CIO Platform Nederland

CAT Data Classification & CEG Information Security

Handleiding Dataclassificatie

Publicatie van
CAT Data Classification & CEG Information Security

CIO Platform Nederland, december 2016

CIO Platform Nederland

CAT Data Classification & CEG Information Security

Opstellers & redactie

Stoffel Bos (Prorail), Hein Laan (Rabobank), Ronald Verbeek (CIO Platform Nederland)

Leeswijzer

Dit document bevat een good practice voor (data)classificatie. Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan.

Doelgroep

Dit document is van belang voor systeemeigenaren, informatiemanagers en (Corporate) information security officers.

Dankbetuiging

Onze dank gaat uit naar het Kwaliteitsinstituut Nederlandse Gemeenten wiens Handreiking Dataclassificatie gediend heeft als bron voor dit document.

Inhoudsopgave

1. Inleiding

Doelstelling handreiking

Deze classificatie handleiding beschrijft een good practice voor classificatie van informatie. Het biedt handvatten om een classificatiesysteem te ontwikkelen of te verbeteren en deze te implementeren.

We praten alleen over classificatie, maar rubricering wordt binnen het vakgebied ook vaak gebruikt. Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan. Classificatie gaat in dit geval niet dieper dan een proces of een systeem.

De in deze handleiding genoemde niveaus en (bewaar)termijnen zijn een voorstel en komen uit verschillende brondocumenten, waaronder: wetgeving, PVIB patronen en de handreiking Dataclassificatie van de Nederlandse Gemeenten.

Classificatie van data is nodig om te kunnen bepalen welke maatregelen genomen moeten worden om die data adequaat te beschermen en geeft ook antwoord op de vraag of de data binnen of buiten de baseline valt.

Belang van classificatie

De mogelijke schade die een dreiging (bijv. misbruik door oneigenlijke toegang) kan toebrengen aan bepaalde informatie en de kans dat het optreedt, kan met een risicoanalyse worden geëvalueerd. Het management dient aan te geven welke risico's aanvaardbaar zijn en welke met maatregelen moeten worden afgedekt. De voorgestelde classificatiemethodiek geeft een snelle indicatie van het belang van de informatie(systemen) en is daarmee een basis voor een risicoanalyse.

Na de classificatie kunnen de juiste maatregelen getroffen worden waardoor enerzijds inbreuken op de veiligheid worden voorkomen en anderzijds niet nodeloos veel inspanning benodigd is.

2. Classificatie van informatie en systemen

Informatiebeveiliging is het geheel van maatregelen en procedures om informatie te beschermen. Het doel is: *waarborgen van de continuïteit, integriteit en vertrouwelijkheid van informatie en de informatievoorziening en het beperken van de gevolgen van eventuele beveiligingsincidenten.*

Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie (verwerkende systemen):

- **Beschikbaarheid**: hoeveel en wanneer data toegankelijk is en gebruikt kan worden. Te onderscheiden niveaus zijn: *Basaal, Laag, Midden, Hoog danwel 0,1,2,3*
- **Integriteit**: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). Te onderscheiden niveaus zijn: *Onbekend, Laag, Midden, Hoog danwel 0, 1,2,3 (Onbekend, Aangenomen Correct, Geverifieerd Correct, Bewezen Correct)*
- **Vertrouwelijkheid**: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. Te onderscheiden niveaus zijn: *Publiek, Laag, Midden, Hoog danwel 0,1,2,3*

De hierboven gebruikte niveaus zijn gebaseerd op NORA: Nederlandse Overheid Referentie Architectuur. De baseline is doorgaans B,I,V = L,L,L

Met het toekennen van classificatieniveaus aan data en/of informatiesystemen maken we het (vereiste) beschermingsniveau kenbaar. Aan de hand hiervan bepaal je welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. De volgende factoren oefenen invloed uit op de adequate beveiligingsmaatregelen: beleidsuitgangspunten, architectuurprincipes, beveiligingseisen (en hoe deze te interpreteren).

Met een classificatiemethode bepaal je of het proces of systeem binnen of buiten de baseline valt. Indien de classificatie hoger dan vertrouwelijk is, zijn extra maatregelen nodig. Soms zijn deze maatregelen al genomen als application control (binnen de applicatie). Soms zijn ze al uitgewerkt door een uitgevoerde risicoanalyse of wordt er binnen de organisatie een risicoafweging gemaakt door het uitvoeren van een risicoanalyse met als resultaat meer passende maatregelen.

2.1 Risicoanalyse & restrisico's

Een organisatie die informatie verwerkt en daarbij informatiesystemen gebruikt loopt bepaalde risico's doordat die informatie en systemen kwetsbaar zijn voor dreigingen van binnen en van buiten.

Het uitvoeren van een risicoanalyse ondersteunt het management bij het vaststellen van de risico's die worden gelopen en hoe groot die risico's zijn. Daarmee wordt vervolgens bepaald welke beveiligingsmaatregelen getroffen moeten worden om de risico's terug te dringen. Vooral bij de vertaling van risico naar maatregel is classificatie een belangrijk hulpmiddel om de ernst van een risico en de reikwijdte van een maatregel te kunnen bepalen. De voorgestelde Classificatie handreiking kan beschouwd worden als een vereenvoudigde vorm van een risicoanalyse.

Bij een risicoanalyse worden bedreigingen benoemd en in kaart gebracht. Per bedreiging wordt de kans van het optreden ervan bepaald en wordt vervolgens berekend wat de schade is die op zou kunnen optreden als een bedreiging zich daadwerkelijk voordoet.

Na de analyse wordt vastgesteld op welke wijze de risico's beheerst kunnen worden, of teruggebracht tot een aanvaardbaar niveau: het treffen van informatiebeveiligingsmaatregelen. Daarbij wordt naast een risicoanalyse ook een kosten en baten analyse uitgevoerd. Op voorhand hoeft niet ieder risico te worden afgedekt: wanneer de kosten van de maatregelen om een risico te beperken hoger zijn dan de mogelijke schade, kan door de eigenaar van de gegevens besloten worden het risico te accepteren.

3. Beleidskaders voor classificatie

In dit hoofdstuk worden aanvullende beleidskaders als voorbeeld weergegeven welke als apart beleid naast het informatiebeveiligingsbeleid van de organisatie uitgegeven kunnen worden.

Voorbeeld beleid:

Het informatiebeveiligingsbeleid van <naam organisatie> beschrijft globaal de normen voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
De onderscheiden niveaus van beschikbaarheid zijn:

- **Basaal:** De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. On beschikbaarheid heeft geen gevolgschade.
- **Laag:** De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Onbeschikbaarheid kan enige (in)directe schade toebrengen
- **Midden:** De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Onbeschikbaarheid kan serieuze (in)directe schade toebrengen.
- **Hoog:** De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Onbeschikbaarheid kan (zeer) grote schade toebrengen.

De onderscheiden niveaus van integriteit zijn:

- **Onbekend**: Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
- **Laag**: Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-)fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van deze classificatie kan enige (in-)directe schade toebrengen
- **Midden**: Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-) fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- **Hoog**: Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen

De onderscheiden niveaus van vertrouwelijkheid zijn:

- **Publiek**: Alle informatie die algemeen toegankelijk is voor een ieder. Er is geen schending van deze classificatie mogelijk.
- **Laag**: Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.
- **Midden**: Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- **Hoog:** Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.

Labeling van Documenten naar aanleiding van het bovenstaande wordt doorgaans: Publiek, Intern, Vertrouwelijk, Geheim.

4. Principes voor classificatie

De volgende principes zijn het uitgangspunt voor (data) classificatie:

1. De eigenaar van de gegevens (veelal ook de proceseigenaar) bepaalt het vereiste beschermingsniveau (classificatie). Wettelijke eisen worden expliciet aangegeven. De eigenaar van de gegevens bepaalt wie toegang krijgt tot welke gegevens.
2. We streven naar een zo 'laag' mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bij de overheid, als voorbeeld, dient informatie voor zoveel mogelijk mensen beschikbaar te zijn in het kader van transparantie.
3. De classificatietabel heeft betrekking op alle gegevensverzamelingen, gegevensdragers, informatiesystemen.
4. Onderdelen in een keten kunnen een verschillend classificatieniveau hebben. Maatregelen worden gebaseerd op het component met de hoogste classificatie in die keten.
5. Het object van classificatie is informatie. De classificatie die door de soort informatie bepaald wordt geldt ook voor het hogere niveau van informatiesystemen (of informatieservices), dat wil zeggen dat als een systeem geheime informatie verwerkt, het hele systeem als geheim wordt aangemerkt tenzij voor dat hogere niveau maatregelen genomen zijn binnen het informatiesysteem. Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de eigenaren en dienen jaarlijks gecontroleerd te worden door de CISO.

In alle gevallen kan de eigenaar van de gegevens zich voor het classificeren laten ondersteunen door beveiligingsspecialisten, zoals de (Corporate) Information Security Officer. Het uitgangspunt is de Baseline Informatiebeveiliging die binnen een organisatie moet zijn vastgesteld. Als meer maatregelen nodig zijn dan dienen deze te worden afgestemd op de risico's, waarbij men rekening dient te houden met technische mogelijkheden en de kosten van de te nemen maatregelen. Dit is vaak situatie-afhankelijk.

Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld.

5. Beveiligingseisen per classificatieniveau

5.1 Beschikbaarheid

Beschikbaarheid stelt in tegenstelling tot integriteit en vertrouwelijkheid geen eisen aan de inhoud van de data. Er gelden daarom geen bijzondere maatregelen voor authenticatie, autorisatie, monitoring en beveiliging, zoals voor integriteit en vertrouwelijkheid. Aangezien de normen voor beschikbaarheid verschillen per serivce moet het classificatieniveau voor beschikbaarheid altijd worden gespecificeerd.

Definitie

Beschikbaarheid is gedefinieerd als 'eigenschappen van het geheel van ICT-diensten, systemen, componenten en gegevensdragers die van invloed zijn op de tijd dat het product of de dienst (en daarmee informatie) beschikbaar is voor de geautoriseerde gebruiker, op de momenten dat het beschikbaar moet zijn'. Beschikbaarheid wordt gemeten aan de hand van de Mean Time Between Failures (MTBF). Dit is de gemiddelde tijd tussen het herstel van het ene incident en het optreden van het volgende incident. De in de onderstaande tabel genoemde waarden zijn een voorbeeld, deze waarden moeten door de organisatie zelf bepaald worden.

Beschikbaarheidsnormen

De normen voor de Kantoor Automatisering (KA), Intranet van <naam organisatie> en de toegevoegde diensten zijn *(let op, dit kan per systeem / klasse worden ingevuld)*:

- KA (basis en plus applicaties): 99,5% beschikbaarheid op werkdagen tussen 7:30 en 18:00
- Intranet <organisatienaam>: 99,5% beschikbaarheid op werkdagen tussen 7:30 en 18:00

Klasse Noodzakelijk		
Werktijden	Van 08:00 tot 17:00 uur op maandag t/m vrijdag behoudens algemeen erkende feestdagen.	
Beschikbaarheid tijdens werktijd	99,6%	(min.)
Beschikbaarheid buiten werktijd	96,1%	(min.)
MTBF	100 dagen	(min.)
MTTR (voor storingen langer dan 3 minuten)	4 uur	(max.)
Aantal storingen:		
3 Minuten of korter	4 per maand	(max.)
Langer dan 3 minuten	1 per maand	(max.)

Klasse Belangrijk		
Werktijden	Van 07:00 tot 21:00 uur op maandag t/m vrijdag behoudens algemeen erkende feestdagen.	
Beschikbaarheid tijdens werktijd	99,6%	(min.)
Beschikbaarheid buiten werktijd	96,1%	(min.)

Klasse Essentieel		
Werktijden	24 uur per dag, 7 dagen per week, behoudens gepland onderhoud.	
Beschikbaarheid	99,9%	(min.)
MTBF	200 dagen	(min.)
MTTR (voor storingen langer dan 3 minuten)	4 uur	(max.)
Aantal storingen:		
3 Minuten of korter	1 per maand	(max.)
Langer dan 3 minuten	1 per halfjaar	(max.)

5.2 Integriteit

Het onderwerp integriteit valt in twee delen uiteen: de integriteit van data communicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het organisatie proces zelf), en de integriteit van de informatie in de applicaties of fysiek (d.w.z. gerelateerd aan het organisatieproces zelf). Integriteit gekoppeld aan de applicatie is altijd situatie afhankelijk en afhankelijk van de eisen van een specifiek proces. Voor de functionele integriteit van de informatievoorziening wordt een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Definitie

Integriteit geeft de mate aan waarin de informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en tijdigheid van de transacties.

Beveiligingsnormen

Onderstaande tabel beschrijft de beveiligingseisen (en maatregelen) per classificatieniveau, onderverdeeld in eisen voor authenticatie, autorisatie, monitoring en beveiliging. De bewaartermijnen zijn indicatief. Deze hangt af van de regels binnen het bedrijf en wetgeving zoals de Archiefwet.

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Onbekend	Geen	Geen	Geen	Geen
Laag	Authenticatie 'basis' vereist.	Autorisatie vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van 1/2 jaar.[1]	Inputvalidatie. Controleren op mutatie tijdens transport. Transportbeveiliging of berichtbeveiliging. Gegevens: Versie van gebruikte gegevens is bekend. [2] [3] Na uitvoering van een service blijven gewijzigde gegevens consistent.
Midden	Authenticatie 'midden' vereist.	Autorisatie vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van maximaal 2 jaar of langer bij vermoeden beveiligingsincident.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Gegevens: Versie van gebruikte gegevens is bekend. Wijzigingen alleen op bron. Na uitvoering van een service blijven gewijzigde gegevens consistent.
Hoog	Authenticatie 'hoog' vereist. Sterke Authenticatie verplicht.	Autorisatie vereist. 4- ogen principe vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van minimaal 3 jaar bij vermoe-den beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Gegevens: Gegevens worden niet buiten hun bron opgeslagen (behalve voor beschikbaarheid~) en niet buiten hun bron gewijzigd. Na uitvoering van een service blijven gewijzigde gegevens consistent.

De authenticatieniveaus verwijzen naar het vereiste beveiligingsmechanisme:

[1] Voor zover niet in strijd met wetgeving wat betreft de vastlegging van gegevens.
[2] Het gaat om de bron van de gegevens of een kopie van de gegevens en het tijdstip van de gebruikte gegevens.
[3] Regels met betrekking tot gegevensuitwisseling met derden worden gedefinieerd in een leveringscontract. Hierin komen ook regels met betrekking tot integriteit en vertrouwelijkheid aan bod.

- **Basis**: authenticatie gebaseerd op iets wat men weet (naam/wachtwoord).
- **Midden**: authenticatie gebaseerd op iets wat men weet en iets wat men heeft (bijv. een token, smartcard of certificaat).
- **Hoog**: authenticatie gebaseerd op eigenschap, bijvoorbeeld irisscan of vingerafdruk.

De autorisatieniveaus verwijzen naar de wijze waarop de controle wordt uitgevoerd. Vanaf 'beschermd' (basis en midden) is altijd autorisatie verplicht en vanaf 'hoog' komt daar het 4-ogen principe bij. Het 4-ogen principe bestaat uit één persoon die vastlegt en één persoon die fiatteert.

In de kolom 'Monitoring' wordt bij de niveaus 'beschermd' en 'hoog' de term 'relevant' gebruikt. Welke gegevens 'relevant' zijn, is ter beoordeling van de eigenaar. Voorbeelden en richtlijnen voor relevante gegevens zijn stamgegevens (gegevens waarop andere gegevens gebaseerd zijn), gegevens in basis- en kernregistraties, privacygevoelige informatie en gegevens beschermd door wet- en regelgeving.

Bij datatransport is berichtbeveiliging te prefereren boven transportbeveiliging. Echter, transportbeveiliging kan in bepaalde gevallen eenvoudiger en/of goedkoper te implementeren zijn. Daarom is bij classificatieniveau 'beschermd' de keuze voor transportbeveiliging en berichtbeveiliging open gelaten. Bij 'hoog' en 'absoluut' is de classificatie zodanig dat berichtbeveiliging toegepast moet worden.

5.3 Vertrouwelijkheid

Definitie

De bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. De onderscheiden niveaus zijn: openbaar, bedrijfsvertrouwelijk, vertrouwelijk en geheim.

Vertrouwelijke gegevens zijn bijvoorbeeld:

- Gegevens die direct of indirect te herleiden zijn naar personen (persoonsgegevens, medische gegevens etc.)
- Bedrijfsgevoelige informatie (bedrijfsgeheim, concurrentiegevoelige gegevens)

Beveiligingsmaatregelen

Onderstaande tabel beschrijft de beveiligingseisen (en maatregelen) per classificatieniveau, onderverdeeld in eisen voor authenticatie, autorisatie, monitoring en beveiliging.

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Publiek	Geen	Geen	Geen	Geen
Laag / (intern vertrouwelijk	Authenticatie 'basis' vereist. Sessie-timeout na 'x'-periode inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'basis' nodig voor deblokkeren.	Autorisatie vereist (lid van organisatie).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip.[4] Monitoring-gegevens bewaren voor periode van 1/2 jaar.	Outputvalidatie. Versleuteling tijdens transport buiten netwerk van Organisatie <organisatienaam> via transportbeveiliging of berichtbeveiliging. Kopieën van gegevens moeten op zelfde niveau worden beveiligd.
Midden (Vertrouwelijk)	Authenticatie 'midden' vereist. Sessie-timeout na 'x'-periode inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'midden' nodig voor deblokkeren.	Autorisatie op 'need to know basis'	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 2 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations binnen en buiten netwerk van <naam organisatie> via berichtbeveiliging. Kopieën van gegevens moeten minimaal net zo goed worden beveiligd. Aantal kopieën minimaliseren. Berichtbeveiliging.
Hoog (Geheim)	Authenticatie 'hoog' vereist. Sessie-timeout na 'x'-periode inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'hoog' nodig voor deblokkeren. Geen Single Sign On toegestaan.	Autorisatie op 'need to know basis'	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 7 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations via berichtbeveiliging. Versleutelde opslag van gegevens. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk van <naam organisatie>. Geen kopieën toegestaan behalve voor beschikbaarheid.

De authenticatie niveaus verwijzen naar het vereiste beveiligingsmechanisme (zie voorgaande paragraaf). Bedrijfsvertrouwelijk verwijst naar de 'organisatie', waarmee wordt bedoeld: de organisatie <organisatienaam>, een organisatiedeel of een dienst.

[4] Onder 'herhaaldelijk foutief' wordt in de context van monitoring gesproken als een identiteit achtereenvolgens drie keer foutief authentiseert. Na correct inloggen wordt de teller 'op nul gezet'.

6. Bepalen van classificatieniveaus

In de voorgaande hoofdstukken is de context beschreven die van belang is bij het toekennen van classificatieniveaus: de beleidsuitgangspunten, architectuurprincipes en beveiligingseisen. Met deze kennis kan data geclassificeerd gaan worden. In dit hoofdstuk zijn de te doorlopen stappen uitgewerkt.

Stap 1: Wettelijke eisen

De eerste stap bij dataclassificatie is nagaan welke wet en regelgeving mogelijk eisen stelt aan gebruik, distributie en opslag van data.

Vooral in de **Wet Bescherming Persoonsgegevens (WBP)** worden eisen gesteld aan de verwerking van persoonsgegevens, waarbij het begrip 'passende beveiligingsmaatregelen' een rol speelt. Voor een zorgvuldige afweging van wat wel/niet toegestaan is, is het raadzaam een jurist of een juridische dienst in te schakelen.

We spreken van een datalek als er een inbreuk is op de **beveiliging van persoonsgegevens** (zoals bedoeld in artikel 13 van de Wet Bescherming Persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Vanaf mei 2018 is de Europese regelgeving rondom datalekkage van kracht. De consequenties zijn op dit moment (2016) nog niet helemaal duidelijk, maar de gevolgen zijn vergelijkbaar met de wijzigingen in de WBP.

Stap 2: Verantwoordelijkheden t.a.v. data

Voor het toekennen van classificatieniveaus is belangrijk om verantwoordelijkheden t.a.v. data en/of informatiesystemen goed in beeld te hebben:

1. Bepaal wie data mag gebruiken, wie bevoegd is het beschermingsniveau te bepalen (rekening houdend met doelbinding in de wetgeving) en welk belang de 'business' heeft bij gebruik van deze data.
2. Bepaal ook wie er allemaal gebruik maakt van data en/of informatiesystemen en welke rechten zij hebben. Dit is relevant bij het bepalen van risico's. Data die slechts voor enkelen toegankelijk is, is minder kwetsbaar dan data die breed wordt gedistribueerd.

Hoewel de eigenaar van de gegevens verantwoordelijk is voor classificatie zal kennis over gebruik, distributie en opslag én kennis van de beveiligingscontext veelal bij anderen liggen. Bij het classificeren kan de eigenaar van de gegevens de hulp inroepen van de verantwoordelijk functioneel beheerder en de persoon die belast is met de rol van informatiebeveiligingsfunctionaris of CISO.

Stap 3: Analyse kritische bedrijfsprocessen

Classificatieniveaus zijn afgeleid van de waarde van data en het belang van het bedrijfsproces waarin deze data een rol speelt. Stel daarom vast wat het belang is van de bedrijfsvoeringsprocessen voor de organisatie en hoe deze processen worden ondersteund door de ICT voorzieningen.

De analyse wordt uitgevoerd met de modelvragenlijsten uit bijlage 2. Deze vragenlijsten geven direct het gewenste classificatieniveau voor beschikbaarheid, integriteit en/of vertrouwelijkheid van een informatiebedrijfsmiddel.

In het kader van reproduceerbaarheid en voor bijvoorbeeld auditpartijen die achtergrondgegevens vragen, maar ook om vergelijkingen mogelijk te maken bij toekomstige herclassificatie, sterk aanbevolen om de ingevulde vragenlijsten te archiveren.

De resultaten van deze stap worden in een compact overzicht van de betrouwbaarheidseisen voor de bedrijfsprocessen opgenomen, bijvoorbeeld zoals in een tabel als hieronder.

Proces	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Proces “x”	Midden	Hoog	Vertrouwelijk
Proces “y’	Hoog	Hoog	Geheim
Proces “z”	Hoog	Hoog	Openbaar

Stap 4: Afweging: criteria bij het bepalen van een goede baseline

Classificeren is geen exacte wetenschap. Bepaling van het classificatieniveau volgt uit een risicobeoordeling waarin de 'waarde' van informatie wordt bepaald. Aangezien 'waarde' lang niet altijd meetbaar is, is toekenning van een classificatieniveau soms arbitrair. In die gevallen kan een afweging worden gemaakt tussen de waarde en het risico van verlies van data. Het classificatieniveau en de daarbij behorende beveiligingseisen en maatregelen moet altijd 'passen' bij het te beschermen gegeven.

Artikel 13 WBP noemt drie criteria die bij de keuze van de te nemen technische en organisatorische maatregelen moeten worden gebruikt:

1. De stand der techniek
   - Hierbij wordt allereerst vastgesteld welke technische maatregelen op dat moment beschikbaar zijn;
   - Ten aanzien van de aanwezige voorzieningen geldt dat achterhaalde technieken niet langer als passend geclassificeerd kunnen worden;
   - Dit betekent dat een verantwoordelijke bij het bepalen van de te nemen technische maatregelen een afstemming moet vinden tussen de technische faciliteiten die in gebruik zijn bij de verwerking en die in gebruik zijn bij de beveiliging van persoonsgegevens;
   - De verantwoordelijke moet deze analyse periodiek herhalen.
2. De kosten van de tenuitvoerlegging
   - Hier moet de verantwoordelijke een keuze maken tussen de mogelijke technische en organisatorische maatregelen: in alle redelijkheid moet worden afgewogen of er een evenredigheid bestaat tussen de kosten van de beveiliging en het effect daarvan voor de beveiliging van persoonsgegevens;
3. De risico's die de verwerking met zich meebrengen
   - Hier wordt vastgesteld welk risico de betrokkene c.q. de verantwoordelijke lopen bij verlies of onrechtmatige verwerking van persoonsgegevens: naarmate het risico toeneemt zullen de maatregelen evenredig verzwaard worden.

Classificeren voer je het beste in workshopverband uit. Dit heeft een lerend effect, geeft commitment, samenwerking en vooral zorgt het voor een gewogen gemiddelde.

Stap 5: Het resultaat

Het resultaat van de analyse vertaalt zich in een classificatierapport met daarbij de ingevulde vragenlijsten als bijlagen.

Bijlage 1: Classificatie leidraad

Het classificatieproces bij <naam organisatie> wordt ondersteund door een drietal vragenlijsten, waarmee de impact op het bedrijfsproces wordt bepaald:

a) Vragen over beschikbaarheid
b) Vragen over integriteit
c) Vragen over vertrouwelijkheid

De impact op het bedrijfsproces wordt beoordeeld op een 5-puntschaal.

Schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de organisatie

Vanuit de impact op de bedrijfsproces beoordelingen (5-puntschaal) kan een vertaling gemaakt worden naar de 3-puntschaal die gebruikt wordt voor de BIV-classificatie.

Voor de classificatie naar de inzichten integriteit en vertrouwelijkheid is de vertaling als volgt:

Bedrijfsproces impact	**I-classificatie**	**V-classificatie**
1	0 – Onbekend	0 – Publiek
2	1 – Laag	1 – Laag / Intern vertrouwelijk
3 + 4	2 – Midden	2 – Midden / Vertrouwelijk
5	3 – Hoog	3 – Hoog / Geheim

Bijlage 2: Classificatie vragenlijsten

Deze bijlage kan als apart invuldocument gebruikt worden en als basis dienen om de classificaties vast te stellen. Vul onderstaande gegevens in.

Document eigenaar	
Functie	
Organisatie onderdeel	
Telefoonnummer	
Laatste datum invullen	

Het resultaat van het onderzoek voor wat betreft de BIV-aspecten voor het proces <procesnaam> van de <naam organisatie> geeft een inschaling op de volgende niveaus.

a) Beschikbaarheid :
b) Integriteit :
c) Vertrouwelijkheid :

Conclusie:

Het proces <procesnaam> valt binnen/buiten de baseline informatiebeveiliging en er zijn wel/niet extra maatregelen nodig. Deze maatregelen kunnen al bestaan als vastgestelde aanvulling of er is een uitgebreide risicoanalyse nodig.

Is er een motivatie om af te wijken van de conclusie (door de systeemeigenaar)?:

Indien er een afwijking is: Is het restrisico acceptabel? JA/NEE [5]

Aldus opgemaakt d.d.

Naam Eigenaar

[5] Doorhalen wat niet van toepassingen is.

A – Vragenlijst Beschikbaarheid

In het kader van beschikbaarheid is het goed te kijken naar hoe groot de schade is, die ontstaat bij een bepaalde uitvalduur.

a) Welke groep gebruikers wordt getroffen door uitval van het informatiebedrijfsmiddel? En hoe groot is die groep? Wat is naar schatting het aantal gelijktijdige gebruikers in het informatiebedrijfsmiddel?
b) Wat moeten de openstellingstijden voor het informatiebedrijfsmiddel zijn? Welk beschikbaarheidspercentage is dan wenselijk?
c) Welke frequentie van systeemuitval wordt nog als acceptabel ervaren? (per maand / kwartaal / jaar)
d) Is er een continuïteitsplan voor het informatiebedrijfsmiddel?
e) Is er sprake van kritieke uitval momenten? (denk bijv. aan salarisadministratie aan het eind van de maand, peildatum rapportages, verkiezingen, openingstijden, calamiteiten)
f) Maximaal toegestane down time?

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de organisatie

Business consequentie	**Business impact**				
Wanneer maximale schade	Uur	Dag	Week	2-3 weken	maand
Management beslissingen Hoe schadelijk is het als op basis van niet beschikbaarheid, verkeerde management beslissingen worden genomen?					
Direct verlies inkomsten Verliezen we inkomsten als de bedrijfsinformatie niet beschikbaar is?					
Publiek vertrouwen Wordt het vertrouwen geschaad of is er imagoschade als informatiebedrijfsmiddel niet beschikbaar is?					
Extra kosten Moeten er extra kosten gemaakt worden als het informatiebedrijfsmiddel niet beschikbaar is?					
Aansprakelijkheid Kan het niet beschikbaar zijn van een applicatie leiden tot enige vorm van aansprakelijkheid?					
Recovery Wat kost het om de achterstand in werk weer weg te werken na een herstart?					
Medewerkers moreel Heeft het nadelige effecten voor het moreel of de motivatie van gebruikers als die applicatie niet beschikbaar is?					
Fraude Kan niet beschikbaar zijn van informatiebedrijfsmiddel leiden tot frauduleuze handelingen?					
Totaalscore In samenvatting: wat de meest ernstige schade is die kan optreden bij uitval op het meest kritische moment?					

B – Vragenlijst integriteit: In het kader van integriteit is het van belang te beoordelen wat de gevolgen kunnen zijn van fouten in gegevens. Dit geldt zowel voor opzettelijke fouten (of fraude) als onopzettelijke fouten. Gaat het bij vertrouwelijkheid om de vraag of een ander het gegeven mag zien, bij integriteit gaat het erom of de ander het gegeven mag muteren. Kernbegrippen zijn juistheid en volledigheid.

a) Vormen de gegevens in het informatiemiddel de basis voor management beslissingen?
b) Welke bewaartermijnen zijn van toepassing? (archiefwet, WBP, fiscale wetgeving,...)
c) Wordt er systematisch gecontroleerd op juistheid en volledigheid?
d) Vanaf welk soort werkplekken moeten gegevens beschikbaar zijn? (altijd en overal, thuis,onderwijslokalen, personeelswerkplek)
e) Kan een gebruiker onrechtmatig voordeel behalen door een gegeven opzettelijk te veranderen? (fraude te plegen)
f) Maximaal toegestaan dataverlies na uitval?

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de organisatie

Business consequentie	**Business impact**				
Wanneer maximale schade	Uur	Dag	Week	2–3 weken	maand
Management beslissingen Hoe schadelijk is het als op basis van niet beschikbaarheid, verkeerde management beslissingen worden genomen?					
Direct verlies inkomsten Verliezen we inkomsten als de bedrijfsinformatie niet beschikbaar is?					
Publiek vertrouwen Wordt het vertrouwen geschaad of is er imagoschade als informatiebedrijfsmiddel niet beschikbaar is?					
Extra kosten Moeten er extra kosten gemaakt worden als het informatiebedrijfsmiddel niet beschikbaar is?					
Aansprakelijkheid Kan het niet beschikbaar zijn van een applicatie leiden tot enige vorm van aansprakelijkheid?					
Recovery Wat kost het om de achterstand in werk weer weg te werken na een herstart?					
Medewerkers moreel Heeft het nadelige effecten voor het moreel of de motivatie van gebruikers als die applicatie niet beschikbaar is?					
Fraude Kan niet beschikbaar zijn van informatiebedrijfsmiddel leiden tot frauduleuze handelingen?					
Totaalscore In samenvatting: wat de meest ernstige schade is die kan optreden bij uitval op het meest kritische moment?					

C – Vragenlijst vertrouwelijkheid: Om te bepalen óf en hoe vertrouwelijk informatie is, is het van belang te weten wat de business consequenties zijn van ongeplande of ongeautoriseerde openbaarmaking of bekend worden van die informatie. Een speciale categorie vertrouwelijke gegevens zijn de persoonsgegevens. Bij de verwerking hiervan hebben we ons te houden aan de Wet Bescherming Persoonsgegevens. Deze laat veel toe maar stelt wel voorwaarden aan de verwerking en dan vooral aan de zorgvuldigheid van omgang met die gegevens.

a) Worden in het informatiebedrijfsmiddel gegevens opgeslagen of verwerkt welke herleidbaar zijn tot natuurlijke personen?
b) Bevat het systeem bijzonder persoonsgegevens als bedoelt in de WBP art. 16?
c) Bevat het informatiebedrijfsmiddel informatie die gecombineerd met informatie uit andere systemen herleidbaar is tot natuurlijke personen?
d) Bevat het informatiebedrijfsmiddel concurrentiegevoelige gegevens (bijv. tarievenopbouw, contracten)?
e) Bevat het informatiebedrijfsmiddel informatie onder embargo?
f) Bevat het informatiemiddel informatie die alleen voor een specifieke doelgroep beschikbaar mag zijn? (denk ook aan licentiebeperkingen)
g) Bevat het informatiebedrijfsmiddel gegevens die gebruikt kunnen worden om fraude te plegen? (denk bijv. aan identiteitsfraude, creditcardnummers, wachtwoordbestanden).

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de organisatie

Business consequentie	Business impact				
Wanneer maximale schade	1	2	3	4	5
Management beslissingen Hoe schadelijk is het als op basis van niet beschikbaarheid, verkeerde management beslissingen worden genomen?					
Direct verlies inkomsten Verliezen we inkomsten als de bedrijfsinformatie in verkeerde handen terecht komt?					
Publiek vertrouwen Hoe groot is de imagoschade als deze informatie publiek wordt, hoe groot zijn de nadelige gevolgen voor het vertrouwen dat klanten in ons hebben?					
Wetgeving Bevat het systeem persoonsgegevens in de zin van de WBP art 16?					
Aansprakelijkheid Kan openbaar maken leiden tot aansprakelijkheidsstelling op basis van wettelijke of contractuele verplichtingen?					
Medewerkers moreel Heeft openbaarmaking nadelige effecten op het moreel of de motivatie van medewerkers?					
Fraude Welke impact hebben frauduleuze handelingen t.g.v. bekend worden van deze gegevens?					
Totaalscore In samenvatting: gegeven de bovenstaande scores (en eventueel andere consequenties) wat is dan de grootste schade die kan ontstaan door het onbedoeld of ongeautoriseerde toegang bieden tot deze informatie? (dit zou normaal minimaal gelijk moeten zijn aan de grootste schade op individuele basis)					

Bijlage 3: Waarderingsschaal

Organisaties dienen zelf vast te stellen of de hieronder genoemde schade niveaus voor hun van toepassing zijn en indien nodig aan te passen.

	Persoons-informatie	**Wettelijke en reglementaire verplichtingen**	**Financieel verlies**	**Beleid en werking van de organisatie**	**Verlies van goodwill**
Enige schade Business impact=1 of 2	Ongemak voor een persoon, maar er wordt geen inbreuk gemaakt op een wet of op regelgeving.	Civiele procedure of strafrechtelijke vervolging, resulterend in een schadevergoeding /boete van minder dan € 5.000.	Resulteert direct of indirect in verliezen van minder dan € 10.000.	Draagt bij aan het niet efficiënt opereren van een deel van de organisatie.	Heeft een negatieve invloed op de betrekkingen met andere delen van de organisatie of het publiek.
Serieuze schade Business impact=3 of 4	Een inbreuk op wet- of regelgeving, resulterend in licht ongemak voor een persoon of groep personen.	Civiele procedure of strafrechtelijke vervolging, resulterend in een schadevergoeding /boete tussen € 5.000 en € 50.000.	Resulteert direct of indirect in verliezen tussen € 10.000 en € 100.000.	Benadeelt het goed besturen en/of functioneren van een deel van de organisatie.	Heeft een negatieve invloed op de betrekkingen met andere organisaties of het publiek, resulterend in plaatselijke negatieve publiciteit.
Zeer grote schade Business impact=5	Een inbreuk op wet- of regelgeving, resulterend in aanzienlijk ongemak voor een persoon of groep personen.	Civiele procedure of strafrechtelijke vervolging, resulterend in een schadevergoeding /boete boven € 50.000 of een gevangenisstraf.	Resulteert direct of indirect in verliezen boven € 100.000.	Benadeelt het goed besturen en/of functioneren van de gehele organisatie.	Heeft een significante invloed op de betrekkingen met andere organisaties of het publiek, resulterend in wijdverspreide negatieve publiciteit.