Zicht en grip op informatie

Auteur: Hugo Leisink
e-mail: hugo@leisink.net
www: https://www.ravib.nl/

5 april 2018

Goed informatiemanagement is noodzakelijk om informatie-beveiliging tot een succes te kunnen maken. Maak het beheren van informatie een belangrijk thema binnen de organisatie. Stel daartoe een informatiemanager aan, die een volwaardige partner is voor de ICT-manager in het spel van vraag en aanbod van ICT. Voer een periodiek overleg in tussen de informatiemanager, de ICT-manager, de Information Security Officer, de Privacy Officer en de CIO. Gebruik het applicatielandschapsoverzicht als beginpunt van deze gesprekken.

We lezen steeds vaker in het nieuws over het op straat komen te liggen van vertrouwelijke informatie, het (D)DoS-en van webdiensten, het op afstand overnemen van systemen en andere gelijksoortige incidenten. Informatiebeveiliging wordt steeds belangrijker. Het staat zelfs op de politieke agenda. We schenken steeds meer aandacht aan het beveiligen van vertrouwelijke en belangrijke informatie, maar het lijkt net zo vaak weer mis te gaan. Grip krijgen op informatiebeveiliging blijkt voor veel organisaties een uitdagende opgave.

De onderliggende uitdaging

Veel organisaties verwerken vandaag de dag veel informatie. In veel gevallen gaat het om bedrijfsgevoelige informatie of persoonsgegevens die goed moeten worden beveiligd. Echter, als onvoldoende duidelijk is om welke informatie het precies gaat, is het beveiligen van deze informatie een lastige of zelfs onmogelijke opgave. Zicht en grip op informatiebeveiliging vereist namelijk zicht en grip op de informatie zelf. Het hebben van zicht en grip op informatie vereist vele zaken, zoals

bijvoorbeeld weten om wat voor een soort informatie het gaat is, wat de waarde is van de informatie en waar die informatie zich bevindt. Maar ook welke verwerkingen en uitwisselingen plaatsvinden en wie daarvoor verantwoordelijk is. Dit alles valt onder de noemer informatiemanagement. Informatiemanagement vormt daarmee een noodzakelijke basis voor informatiebeveiliging.

Bij een organisatie waar informatiemanagement niet goed is ingericht, is de kans aanwezig dat de ICT-manager half op de stoel van de informatiemanager gaat zitten. Het risico daarvan is dat de ICT-beheerorganisatie levert wat niet echt door de organisatie gevraagd wordt of zelfs niet levert wat juist wel gevraagd wordt. Dat kan zijn uit gemakzucht, uit een kostenoverweging, vanwege kennis en/of capaciteitsgebrek, om bij te blijven qua techniek of omdat een bepaalde techniek leuk en uitdagend is voor techneuten. De ICT-beheerorganisatie heeft in die situatie te veel macht over ICT binnen de organisatie, waarbij de organisatie zich in bochten moet wringen om met de geleverde ICT haar werk te kunnen doen. Het gevaar daar weer van is dat medewerkers buiten de ICT-beheerorganisatie om zelfstandig ICT-zaken gaan inrichten of externe middelen gaan gebruiken, zoals Gmail of Dropbox. Het zicht op waar bedrijfsinformatie zich bevindt is dan nog meer zoek.

Dit artikel beschrijft het belang van informatiemanagement, welk voordeel een organisatie kan hebben van het goed inrichten daarvan en hoe dit kan helpen bij het aanpakken van informatiebeveiliging. Het is geschreven vanuit de belevingswereld van een informatiebeveiliger en bevat dus geen volledige beschrijving van wat informatiemanagement allemaal inhoudt.

De ondersteuning bij informatiebeveiliging

Goed ingericht informatiemanagement is noodzakelijk om informatiebeveiliging tot een succes te kunnen maken. Is informatiemanagement niet goed ingericht, dan ondervindt de persoon die verantwoordelijk is voor het inrichten van informatiebeveiliging daar hinder van. Hieronder volgt een overzicht van een aantal onderdelen van informatiemanagement die een Information Security Officer kunnen helpen bij het inrichten van informatiebeveiliging.

Systeemeigenaarschap

Voor ieder informatiesysteem dient iemand aangewezen te worden als formeel systeem-eigenaar. Dit is bij voorkeur een lijnmanager met voldoende bevoegdheid (tijd, inzet van personeel en budget) om zaken rondom beheer in te (laten) richten. Het niet invullen van het eigenaarschap voor de informatiesystemen houdt in dat een Information Security Officer geen aanspreekpunt heeft om de beveiliging van een informatie-systeem te bespreken. Informatie- systemen hebben daardoor mogelijk niet het noodzakelijke of gewenste beveiligingsniveau. In de praktijk gebeurt het vaak dat meerdere managers zeggen eigenaar te zijn bij vragen over wie wat mag met de in het systeem opgeslagen informatie, maar een andere kant op kijken in het geval van problemen of bij vervelende vragen, zoals vragen over informatiebeveiliging.

Veel organisaties maken gebruik van cloudservices voor hun ICT. De veronderstelling dat eigenaarschap daarbij niet meer nodig is, is onjuist. Het gaat namelijk niet om de systemen, maar om de informatie in die systemen. De informatie dient ook bij cloudservices nog steeds een eigenaar te hebben. Het gebruikelijke woord systeemeigenaar is dan ook misleidend. Informatie-eigenaar zou eigenlijk een betere term zijn.

Een systeemeigenaar is verantwoordelijk voor het organiseren van de volgende zaken rondom het goed en veilig omgaan met informatie:

- **Goed afgestemd SLA:** Een systeemeigenaar is verantwoordelijk voor een informatiesysteem in het geheel, maar legt de taak van het up-and-running houden van het systeem meestal neer bij de ICT-beheerorganisatie of de SAAS-leverancier. Echter, het is en blijft de verantwoordelijkheid van de systeemeigenaar om daarover juiste afspraken te maken. Afspraken over beschikbaarheid, frequentie van het maken van backups, hoelang het maximaal mag duren om een gecrashte applicatie weer werkend te krijgen en hoeveel dat dan mag kosten zijn daar belangrijke onderdelen van. Zeker met een interne ICT-afdeling kan het

voorkomen dat voor informatiesystemen geen expliciete afspraken worden gemaakt en dus de standaard SLA gehanteerd wordt, maar waarbij systeemeigenaren eigenlijk geen beeld hebben van wat die standaard SLA vervolgens inhoudt. Een incident met een kritische applicatie zorgt dan voor grotere problemen dan nodig is.

- **Noodplannen:** Zoals hierboven beschreven behoort een systeemeigenaar afspraken te maken met een ICT-beheerorganisatie over de beschikbaarheid van een applicatie. Daarin staat hoe vaak en voor hoe lang een systeem voor onderhoud of voor welke reden dan ook, offline mag zijn. Ook worden afspraken gemaakt over hoe snel en met hoeveel moeite een ICT-beheerorganisatie aan de slag moet op het moment dat een applicatie crasht of ongepland offline gaat. Echter, het kan gebeuren dat een applicatie een probleem heeft waar de ICT-beheerorganisatie niks aan kan doen, maar waardoor de SLA niet waargemaakt kan worden. Daarnaast houdt een ICT-beheerorganisatie zich alleen maar bezig met de beschikbaarheid van een applicatie, niet met de integriteit of vertrouwelijkheid van de in het systeem opgeslagen informatie. In geval van problemen met de beschikbaarheid waarbij de SLA niet waargemaakt kan worden of problemen met de integriteit en/of vertrouwelijkheid van de informatie, is sprake van een incident. Om goed met een incident om te kunnen gaan, om in andere woorden goed weerbaar te zijn, is het verstandig om een noodplan te hebben. Dit dwingt je om na te denken over wie en wat geraakt wordt door het uitvallen van de applicatie. Bijvoorbeeld wie wat gaat doen om het probleem aan te pakken en welke interne en externe communicatie je doet. Of wat nodig is om tijdelijk zonder de applicatie verder te kunnen werken en wat nodig is om na het weer beschikbaar komen van de applicatie nodig is om de resultaten van het offline werken weer op te nemen in de applicatie. Zonder zo'n noodplan bestaat de kans dat door de uitval van een systeem onnodige problemen ontstaan en deze problemen groter worden en langer duren dan noodzakelijk is. Een Information Security Officer kan door het ontbreken van noodplannen lastiger inschatten of een organisatie goed is voorbereid op incidenten.

- **Voldoen aan de privacywetgeving:** Sinds 2001 heeft Nederland een wet ter bescherming van persoonsgegevens, de Wbp. Sinds 2016 is deze wet uitgebreid met o.a. regelgeving over het melden van datalekken en is een Europese wet, de Algemene Verordening Gegevens-bescherming (AVG), van kracht die de Wbp in mei 2018 gaat vervangen. Om zaken goed op orde te hebben wat betreft deze wetgeving, zoals een rechtmatige verwerking, respecteren van de rechten van de betrokkenen, goede beveiliging, etc, is het belangrijk dat iedere systeemeigenaar dit voor zijn of haar applicaties zelf organiseert. Zij zijn namelijk als eigenaar verantwoordelijk voor de in die applicaties opgeslagen informatie. Verwachten dat een Privacy Officer of Information Security Officer dit oppakt is niet terecht, want zij beschikken niet over het juiste mandaat. Eén van hen dat mandaat geven is de verkeerde aanpak, want dan krijg je twee kapiteins met verschillende belangen op één schip. Bij een incident met privacygevoelige informatie loopt de organisatie het risico op een flinke boete vanuit de Autoriteit Persoonsgegevens (AP), indien je je zaken niet aantoonbaar op orde hebt. Zicht op de verwerking van persoonsgegevens (een vereiste volgens artikel 30 van de AVG) is een belangrijke eerste stap in het voorkomen van een datalek.

- **Toegang tot een applicatie:** Bepalen wie toegang krijgt tot (delen van) een applicatie, is bij uitstek een taak van iemand die verantwoordelijk is voor de in die applicatie opgeslagen informatie en die tevens kennis heeft van de waarde van deze informatie. Deze persoon is niemand minder dan de systeem-eigenaar. Het is dan ook zijn of haar taak om de toegangscriteria op te stellen en te regelen dat deze bij het toekennen en voor het intrekken van toegangsrechten worden gehanteerd. Bij het niet goed inrichten van de toegang tot applicaties loopt de organisatie het risico dat meer medewerkers toegang hebben tot bedrijfsvertrouwelijke of privacygevoelige informatie dan wenselijk of wettelijk toegestaan is.

- **Documentatie:** Voor een informatiesysteem is vaak tal van documentatie beschikbaar. Denk aan een functioneel en technisch ontwerp bij

zelfbouw, een installatiehandleiding, beheerhandleiding en gebruikershandleiding. Bij voorkeur wordt dit soort documentatie centraal beheerd, maar het is de verantwoordelijkheid van een systeemeigenaar om deze documentatie bij ontwikkeling of aanschaf te (laten) verzamelen en aan de juiste persoon aan te (laten) leveren. Daarnaast verzamelen medewerkers (zowel beheerders als gebruikers) een hoop kennis. Het is niet onverstandig om ook deze kennis te laten documenteren. Maar weinig mensen realiseren zich hoeveel kennis een organisatie kan verlaten bij de uitdiensttreding van een medewerker.

Overzicht applicatielandschap

Een ICT-beheerorganisatie heeft vaak een overzicht van haar digitale infrastructuur. Daarop staan servers, routers, firewalls, etc. aangegeven. Dit is echter onvoldoende voor een Information Security Officer om zicht te krijgen op de informatie-voorziening. Een Information Security Officer houdt zich namelijk op de eerste plaats bezig met het beveiligen van informatie, niet van hardware. Een applicatielandschapsoverzicht is dan ook een heel ander soort overzicht. In een applicatie-landschap staat de informatie en het gebruik en de uitwisseling van deze informatie centraal. Het niet hebben van een applicatielandschapsoverzicht maakt het voor een Information Security Officer lastig om te achterhalen welke informatie een organisatie in huis heeft en waar zijn aandacht qua beveiliging naar toe moet gaan.

Vanwege het belang van het hebben van een goed overzicht van het applicatielandschap, wordt dit onderwerp in een later hoofdstuk verder toegelicht.

Informatie en processen

Veel van de informatie waar we vandaag de dag mee werken bestaat in digitale vorm. Waar bijvoorbeeld vroeger een gemeenteambtenaar een papieren dossier tevoorschijn haalde bij een bezoek aan het gemeentehuis, treffen we nu een gemeenteambtenaar achter een PC aan. Met behulp van de ICT-beheerorganisatie is de

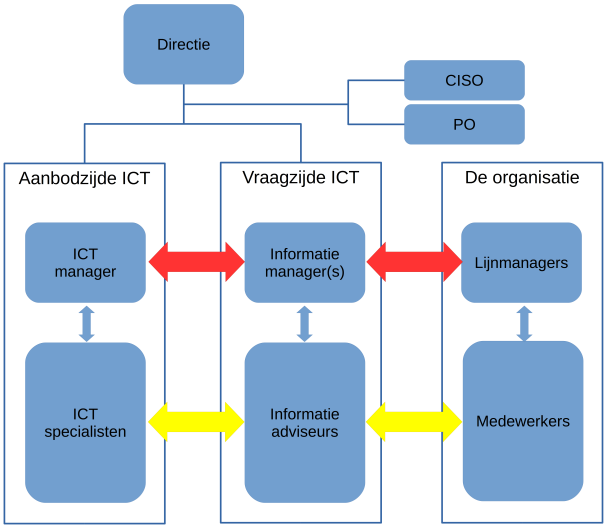
beschikbaarheid van informatie veranderd van een analoge vorm naar een digitale vorm. De transitie van analoge informatie naar digitale informatie is bij de meeste organisaties voor het belangrijkste deel wel voltooid.

Al vele jaren is er ook een andere transitie gaande. In plaats van langsgaan bij het gemeentehuis, bestaat voor veel zaken ook de mogelijkheid om dit te regelen via de website van de gemeente. Niet alleen informatie is gedigitaliseerd, ook processen worden dus steeds meer gedigitaliseerd. Maar waar een ICT- beheer-organisatie de juiste partij is voor het digitaliseren van informatie, is dat niet het geval voor het digitaliseren van processen. Een ICT- beheer-organisatie gaat immers alleen over de beschikbaarheid van informatie. Voor het digitaliseren van processen is meer kennis nodig, namelijk kennis over de organisatie en de processen zelf. Dit is het werkterrein van informatiemanagement.

Door onvoldoende kennis over het verschil tussen het digitaliseren van informatie en het digitaliseren van processen, kijken organisaties onterecht naar de ICT-beheerorganisatie voor ondersteuning bij het digitaliseren van processen. Organisaties blijven dus teveel leunen op de ICT- beheer-organisatie, terwijl ze feitelijk met informatie-management aan de slag moeten gaan.

Organiseren van de informatievoorziening

Het helder definiëren van de verschillende taken en verantwoordelijkheden en het beleggen daarvan bij de juiste personen, is belangrijk bij het op orde krijgen van informatiemanagement binnen de organisatie. Zorg daarbij voor een goede verdeling tussen de vraagzijde en de aanbodzijde van ICT. De ICT-manager is verantwoordelijk voor de inrichting en organisatie van de aanbodzijde en de informatiemanager is verantwoordelijk voor de inrichting en organisatie van de vraagzijde. De informatiemanager brengt de behoefte aan informatievoorzieningen vanuit de organisatie in kaart. Deze behoefte is het uitgangspunt voor een gesprek tussen de informatiemanager en de ICT-manager. De ICT-manager beperkt de levering van ICT tot wat nodig is om aan de vraag te kunnen voldoen.



Figuur 1: Inrichting van informatievoorziening

De strategische keuzes rondom informatie-voorziening en ICT worden gemaakt door de directie, in nauw samenspraak met de informatie-manager en de ICT-manager. De directie is en blijft eindverantwoordelijke voor zowel informatie-management als informatiebeveiliging. Een van de directieleden (in de praktijk vaak de CIO of de CFO) is vanuit de directie aanspreekpunt voor informatiemanagement en informatiebeveiliging.

De tactische keuzes worden gemaakt door de informatiemanager, de ICT-manager en de lijnmanagers (rode pijlen uit figuur 1). De Information Security Officer (ISO) en de Privacy Officer (PO) adviseren daarbij op het gebied van informatiebeveiliging en privacy en zijn staffuncties van de directie. Zowel de ICT-manager als de informatiemanager worden op gelijke hoogte in de organisatie geplaatst, namelijk direct onder de directie.

De concrete, operationele keuzes worden gemaakt door de ICT-specialisten en de informatieadviseurs, waarbij zij nauw contact hebben met de mede-werkers die uiteindelijk met de oplossing aan de slag zullen gaan (gele pijlen uit figuur 1). Het is zeer belangrijk dat de mensen uit alle kolommen goed met elkaar in contact blijven, zodat de juiste keuzes gemaakt worden (blauwe pijlen uit figuur 1).

De kans is aanwezig dat de ICT-manager door deze nieuwe werkwijze minder vrijheid heeft in de levering van ICT of minder verantwoordelijkheid heeft dan in de oude werkwijze. Om problemen in de onderlinge verstandhoudingen te voorkomen, dient zo'n transitie op een zorgvuldige en tactische wijze te worden aangepakt.

Binnen de organisatie dient afgesproken te worden dat iedere vraag op het gebied van ICT of informatievoorziening via een informatieadviseur loopt. Een informatieadviseur zorgt ervoor dat de vraag op een goede en heldere omschreven manier vast komt te liggen, dat voldaan wordt aan het ICT-beleid, informatiebeveiligingsbeleid en het privacybeleid en dat de ICT-oplossing voldoende toekomstbestendig is. Hierdoor draagt een informatieadviseur bij aan de kwaliteit van de informatievoorziening, waardoor kosten en tijd bespaard worden.

Vastleggen van het applicatielandschap

Zoals eerder gesteld is het hebben van zicht op de informatie zelf, noodzakelijk om deze goed te kunnen beveiligen. Het maken van een overzicht van het applicatielandschap is slechts één van de taken die hoort bij informatiemanagement. Maar omdat zo'n overzicht een goed startpunt is voor informatiemanagement en een goed hulpmiddel bij de verdere aanpak daarvan, is dit een belangrijk onderdeel. Om die reden wordt dit onderdeel hier apart besproken.

Hoewel gesproken wordt over een applicatie-landschap, gaat het daarbij niet zozeer om de applicaties, maar om de informatie die in deze applicaties opgeslagen ligt. Het zou dus beter zijn om te spreken van een informatielandschap. Echter, de meeste informatie zit vandaag de dag opgeslagen in applicaties. Om die reden spreekt men van een applicatielandschap. Echter, het is uiteraard toegestaan om zaken waar informatie in opgeslagen ligt maar wat geen applicatie is, zoals een papieren archief, in het overzicht op te nemen.

Zicht op de eigen informatieverwerking kan het beste verkregen worden door een organisatie-breed applicatielandschapsoverzicht te maken. In zo'n overzicht dient de volgende informatie opgenomen te worden:

- **Applicaties:** Het overzicht bevat een lijst van alle applicaties binnen de organisatie. Een applicatie die, vanwege bijvoorbeeld capaciteitsredenen of

De auteur heeft in het verleden gezocht naar een hulpmiddel om een applicatielandschap in vast te kunnen leggen. De software die hij hierbij is tegengekomen was prijzig, ingewikkeld qua gebruik of bood geen mogelijkheid om het applicatielandschap op een makkelijke manier te delen met de rest van de organisatie. Om die reden besloot hij zelf de benodigde software te ontwikkelen en deze als gratis en open source software aan te bieden. Met deze software is het al mogelijk een applicatielandschap vast te leggen, maar de software bevindt zich nog wel in de beta-status. Het schrijven van deze software vormt namelijk onderdeel van zijn zoektocht naar op welke wijze een applicatielandschap het beste vastgelegd kan worden.

De software van Gitlab te downloaden via https://gitlab.com/hsleisink/landscape. Een demo-omgeving is te bekijken op https://landscape.leisink.net/, met 'demo' als gebruikersnaam en wachtwoord.

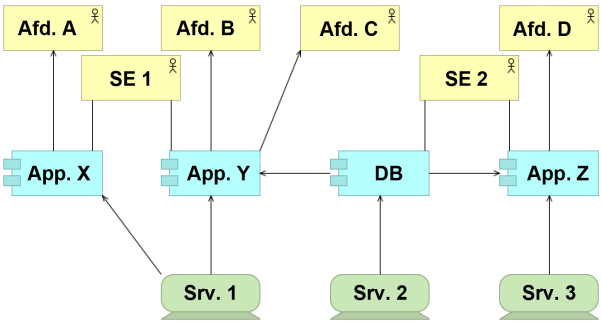
geografische redenen, meervoudig is geïmplementeerd, wordt slechts eenmaal genoemd. Per applicatie wordt aangegeven welke informatie daarin opgeslagen ligt en de classificatie voor beschikbaarheid, integriteit en vertrouwelijkheid die daarbij geldt. Voor iedere applicatie wordt opgegeven welke koppeling deze heeft met een andere applicatie, welke informatie daarbij wordt uitgewisseld, in welk formaat en via welk protocol, hoe vaak en om welke reden dit gebeurt. In dit overzicht kan ook de verwerking van persoonsgegevens opgenomen worden, zoals vereist in artikel 30 van de Algemene Verordening Gegevensbescherming.

- **Dataverzamelingen:** Met name fileserver systemen bevatten meerdere op zichzelf staande stukken informatie, waardoor het niet handig is om zo'n systeem in z'n geheel te beoordelen. Neem deze stukken informatie apart op in het overzicht, vermeld daarbij op welk informatie-systeem deze informatie zich bevindt, wat de classificatie is en wie de eigenaar en de gebruikers zijn.

- **Business:** Hierbij wordt aangegeven welke afdelingen gebruik maken van welke applicatie of wie de systeemeigenaren zijn van de verschillende applicaties. Deze informatie is noodzakelijk om bij een (beveiligings)incident tijdig de betrokken afdelingen en verantwoordelijken te kunnen waarschuwen.

- **Hardware:** Het opnemen van een lijst van de (virtuele) hardware waar de applicaties op draaien, is puur om te zien welke applicaties op dezelfde hardware draaien. Deze informatie is belangrijk bij het maken van een impactanalyse in het geval van een (beveiligings)incident met een applicatie of server.

Managers hebben vaak weinig tot geen technische ICT-kennis. Door een applicatielandschap op deze manier vast te leggen, is de werking van de informatievoorziening binnen een organisatie ook aan hen uit te leggen. Het applicatielandschap kan gebruikt worden om aandacht te vragen voor zaken die inzet en/of geld nodig hebben. Hierdoor is het voor managers mogelijk om te sturen op informatiebeveiliging en privacyzaken.



Figuur 2: Voorbeeld van een schematisch applicatielandschapsoverzicht

In figuur 2 is een voorbeeld applicatielandschap volgens de eerdere gegeven beschrijving schematisch weergegeven.

Is bijvoorbeeld applicatie Y uit figuur 2 gehackt, dan is het voor een manager zonder zo'n overzicht lastig om daarop te sturen. Maar met zo'n overzicht kan hij, zonder verstand te hebben van alle techniek, vragen naar de impact voor afdeling B en C, of de hack via server 1 ook invloed heeft op applicatie X en dus op afdeling A, of de hack

eventueel via de database ook vloed heeft op applicatie Z en dus op afdeling D en met de verantwoordelijk systeemeigenaren praten over de impact en het afhandelen van het incident. Dus door zicht op de informatievoorziening is hij in staat om te sturen op informatiebeveiliging.

Samenvattend

Goed informatiemanagement is noodzakelijk om informatiebeveiliging tot een succes te kunnen maken. Maak het beheren van informatie een belangrijk thema binnen de organisatie. Stel daartoe een informatiemanager aan, die een volwaardige partner is voor de ICT-manager in het spel van vraag en aanbod van ICT. Voer een periodiek overleg in tussen de informatiemanager, de ICT-manager, de Information Security Officer, de Privacy Officer en de CIO. Gebruik het applicatielandschapsoverzicht als beginpunt van deze gesprekken.

Over de auteur

Hugo Leisink is senior adviseur bij het Nationaal Cyber Security Centrum. Hij is bereikbaar via hugo@leisink.net. Dit artikel is op persoonlijke titel geschreven.