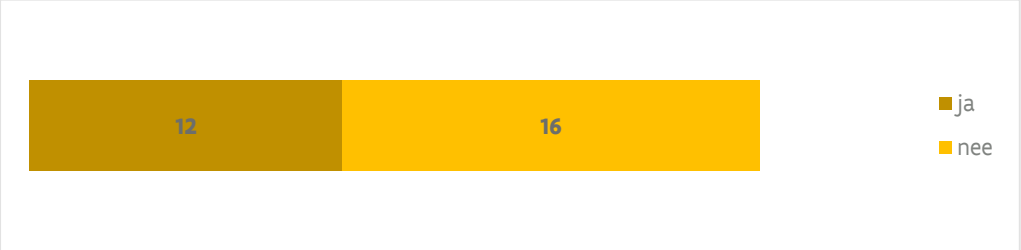


Besteden de geauditeerde besturen voldoende aandacht aan de fysieke beveiliging van hun primaire serverruimte?

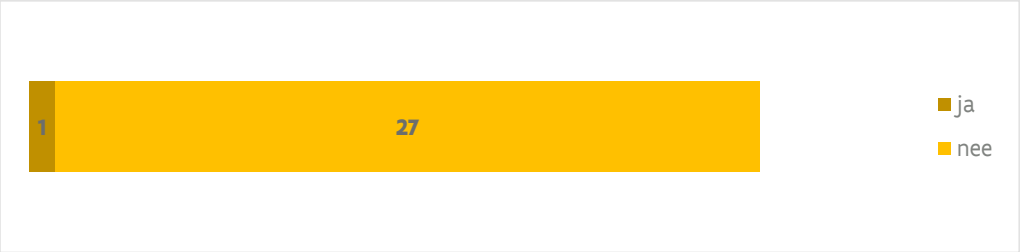


Zijn de archiefruimtes van de geauditeerde besturen steeds afgesloten?

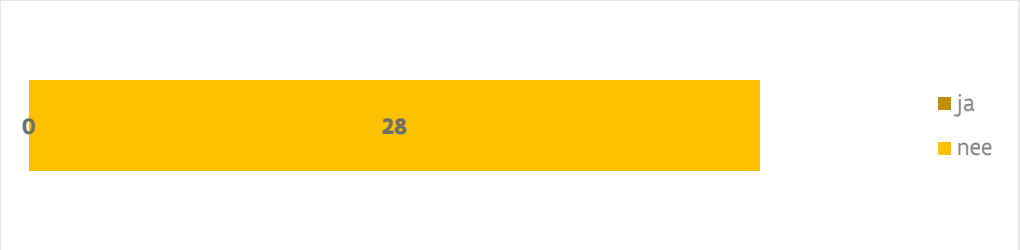
Voeren de geauditeerde besturen een clean desk of clear desk beleid?



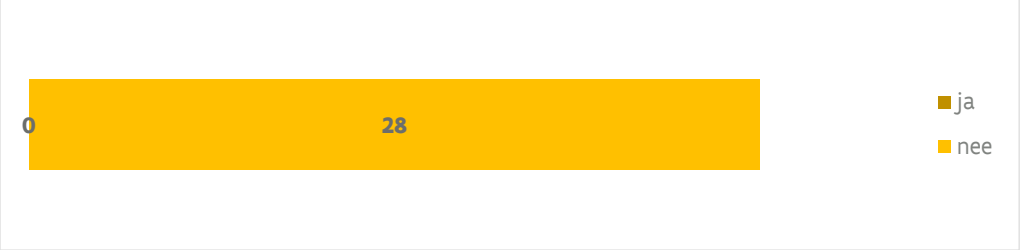
Gebruiken de geauditeerde besturen zelf al periodieke aanvals- en penetratietesten om de effectiviteit van hun inspanningen op te volgen?



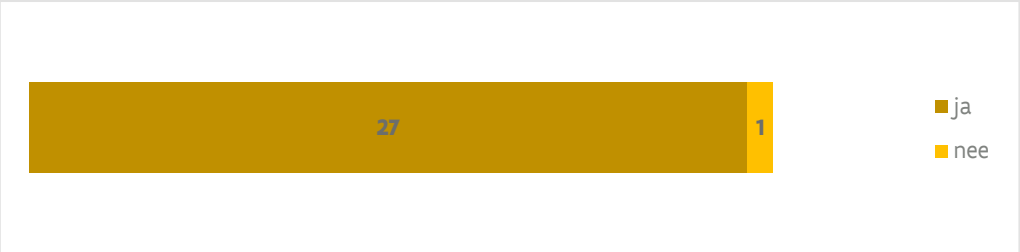
Beschikken de geauditeerde besturen over een gecentraliseerde opslag van logging-gegevens die hen toelaat om bij een hacking (en bij defecten) waarbij het IT-systeem volledig verloren gaat, te onderzoeken welke kwetsbaarheden moeten worden opgelost om herhaling van de hacking te voorkomen?



Passen de geauditeerde besturen binnen hun interne IT-netwerk een vorm van segmentatie of monitoring toe die om te vermijden dat bij de besmetting van een individuele eindgebruikerscomputer ongemerkt en ongehinderd de achterliggende centrale IT-apparatuur (bv. de servers) kan worden aangevallen?



Is er binnen de IT-omgeving van de geauditeerde besturen vertrouwelijke en/of (persoons)gevoelige informatie opgeslagen die onbedoeld door alle aangemelde computergebruikers kan worden geraadpleegd?



Konden tijdens de technische testen in het kader van deze thema-audit bij de geauditeerde besturen wachtwoorden van gebruikers (eindgebruikers, beheerders en/of technische accounts) worden achterhaald?

Laat de configuratie van de diverse IT-systemen bij de geauditeerde besturen toe dat een hacker sommige gebruikersnamen en/of wachtwoorden kan uitlezen?

Kunnen hackers één of meerdere van de binnen het interne IT-systeem uitgewisselde informatiestromen onderscheppen en de vertrouwelijke en/of (persoons)gevoelige informatie er in uitlezen?

Kon tijdens de technische testen in het kader van deze thema-audit bij de geauditeerde besturen van binnen het interne netwerk uit controle worden verkregen over de volledige IT-omgeving of de belangrijkste delen ervan?

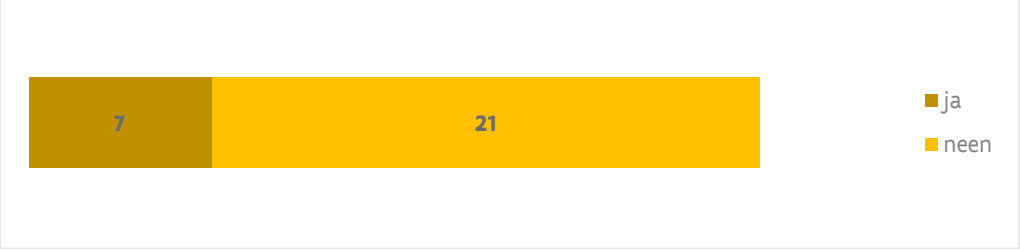
Logisch toegangsbeheer

Passen de geauditeerde besturen reeds een classificatie van informatie toe om informatie in functie van de vertrouwelijkheid ervan anders te behandelen?

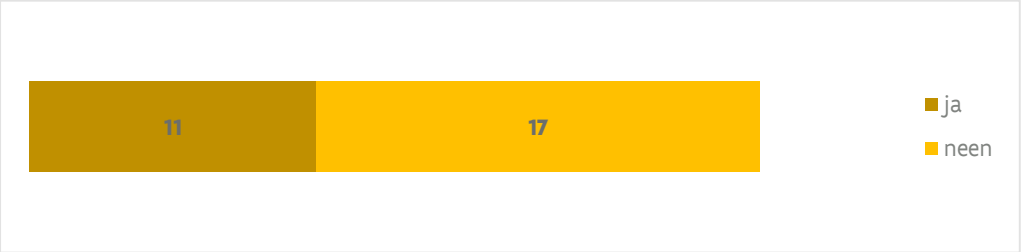
Hebben de geauditeerde besturen een proces om rechten en toegangen te beheren of voeren ze dat beheer ad hoc uit?

Hebben de geauditeerde besturen een wachtwoordbeleid?

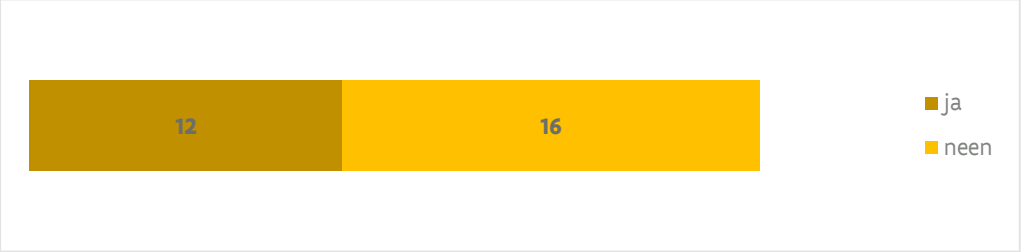
Dwingen de geauditeerde besturen bij het aanmaken of wijzigen van wachtwoorden af dat het voldoende sterke wachtwoorden moeten zijn?



Verplichten de geauditeerde besturen de gebruikers om periodiek hun wachtwoord voor het centrale gebruikersbeheer (active directory) te wijzigen?

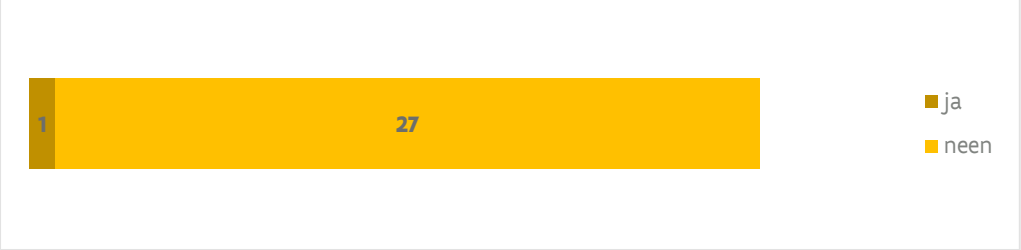


Sensibiliseren de geauditeerde besturen hun gebruikers om veilig om te gaan met hun wachtwoorden?



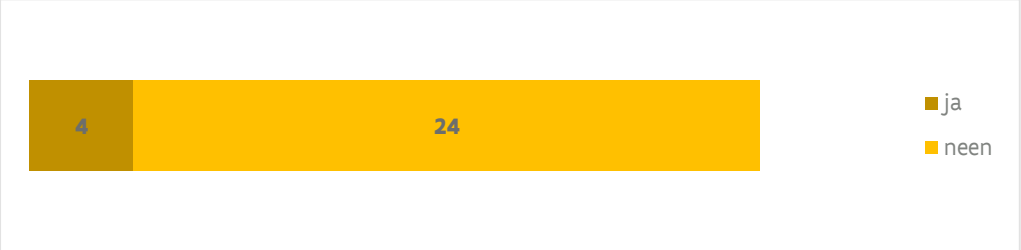
Continuïteit

Hebben de geauditeerde besturen een volwaardig bedrijfscontinuïteitsplan?

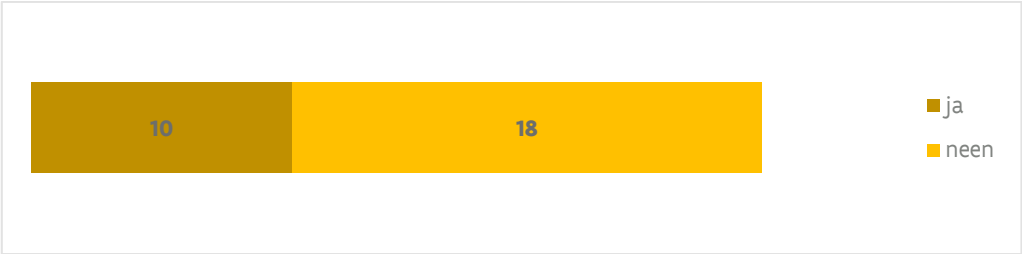


Incidentenbeheer

Hebben de geauditeerde besturen een procedure om informatiebeveiligingsincidenten te identificeren en af te handelen?



Houden de geauditeerde besturen een incidentenregister bij?



COLOFON

VERANTWOORDELIJKE UITGEVER
Mark Vandersmissen
Administrateur-generaal
Audit Vlaanderen

CONTACT
Audit Vlaanderen
Havenlaan 88, bus 24
1000 Brussel
02 553 45 55

Deze publicatie is ook beschikbaar op www.auditvlaanderen.be