Ontwikkelingen op het Gebied van Data, Applicatie en IT-Control

Positioneringsdocument A

Gezien de ontwikkelingen in het gemeentelijk domein zal de informatievoorziening een steeds grotere rol vervullen, ook op het gebied van control. De vraag is niet óf big en open data, cyber bedreigingen, cloud computing, en al die andere ontwikkelingen optreden. De vraag is hoe de gemeente hiermee moet omgaan. Voldoen aan de gestelde normen (KIDO, BIG) van het Rijk, self-compliant te zijn en blijven, adequaat inspelen op digitalisering en het vormgeven van general/application controls vereist een betere en innovatieve verankering van IT binnen de gemeentelijke organisatie.

Michelle van Geffen

10-11-2016

ONTWIKKELINGEN OP HET GEBIED VAN DATA, APPLICATIE EN IT-CONTROL

Positioneringsdocument A

Digitalisering & Datastromen

De digitalisering van de maatschappij vertaalt zich in een exponentiële groei van informatie, hoge verwachtingen over de beschikbaarheid van die informatie en steeds veranderend gebruik ervan. Gemeente Haarlem ontwikkelt zich in dit licht snel van een papieren organisatie naar een digitale organisatie. Dat geldt o.a. voor de dienstverlening aan en communicatie met burgers, de digitale wensen en eisen voor de eigen bedrijfsvoering, het uitwisselen van gegevens binnen het Sociaal Domein en voor het digitaal beheren, archiveren en ontsluiten van bestuurlijke besluitvorming. De inzet van de gemeente om de digitale dienstverlening naar burgers en bedrijven te verbeteren past binnen de Rijksagenda voor Dienstverlening 2020.

In het kader van de decentralisaties van rijkstaken naar gemeenten zijn er de afgelopen jaren taken bijgekomen en veranderd (WMO hh zorg, invoering WABO en Sociaal Domein taken). Die taken gaan gepaard met bijhorende grote (privacygevoelige) datastromen. Veel van deze nieuwe taken worden in regionaal verband georganiseerd. Door het overbrengen van taken naar regio-organisaties en veranderen/uitbreiding van de uitvoeringstaken neemt ook de noodzaak toe van het werken in informatieketens binnen de verschillende beleidsdomeinen. Ook de ontwikkelingen rondom basisregistraties (eenmalige uitvraag, meervoudig verplicht gebruik) en smart cities noodzaken tot afwegingen op het gebied van privacy en beveiliging en samenhang in processen. En ook de nieuwe Omgevingswet, waarvan de eerste fase gerealiseerd moet zijn in 2018, dwingt de overheid om de ontwikkeling van een volwassen digitale samenleving te versnellen.

Naast de inzet van de gemeente om de digitale dienstverlening te verbeteren, biedt de toepassing van big data kansen om het beleidsproces te innoveren. Big data toepassing stelt een gemeente daarnaast in staat om tussentijds real time feedback te krijgen over de effectiviteit van het beleid.

In bijna alle werkprocessen en de vastlegging/uitwisseling van data en informatie speelt digitalisering of automatisering een rol. Het zorgvuldig omgaan met de digitale informatie en gegevens van burgers, bedrijven en ketenpartners is voor gemeenten van groot belang. Het is daarom voor de gemeente zaak dat zij haar processen zodanig inricht dat zij grip houdt op de veelheid aan informatie die zij produceert, beheert en deelt.

Kwetsbaarheden & Bedreigingen

Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van gemeenten. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de gemeente en daarmee van de overheid in het algemeen wordt geschaad.

Zo heeft de DigiNotar-crisis (zie kader) aangetoond dat de ICT-infrastructuur van gemeenten kwetsbaar is. Zie voor een actueel beeld van cyber dreigingen t.o.v. de overheid bijlage 2.

DigiNotar was een Nederlands commerciële Certificaatautoriteit dat de PKI-overheidcertificaten verzorgde voor delen van de Nederlandse overheid. Het bedrijf kwam in opspraak toen bleek dat de veiligheidscertificaten niet waterdicht waren. Als gevolg van een hack (juni 2011) konden valse certificaten worden uitgegeven waardoor de afzender van websites niet meer gegarandeerd werd. Op 2 september 2011 zegde de overheid het vertrouwen in DigiNotar op. Toezichthouder OPTA3 besloot op 13 september 2011 dat de uitgegeven certificaten moesten worden ingetrokken. Kort daarna, op 20 september 2011, is het bedrijf DigiNnotar failliet verklaard. Deze casus toont aan dat de gemeente kwetsbaar is, en bij een dergelijke organisatie de controleverklaring nauw samen hangt met de continuïteit van de IT.

Wet-& regelgeving

Vanuit wetgeving zijn allerlei normen van toepassing op de gemeentelijke informatievoorziening. Conform de **Wet hergebruik overheidsinformatie** zijn decentrale overheden verplicht hun informatie zoveel mogelijk “open” aan te bieden, wat met zich meebrengt dat deze informatie digitaal beschikbaar moet zijn. Dit stelt hoge eisen aan de informatieverwerking en het informatiebeheer (van kracht sinds 18 juli 2015). In eerste instantie dient de juiste informatie op het juiste moment in de diverse werkprocessen te kunnen worden gebruikt. Vervolgens dient informatie ook op langere termijn duurzaam en onveranderd beschikbaar te zijn voor onder meer reconstructie van overheidshandelen en historisch onderzoek. Voor informatiebeheer is een overzicht te vinden in de Handreiking **Kwaliteitssysteem Informatiebeheer Decentrale Overheden** (KIDO). KIDO richt zich op het ontwikkelen van een kwaliteitssysteem voor informatiebeheer, zoals bedoeld in artikel 16 van de Archiefregeling. Het beheer van de informatie moet voldoen aan toetsbare eisen van een door de zorgdrager toe te passen kwaliteitssysteem, zowel op strategisch, tactisch als uitvoerend niveau.

Op het gebied van informatiebeveiliging & privacy zijn verschillende normen van toepassing. Op 1 januari 2016 is de **Wet meldplicht datalekken** (Wmd) van kracht gegaan. Iedere burger heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer

en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Hierin staat dat de persoonsgegevens die verwerkt worden door de gemeente beveiligd moet worden tegen verlies en tegen onrechtmatige verwerking. De Wet meldplicht datalekken (Wmd) gaat in op de gevolgen van een inbreuk op de beveiliging van persoonsgegevens. De wet stelt dat een datalek moet worden gemeld aan de Autoriteit Persoongegevens. Een beveiligingsincident hoeft niet perse te leiden tot een datalek, daarom omschrijft de Wmd wat een datalek is en in welke gevallen melding moet worden gemaakt. In het verlengde van (en straks in plaats van) het Wbp is de **Europese Privacy Verordening (EPV)** aangenomen en wordt van kracht op **26 mei 2018.** Zo wordt het verplicht voor gemeente om een Functionaris Gegevensverwerking (of Data-protection officer) aan te stellen. Op grond van de EPV zal het straks verplicht zijn voor de organisatie om aan te tonen dat men voldoet aan de wet. Het zogeheten 'accountability principe'. Voorlopig lijken de grootste uitdagingen te zitten in het sociaal domein. In dit kader verwerkt de gemeente een heleboel persoonsgegevens. Dat roept vragen op als: mogen systemen aan elkaar gekoppeld worden? mag je vanuit de Jeugdwet inzage in de het Wmo-dossier van de ouders? etc. De Functionaris Gegevensverwerking zal hier een kader voor moeten opstellen[1].

Met de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de **Baseline Informatieveiligheid Gemeenten** (BIG) te implementeren.[2] Deze baseline is nu de kern van de verantwoording over informatieveiligheid aan de gemeenteraad. De horizontale verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag. Over de BRP, PUN, Suwinet, BAG, BGT en DigiD moeten gemeenten ook verantwoording afleggen. De horizontale verantwoording richting gemeenteraad vormt hiervoor de basis. BIG is opgezet rondom bestaande normen; de NEN/ISO 27002:2007, NEN/ISO 27001:2005 en de BIR.

De externe druk om aan de hierboven genoemde normen te voldoen neemt toe. Door de stijging van het aantal bedreigingen/kwetsbaarheden en regelgeving omtrent compliance eisen, zal parallel de noodzaak toenemen van **de bewijslast** dat adequaat en betrouwbaar bestuur van informatiebeveiliging is geïmplementeerd, en effectief blijft opereren binnen de gehele organisatie en zijn IT infrastructuur. De vergaande automatisering binnen de gemeente heeft ertoe geleid dat een groot gedeelte van de interne controle is geautomatiseerd en dat zogenaamde "controles buiten het systeem om" niet meer toereikend zijn. Het is dan ook niet verrassend dat vanuit het Rijk **verplichte IT audits** [3]in het kader van de BIG en aanverwante normenkaders aangekondigd zijn, **te beginnen in 2017**. Gezien dit feit, is het relevant om ook de trends te duiden op het gebied van interne beheersing gerelateerd aan IT.

---

[1] Om gemeenten te helpen privacy goed te waarborgen, heeft de VNG een raamwerk ontwikkeld. Zie VNG – Privacy en Gegevensuitwisseling

[2] Strategische Baseline Informatieveiligheid Gemeenten en Tactische Baseline Informatieveiligheid Gemeenten

[3] Voor de wet Basisregistraties Adressen en Gebouwen (BAG) vindt een externe audit plaats, mogelijk zou het voorbereidende werk deels opgepakt kunnen worden door de aan te stellen auditor.

Trends in IT- Control

De aandacht voor ICT beheermodellen en ICT procesmanagement binnen de gemeenten stijgt, blijkt uit het jaarlijkse ICT Benchmark onderzoek uitgevoerd door M&I[4]. De meerderheid van de trends genoemd in het onderzoek hangen samen rond het overkoepelende thema 'governance op het applicatielandschap en het beheer daarop'. Daarnaast blijft ICT beveiliging en privacy een belangrijke trend voor gemeenten.

Het belang van governance op het applicatielandschap en het beheer hierop komt mede door de zogenaamde toename in "de-perimeterisation[5]" van organisaties, en de gemeente. Denk bij de-perimeterisation aan bijvoorbeeld het internet, wat toegang verschaft (van buitenaf) tot voorheen afgesloten systemen. En denk bijvoorbeeld ook in dit kader aan, de Wet Hergebruik Overheidsinformatie die gemeentes verplicht hun informatie zoveel mogelijk "open" aan te bieden, of de informatie-uitwisseling in kader van het Sociaal Domein. Oftewel, alle informatie verwerkende systemen vallen onder de reikwijdte van informatiebeveiliging.

Deze ontwikkelingen "vervagen" het verschil tussen de zogenaamde organisatie grens en de Informatie Technologie (IT) grens. Een ander goed voorbeeld wat leidt tot "de-perimeterisation" is de ontwikkeling van tijd- en plaats onafhankelijk werken en "Bring your own Device".

Dit "vervagen" van het verschil tussen de zogenaamde *organisatie grens* en de *Informatie Technologie* (IT) grens heeft een aantal gevolgen voor IT-control:

- Een steekproef van gedecentraliseerde componenten geeft mogelijk geen goed beeld van de al gehele IT control omgeving.
- Control punten die gecentraliseerd zijn en hiermee extern van applicaties/ systemen zullen verschuiven naar control punten die meer applicatie en data-beveiliging centrisch zijn.
- Door vergrote afhankelijkheid op het data centrum, cliënt en applicatie controls[6] verandert de focus en het belang van kern IT systemen.

Een verschuiving naar zogenaamde 'application controls' is dan ook nodig om de benodigde inspanning om in control te zijn en blijven, te doen afnemen.

Application controls; zijn interne beheersingsmaatregelen binnen de applicatie. Application controls kunnen preventief of detecterend van aard zijn en zijn opgezet om te zorgen voor de integriteit van de administratieve vastleggingen.

Denk bij "application controls" bijvoorbeeld aan geïmplementeerde functiescheidingen aan de hand van autorisatietabellen in de applicatie.

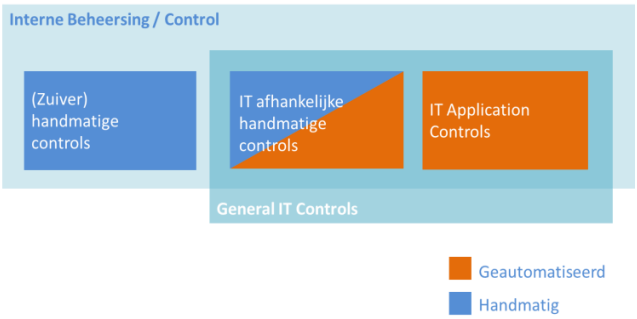
[4] ICT Benchmark onderzoek (M&I) 2016

[5] Metaforisch, de-perimeterisation is vergelijkbaar met de historische ontmanteling van de stadsmuren om vrije verkeer van goederen en informatie mogelijk te maken. Om dit te bereiken werden er staande legers gecreëerd, de stadsgrenzen verschoven zodat ze meerdere steden omringen, oftewel een verschuiving van stadstaten naar natiestaten.

[6] Application controls; zijn interne beheersingsmaatregelen binnen de applicatie. Zie kader.

General IT controls; zijn de interne beheersingsmaatregelen met betrekking tot de geautomatiseerde gegevensverwerking en dienen de betrouwbare werking van deze geautomatiseerde gegevensverwerking te waarborgen.

Denk hierbij bijvoorbeeld aan de toegangsbeveiliging van het netwerk en de



In tegenstelling tot de traditionele controleaanpak waarbij meerdere malen proceduretests worden uitgevoerd om de werking van een interne beheersingsmaatregel vast te stellen, kunnen in plaats daarvan application controls ingebouwd worden. In principe hoef je een application control niet op werking te testen indien je het bestaan ervan hebt vastgesteld. Door het bestaan vast te stellen heb je eenmaal de werking vastgesteld. Denk bijvoorbeeld aan geïmplementeerde functiescheidingen aan de hand van autorisatietabellen in de applicatie. Die blijven altijd hetzelfde werken, tenzij je veranderingen doorvoert. Hierdoor is het - indien geen wijzigingen hebben plaatsgevonden voldoende om eenmaal de werking vast te stellen. Dit geldt alleen indien de general IT controls (denk bijvoorbeeld aan; de toegangsbeveiliging van het systeem en het wijzigingsmanagement)- gedurende de gehele controleperiode goed functioneren.

Application controls en general IT controls staan met elkaar in verband. De relatie is zodanig dat general IT controls nodig zijn om het functioneren van application controls te ondersteunen, en beiden zijn nodig om de volledige en accurate informatieverwerking te verzekeren.

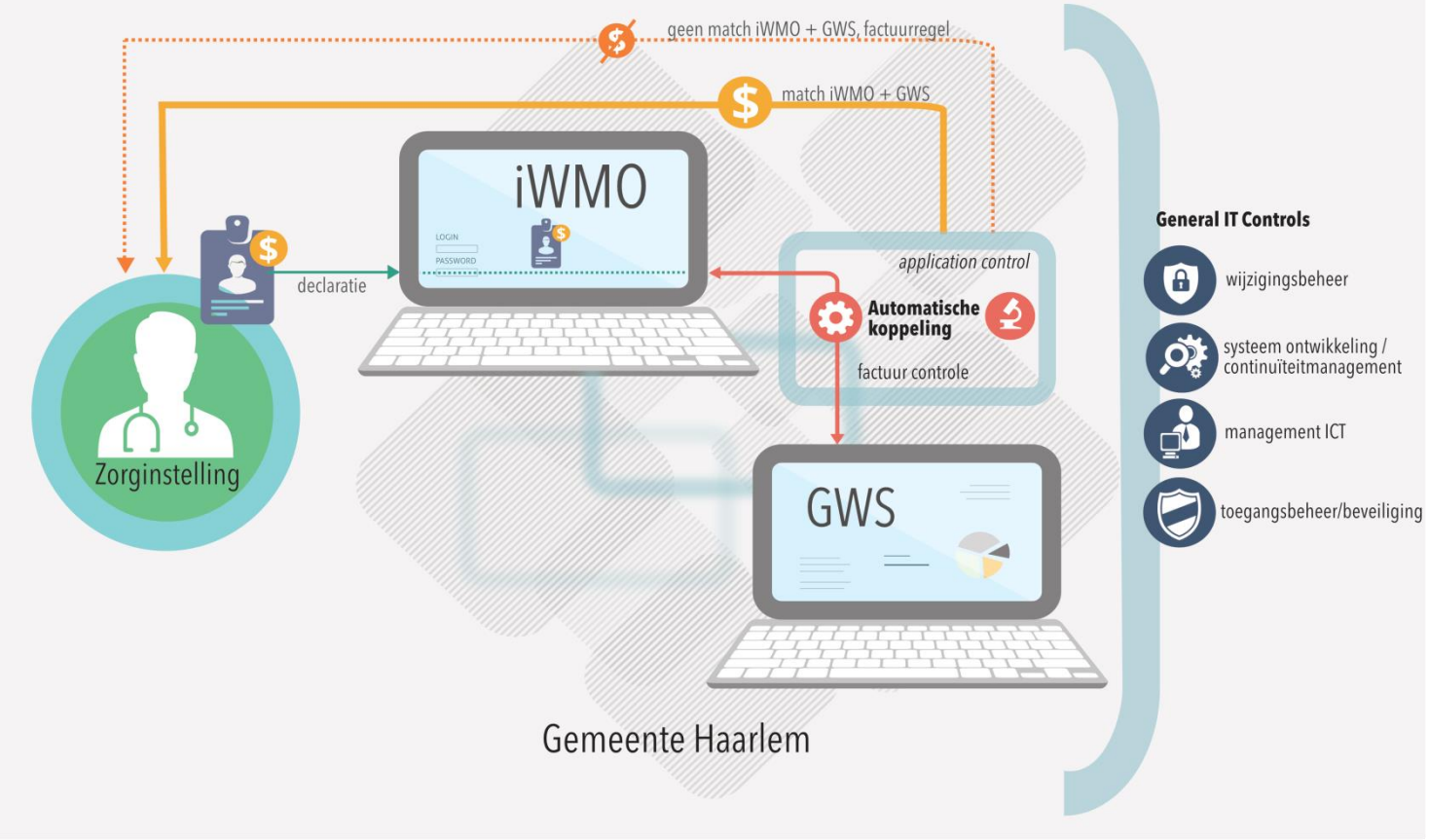
Gevolgen, de praktijk van de Gemeente

Wat betekent dit in de praktijk? Een goed voorbeeld in de Gemeente Haarlem waar het verband tussen application controls & general IT controls een rol speelt voor de volledige en accurate informatieverwerking, vinden we binnen het sociale domein. Met de transitie in het sociaal domein, heeft de gemeente er taken en verantwoordelijkheden bijgekregen, die gepaard zijn gegaan met een taakstelling en grote (privacygevoelige) datastromen (zie bovenstaand). De Gemeente erkent dat rol van ICT hierbij onmisbaar is.

Zo is de intentie van Gemeente Haarlem dat alle facturen door de zorgleveranciers/aanbieders worden aangeleverd in iWmo en de factuurcontrole middels een automatische koppeling (application control) tussen GWS en iWmo zal gaan plaatsvinden. Het wijzigingsbeheerproces met betrekking tot de applicatie gebruikt voor het sociaal domein, kan echter op dit moment niet worden vastgelegd (general IT control). Hierdoor bestaat het risico dat wijzigingen zonder goedkeuring of volledige testen direct

door functioneel beheer in de productieomgeving kunnen zijn gezet. Dit heeft mogelijk gevolgen voor de werking van de applicatie, gezien foutieve programmatuur in de productieomgeving kan worden gebruikt. De betrouwbaarheid van de data en de match tussen de binnenkomende facturen komen hierdoor in het geding. Als de gemeente in plaats van op handmatige factuur controles meer wilt steunen op dit soort geautomatiseerde processen/data dient de gemeente zorg te dragen dat de IT-randvoorwaarden (general IT & application controls) hier passend bij zijn. Zo constateerde het Audit Team van Gemeente Haarlem dat diverse controles noodzakelijk zijn om de betrouwbaarheid van het berichtenverkeer en de automatische factuurcontrole (matching) naar aanleiding hiervan vast te stellen. Oftewel om de benodigde inspanning om in control te zijn en blijven, te doen afnemen, zal de gemeente de trends op het gebied van data, control en IT moeten volgen en vervolgstappen moeten maken om de verschuiving te maken naar general & IT application controls.

Figuur 1: Voorbeeld Application - IT controls in het sociaal domein



Een andere realiteit van de-perimeterisation voor gemeenten is dat; naast de eigen IT omgeving van de gemeenten, accountants en IT-auditors bij de auditwerkzaamheden voor de jaarrekeningcontrole steeds vaker te maken met krijgen met cloudapplicaties die door externe dienstverleners worden beheerd voor de gemeente. Auditors willen binnen hun controlewerkzaamheden kunnen steunen op assurance rapporten van de dienstverleners en de integriteit van de data uit cloudapplicaties. Volgens kritische rapporten blijkt dat

accountants in de praktijk moeite hebben met de complexiteit die voorkomt bij het controleren van externe dienstverleners.

Kortom, de ontwikkelingen op het gebied van digitalisering en geassocieerde compliance eisen, dagen de gemeente uit om toe te werken aan een adequaat en betrouwbaar bestuur van informatiebeveiliging/voorziening. Gelijktijdig biedt deze trend ook kansen voor een efficiëntere interne beheersing.

Conclusie

Gezien de ontwikkelingen in het gemeentelijk domein zal de informatievoorziening een steeds grotere rol vervullen, ook op het gebied van control. De vraag is niet óf big en open data, cyber bedreigingen, cloud computing, en al die andere ontwikkelingen optreden. De vraag is hoe de gemeente hiermee moet omgaan. Voldoen aan de gestelde normen (KIDO, BIG) van het Rijk, self-compliant te zijn en blijven, adequaat inspelen op de bovengenoemde trends en het vormgeven van general/application controls vereist een betere en innovatieve verankering van IT binnen de gemeentelijke organisatie. Kortom het is voor de gemeente zaak dat zij haar processen zodanig inricht dat zij grip houdt op de veelheid aan informatie die zij produceert, beheert en deelt.

Positioneringsdocument B zet uiteen hoe Gemeente Haarlem de informatievoorziening kan verankeren binnen de organisatie.

Bijlage 1: Normkaders

In KIDO toelichting op normkaders.

NEN-ISO 27001	Managementsystemen voor informatiebeveiliging - Eisen
NEN-ISO 27002	Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging
NEN-ISO 27005	Information security risk management
NEN-ISO 27013	Guidance on the integrated implementation of 27001 and 27002
ISAE-3000	International Standard on Audit Engagements 3000 (ook wel COS/Richtlijn 3000)
NEN-ISO 15489	Informatie en documentatie - Informatie- en archiefmanagement
NEN 2082	Eisen voor functionaliteit van informatie- en archief-management in programmatuur
ISO 14721	referentiemodel voor een Open Archival Information System (OAIS)
NEN-ISO 30301	Informatie en documentatie - Managementsystemen voor archivering - Eisen
DUTO	normenkader Duurzaam Toegankelijke Overheidsinformatie

Bijlage 2: Dreigingsmatrix

Cybersecuritybeeld Nederland, CSBN 2016; uitgave van het Nationaal Cyber Security Centrum

Tabel 1 **Dreigingsmatrix**

	Doelwitten		
Bron van Dreiging	**Overheden**	**Private organisaties**	**Burgers**
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie
	Manipulatie van informatie	Manipulatie van informatie	Manipulatie van informatie
	Verstoring van ICT	Verstoring van ICT	Verstoring van ICT
	Overname van ICT	Overname van ICT	Overname van ICT
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	
Terroristen	Verstoring/overname van ICT	Verstoring/overname van ICT	
Cybervandalen en scriptkiddies	Diefstal van informatie	Diefstal van informatie	Diefstal van informatie ↘
	Verstoring van ICT ↗	Verstoring van ICT ↗	
Hacktivisten	Diefstal en publicatie van verkregen informatie ↗	Diefstal en publicatie van verkregen informatie ↗	
	Defacement	Defacement	
	Verstoring van ICT	Verstoring van ICT	
	Overname van ICT	Overname van ICT	
Interne actoren	Diefstal en publicatie of verkoop van verkregen informatie ↘	Diefstal en publicatie of verkoop van verkregen informatie ↘	
	Verstoring van ICT	Verstoring van ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal van informatie (bedrijfs-spionage)	Commercieel gebruik, misbruik of 'doorverkopen' van gegevens
Geen actor	Uitval van ICT	Uitval van ICT	Uitval van ICT
↘ ↗ *Verandering ten opzichte van CSBN 2015*	*Er worden geen nieuwe trends of fenomenen onderkend waar de dreiging van uitgaat. OF Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. OF Er hebben zich geen noemenswaardige manifestaties van de dreiging voorgedaan in de rapportageperiode*	*Er worden nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat. OF Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen. OF Incidenten hebben zich voorgedaan buiten Nederland, enkele kleine in Nederland.*	*Er zijn duideljke ontwikkelingen die de dreiging opportuun maken. OF Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. OF Incidenten hebben zich voorgedaan in Nederland.*

Voor overheden is de grootste dreiging momenteel gericht op vertrouwelijkheid van informatie en continuïteit van onlinedienstverlening (incl. generieke voorzieningen) en eigen ICT.