Bijlage 2a. Logbeleid

GEMEENTE TILBURG

Logging

Beleid en Procesaanpak

V1.0

Vastgesteld in Taakgroep Informatie Beveiliging dd 20160113
Vastgesteld in I-Teammanagers overleg dd 20160308

Documentbeheer

Status en Versie

Versie	Datum	Auteur	Status/Wijzigingen
0.10	06/10/14	Marius van Oers	Initieel concept
0.14	01/12/14	Marius van Oers	Beleidsuitgangspunten overgenomen van het IBD document genaamd "Aanwijzing Logging".
0.15	2/18/15	Marius van Oers	Plan van aanpak applicatie naamgevingen geactualiseerd.
0.16	10/06/15	Jan van Tiggelen	Document leesbaar gemaakt. Op verzoek van Rob Bots en Marius van Oers zijn er inhoudelijk geen wijzigingen aangebracht.
0.17	30/12/15	Marius van Oers	Diverse kleine wijzigingen. 4.1 Plan van aanpak bijgewerkt met de actuele lijst van kritische processen en applicaties. 4.2 Inrichting logging bijgewerkt.
1.0	18/01/16	Marius van Oers	Concept v0.17 is besproken en vastgesteld in de taakgroep ib dd 20160113 met de opmerking/afspraak dat in 2016Q1Q2 de focus ligt op kwalitatieve inregeling van logging op de puntproducten. In 2016Q3Q4 komt de focus te liggen op correlatie met siem. 4.1 Plan van aanpak bijgewerkt. Versie nummer aangepast naar 1.0
1.0	08/03/16	Marius van Oers	Besproken en Vastgesteld in I-Teammanagers overleg dd 20160308

Management samenvatting

Doel van dit document.

In dit document wordt het doel van logging, het logbeleid en de implementatie van het logproces beschreven.

Aanleiding.

Uit onder andere diverse audits, zoals de kwaliteitstoets informatiebeveiliging (KIB2013), IT Audit 2014/2015, onderzoek van Gartner en zelfanalyse Suwinet is gebleken dat er wel logging is maar deze niet algemeen ingeregeld is aan de hand van beleid. Het juist inregelen van logging is een punt van aandacht.

Een korte argumentatie.

Dit document voorziet naast de procesaanpak om logging naar een volwassen niveau te brengen ook de beleidsregels van een minimale logging die nodig is om te voldoen aan de diverse wettelijke audits.

Hoe moet het vervolg.

Deze procesaanpak logging geeft een algemene richting aan. De daadwerkelijke invoering bestrijkt in elk geval de planperiode van het Informatiebeveiligingsbeleid, dit wil zeggen tot en met 2016.

Organisatorische veranderingen.

Deze aanpak moet voor de komende jaren de norm zetten voor het loggen en richting geven aan de manier van loggen. Elke applicatie of onderliggend besturingssysteem waarvan de logging cruciaal is voor de controle op het systeem heeft aan het eind van deze aanpak een volwaardig logsysteem.

Andere consequenties en effecten.

Aan het eind van deze aanpak kunnen we bij periodieke audits duidelijk maken dat we "in control" zijn.

Inhoudsopgave

1. Inleiding

Logging is een chronologische registratie van gegevens over belangrijke gebeurtenissen, die zich gedurende een periode in een verwerking voordoen. Informatiesystemen en ICT-infrastructuur genereren verschillende soorten loginformatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten. Kortom, een log beschrijft wat er gebeurt binnen systemen.
Deze registratie van gebeurtenissen kunnen soms zo gedetailleerd zijn dat ze compleet beschrijven waarom een gebeurtenis heeft plaatsgevonden (machine data). Machine-gegenereerde data is heel waardevol vanwege een definitief overzicht van alle gebruiker-transacties, klantgedrag, machine gedrag, bedreigingen van de veiligheid, frauduleuze activiteiten en nog veel meer.
Door verschillende logactiviteiten van verschillende systemen met elkaar te vergelijken verandert machine data in waardevolle inzichten (operational Intelligence). Cruciaal voor dit soort analyses is de tijd waarop bepaalde gebeurtenissen hebben plaatsgevonden. Daarom is het van belang dat de tijd van alle systemen synchroon loopt.

Een log kan geschreven worden in verschillende vormen weggeschreven worden. Soms als "platte tekst" maar ook in databasetabellen.

Goede logging kan gebruikt worden voor:

- Het ondersteunen van capaciteitsbeheer door het krijgen van statusinformatie van systemen.
- Het ondersteunen bij het ontdekken van fouten in soft- en hardware.
- Het ontdekken van menselijke fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen.
- Het ontdekken van corruptie van data of programmatuur en antivirusmeldingen.
- Het ondersteunen bij forensisch onderzoek van systemen.
- Het ondersteunen van onderzoek na een incident.
- Als basis voor implementatie van Security Incident en Event Management systemen (SIEM).
- Het ondersteunen van SLA Compliance Monitoring.
- Het leveren van informatie ten behoeve van een wettelijk voorgeschreven audit;
- Het leveren van informatie om te onderzoeken of voldaan wordt aan beleid (bijvoorbeeld of er vreemde apparaten aangesloten zijn geweest).
- Het leveren van informatie om onweerlegbaar aan te tonen dat een bepaald bericht wel of niet verzonden is, of dat een activiteit is uitgevoerd.
- Rapportage over systeemgebruik en incidenten aan de systeemeigenaar en de Chief Information Security Officer (CISO).

2. Logbeleid gemeente Tilburg

Ten behoeve van de beveiliging van informatie is er een logging-beleid voor alle gemeentelijke ICT-voorzieningen. Het doel van dit beleid is duidelijke regels neer te leggen die in relatie tot logging genomen moeten worden binnen de gemeente.
De gemeente Tilburg hanteert de volgende beleidsuitgangspunten welke zijn ontleend aan de Baseline Informatiebeveiliging Gemeente (BIG) en aanvullend zijn op het algemene beveiligingsbeleid van de gemeente:

2.1 Audit logging

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

1. Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
2. Een logregel bevat minimaal:
    - De datum en het tijdstip van de gebeurtenis
    - De gebeurtenis (zie Normenkader 10.10.2.1)
    - Waar mogelijk een tot een natuurlijk persoon herleidbare gebruikersnaam of identificatie
    - Waar mogelijk de identiteit van het werkstation of de locatie:
        - Host naam
        - Operating System (OS)
        - Naam van de toepassing
        - IP-adres(sen)
        - Locatie(s)
    - Het object waarop de handeling werd uitgevoerd
    - Het resultaat van de handeling
3. In een log-regel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera). In de log-regel mogen ook geen persoonsgegevens worden opgenomen uit systemen van de gemeente zelf (dus wel gebruikersnamen of inlog accounts)
4. Logberichten worden overzichtelijk samengevat. (Daartoe zijn systemen die logberichten genereren bij voorkeur aangesloten op een monitoringsysteem zoals een Security Information and Event Management systeem (SIEM). Hiermee worden meldingen en alarmoproepen aan de beheerorganisatie gegeven.)
5. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.
6. Controle op opslag van logging: het vol lopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt ook gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).
7. Alle ongeautoriseerde toegangspogingen zijn beveiligingsincidenten en vereisen directe opvolging door melding aan de coördinator informatiebeveiliging van de gemeente Tilburg.

2.2 Controle van het beleid op systeemgebruik

Er behoren binnen de gemeente procedures te zijn vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld. Zoveel als mogelijk wordt systeemgebruik automatisch gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een logboek door bijvoorbeeld beheerders.
De volgende gebeurtenissen moeten zijn opgenomen in de logs:

1. Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
2. Gebruik van functies voor functioneel beheer, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases).
3. Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
4. Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services).
5. Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen).
6. Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.
7. Bij online transacties moet minimaal de volgende drie punten worden gelogd:
    - datum en tijd
    - het bericht-ID
    - aanroepend en verzendend systeem en proces

2.3 Bescherming van informatie in logbestanden

Logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. De volgende beleidsregels zijn hierop van toepassing:

1. Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang
2. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
3. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
4. Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
5. De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingenaangepast moeten worden zal daarbij altijd het vier ogen principe toegepast worden.
6. De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
7. Het goed functioneren van de logging wordt continue gemonitord voor essentiële systemen.
8. Controle op opslag van logs: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld: een logserver die niet bereikbaar is).

2.4 Bewaartermijnen

Mits wettelijk niet anders bepaald geldt voor:

Integriteit

Niveau	Monitoring	Periode
Niet zeker	Geen	
Beschermd	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoring-gegevens bewaren voor periode van een half jaar.	1/2 jaar
Hoog	**Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoring-gegevens bewaren voor periode van maximaal twee jaar of langer bij een vermoed beveiligingsincident.**	**2 jaar**
Absoluut	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of -service. Monitoring-gegevens bewaren voor periode van minimaal drie jaar bij een vermeend beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.	3 jaar

Vertrouwelijkheid

Niveau	Monitoring	Periode
Openbaar	Geen	
Bedrijfs-vertrouwelijk/Intern	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van een half jaar.	1/2 jaar
Vertrouwelijk	**Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van twee jaar.**	**2 jaar**
Geheim	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van zeven jaar.	7 jaar

NB, het niveau "Bedrijfs-vertrouwelijk" wordt bij de Gemeente Tilburg aangeduid als zijnde "Intern".

2.5 Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen van de gemeente behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

1. Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse (correlatie) van logbestanden mogelijk is.

3. Rollen en verantwoordelijkheden

- De afdeling PO&I adviseert de directie, afdelingen en het college inzake beveiliging, formuleert het beveiligingsbeleid, bewaakt de stuurcyclus en treedt op als opdrachtgever van controle programma's. Hiertoe is binnen de afdeling PO&I de strategisch adviseur informatisering aangewezen als Security Officer.
- De Security Officer is verantwoordelijk voor het opstellen van het logging beleid en de methodiek.
- De Coördinator Informatiebeveiliging kan steeksproef gewijs lijncontroles uitvoeren op naleving en werking van de technische uitwerkingen, in deze context wordt bedoeld controle op de logging. Als het de situatie toelaat, kan de Coördinator Informatiebeveiliging zonder aankondiging door middel van checks, audits, penetratie- en kwetsbaarheidstesten controles uitvoeren op naleving en werking.
- De teammanager ziet toe op het naleven van de procesaanpak en is mede verantwoordelijk voor het uitdragen van de opgestelde procesaanpak. Bij het niet naleven van de afspraken neemt de teammanagerpassende maatregelen.
- De beveiligingsspecialist bij de desbetreffende afdeling levert periodiek (1x per kwartaal) een rapportage aan - aan de coördinator informatiebeveiliging en security officer - ter controle of de juiste logging inrichtingen volgens de procesaanpak worden uitgevoerd.
- De beheerders van de diverse systemen zijn zelf verantwoordelijk voor de uitvoering van de procesaanpak logging voor hun eigen systeem software.
- Indien er, met betrekking tot logging issues/inrichting, security vraagstukken zijn dan dienen die eerst intern in het desbetreffende team (sb/ao/fab) gecommuniceerd en geaddresseerd te worden. Aanspreekpunt is de security technisch operationeel contactpersoon bij het desbetreffende team. Komt men er niet uit dan kan advies worden gevraagd van de coördinator informatiebeveiliging en eventueel security officer.

4. Inrichting logging

4.1 Plan van aanpak

Omdat nog niet actief gebruik gemaakt wordt van logging binnen de gemeentelijke infrastructuur is het ondoenlijk om volledig te beginnen bij alle hard- en software componenten. Loggen en de controle hierop kost menskracht, tijd en geld. Het is daarom beter om klein te beginnen en dit op termijn uit te breiden naar uiteindelijk een volledig geautomatiseerd logmanagement oplossing. Die op haar beurt later weer door kan groeien naar een Security Information and Event Management (SIEM) oplossing. Het puur en alleen handmatig beoordelen van alle logs is ondoenlijk, begin bij voorkeur klein en geautomatiseerd.

Qua plan van aanpak is de afspraak dat in 2016Q1Q2 de focus ligt op kwalitatieve inregeling van logging op de puntproducten. In 2016Q3Q4 komt de focus dan vervolgens te liggen op correlatie met siem.

Omdat ook nog niet elke applicatie of operatingsystem op de juiste manier logt, kan men beter klein beginnen om minimaal de basis logging (Baseline Logging) te voldoen en het volgende groeipad volgen:

1. Begin met de wettelijk vereiste systemen die periodiek een audit ondergaan zoals GBA, DigiD en Suwinet.
2. Daarna met de "perimeter", de buitenkant van het netwerk van de gemeente en de systemen en netwerk componenten in de Demilitarized Zone (DMZ).
3. Dan netwerkcomponenten binnen het gemeentelijke netwerk.
4. De essentiële systemen, applicaties, databases, servers et cetera.
5. De belangrijke systemen, applicaties, databases, servers et cetera.
6. De overige systemen.

Voor de aanpak van logging ontwikkelen we een standaard toe te passen methodiek procesaanpak inrichting logging. Logging moet voldoen aan de toets van de accountant, vandaar de noodzaak om de procedure inrichting logging in hoofdstuk 4.2 te volgen.

Het ideaal is dat voor alle processen (applicaties etc) logging goed wordt geregeld.
Dit kan niet in één jaar en dit is ook een permanente PDCA cyclus.
Qua prioritering wordt lijst met kritische processen en applicaties aangehouden, dynamisch te vinden op:
P:\@Vertrouwelijk\ICT informatiebeveiliging\Applicatie Security\Algemeen\Kritische Processen en Applicaties
Aangezien deze lijst dynamisch is, is onderstaande planning onder voorbehoud.

Planning op hoofdlijnen:

	proces	**applicaties**	**privacy**
1.	Financiële processen	JDE	beperkt
2.	Beheer Oracle	Oracle beheer "aan de achterkant"	ja
3.	Werk en inkomen	Suwinet, Civision SAM, Dirigent, Liaan	ja
4.	Zaaksysteem	Excellence	ja
5.	Burgerzaken en stadswinkels	Key2 Burgerzaken, GBA-V, VOA web	ja
6.	Inkomensondersteuning/ bijzondere bijstand	Civision SAM, Dirigent	ja
7.	Schuldhulpverlening	Opus D, Allegro	ja
8.	Belastingen	Key2Belastingen	ja
9.	WMO	Civision SAM	ja
10.	Grondexploitatie	Squit XO, CMP	beperkt
11.	Bouwvergunningen	Squit XO, CMP	beperkt
12.	Parkeren	Key2parkeren	beperkt
13.	Veiligheid	Invoerschil veiligheid	ja

Nadat bovenstaande lijst is afgewerkt dienen de loggingsprocedures in het regulier werkproces van alle functioneel & applicatie beheers te worden opgenomen.

4.2 Inrichting logging

Onderstaande methode is een handreiking die volgens auditors gevolgd moet worden om tot een effectieve inrichting van logging te komen.

De procedure om tot het inrichten van logging te komen is:

1. Bepaal welke **Processen** er zijn en welke systemen die ondersteunen.
   De business bepaalt welke processen er nodig zijn. De functioneel & applicatie beheerders geven aan welke systemen de processen ondersteunen.

2. Voer een **Risicoanalyse** uit ter bepaling van de meest kritische processen; de processen waar de grootste risico's/kwetsbaarheden zich bevinden. Een business impact analyse/risicoanalyse dient door de business uitgevoerd te worden.

3. Bepaal vervolgens de meest **Kritische Processen**; de processen waar de grootste risico's/kwetsbaarheden zich bevinden. De business bepaalt initieel welke kritische processen er zijn.

4. Welke **Systemen** ondersteunen die kritische processen? De functioneel & applicatie beheerders geven aan welke systemen de meest kritische processen ondersteunen.

5. Welke **kritische transacties/handelingen** vinden er plaats?
   Dit dient te worden bepaald door de business.

6. Richt **logging** in op de kritische processen en kritische transacties.
   Dit dient initieel door de applicatie beheerders te worden ingeregeld, in overleg met de functioneel en technisch beheerders.
   Alles loggen is meestal niet effectief, logging dient ingericht te worden op de kritische processen en kritische transacties.

7. Voer een periodieke **check** op de logging uit, minimaal 1x per week, meer indien noodzakelijk. De functioneel beheerder checkt de logging en rapporteert dit aan de verantwoordelijke manager. Mede op basis van dit overzicht controleert het management of de systeem-, gegevens-, of proceseigenaren of er oneigenlijke toegangspogingen en of - handelingen/transacties zijn verricht door medewerkers binnen de informatiesystemen waar zij verantwoordelijk voor zijn, en brengt indien nodig ook een rapportage uit aan de Security Officer.

Bovenstaande handreiking geeft de procedure om tot het inrichten van logging te komen is indien er vanaf scratch begonnen moet worden. Bij de Gemeente Tilburg is er echter al bijvoorbeeld een lijst met kritische processen en applicaties etc.

- Vandaar dat we in het algemeen kunnen volstaan met de blauw gemarkeerde items #5-6-7.

5. Scope

Deze procesaanpak logging is van toepassing op de applicaties en netwerk infrastructuur waar de Gemeente Tilburg eigenaar van is en/of het beheer van doet.
Van leveranciers wordt hetzelfde verwacht; dit wordt afgesproken in contracten en er wordt toegezien op de naleving hiervan. Enkele voorbeelden van componenten die hieronder vallen zijn onder andere:

- Alle door de Gemeente Tilburg ondersteunde software.
- Externe leveranciers; bijvoorbeeld SaaS/LaaS/PaaS providers

6. Bijlage A (Aanwijzing Logging IBD)

HIERONDER DUBBELCLICKEN OM IN ZIJN GEHEEL TE OPENEN:

INFORMATIE
BEVEILIGINGS
DIENST

AANWIJZING LOGGING

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

7. Bijlage B (Mapgood Checklist Risicoanalyse)

Mapgood Checklist Risicoanalyse.

Mapgood heeft een breder doel dan alleen logging. De opneming hier is illustratief voor de risicoanalyse genoemd in punt 2 van de Procedure Inrichting Logging.

CHECKLIST RISICO ANALYSE INFORMATIEBEVEILIGING ISO 27001 EN NEN 7510
MAPGOOD staat voor de beginletters van de belangrijkste onderdelen van het normenkader voor informatiebeveiliging, wat we ook in Tilburg toepassen: Mens, apparatuur, programmatuur, gegevens, organisatie, omgeving en diensten. Met deze checklist kan een risicoanalyse op een proces of op een afdeling worden uitgevoerd. In de checklist is een juiste balans gevonden tussen zorgvuldigheid, volledig en hanteerbaarheid. In de praktijk blijk deze makkelijk hanteerbaar en ook methodisch gedegen in elkaar te zitten, zodat deze door accountants wordt geaccepteerd.

Veel organisaties willen in het kader van informatiebeveiliging bepalen wat hun risico's zijn. Dit even los van het feit of certificering voor ISO 27001 of NEN 7510 het doel is. Er zijn diverse tools voor risicoanalyse met bijbehorende checklists beschikbaar. Veelal echter stammen die nog uit de vorige eeuw, toen internet, sociale media, laptops, smartphones, de cloud, BYOD en het nieuwe werken nog niet bestonden en de hackers nog vanaf zolderkamertjes werkten.

De uitkomst van de meeste checklists is dat organisaties een diarree aan maatregelen moeten implementeren. Een kind begrijpt, dat er dan een papieren tijger wordt gecreëerd, waarvan de naleving een luchtkasteel is. Als u geen financiële instelling, ziekenhuis of politiedienst bent, dan heeft u een dergelijke overkill niet nodig.

In het artikel 'Is beveiliging een groeiend probleem' beschrijven we dat u onderscheid moet maken tussen normale informatie en uw kroonjuwelen. Voor uw organisatie ligt die verhouding waarschijnlijk ongeveer op >99% normaal tegen <1% kroonjuwelen. Voor de kroonjuwelen geldt, dat u er een kluis voor moet creëren met een hoger beveiligingsniveau. Voor die >99% echter loopt u minder risico's en hoeft u in feite alleen een aantal basismaatregelen te treffen. Op dit idee is ook de wetgeving in Nederland gebaseerd evenals certificering op basis van ISO 27002 of NEN 7510.

Helaas blijkt in de praktijk, dat organisaties wel maatregelen hebben genomen tegen een aantal risico's (vooral op ICT-gebied), maar dat op allerlei andere terreinen zelfs het basisniveau niet gehaald wordt. Vaak heeft men zelfs geen idee van wat wel en niet acceptabel is. Organisatie kunnen hiervoor echter aansprakelijk gesteld worden en lopen een aanzienlijk risico op reputatieschade. Daarom is het handig om de risico's en de tekortkomingen inzichtelijk te maken.

Risicoanalyse informatiebeveiliging

Op dit idee moet ook uw risicoanalyse zijn gebaseerd. De kroonjuwelen moet u afbakenen. Zij vormen een apart verhaal. We zullen ons nu richten op de >99% normale informatie. Hieronder vindt u een eenvoudige checklist gebaseerd op MAPGOOD (mensen, apparatuur, programmatuur, gegevens, omgeving, organisatie en diensten), die u voor uw risicoanalyse kunt gebruiken. In de praktijk wordt de risicoanalyse zo ook gedaan (en door auditors geaccepteerd) in certificeringstrajecten voor ISO 27001 en NEN 7510. Deze risicoanalyse is direct afgeleid van het VIR, zodat ook (semi-) overheidsinstanties hier gebruik van kunnen maken.

Het zijn de bestuurders van een organisatie, die hierbij vastleggen wat zij voor hun organisatie beschouwen als belangrijke risico's en waarop zij maatregelen nemen. Als achteraf blijkt dat dit foutief is ingeschat, is hiermee zelfs de aansprakelijkheid voor bestuurders afgedekt.

Hieronder een weergave van een deel van de checklist voor de risicoanalyse.

MAPGOOD	#	Dreiging	Detail	Kans	Impact	Risico	Risicoomschrijving
Mens	R1	Wegvallen personeel	voorzienbaar, onvoorzienbaar				
	R2	Onopzettelijke fouten (ook derden)	onkunde, slordigheid, stress				
			foutieve procedures				
			complexe en/of foutgevoelige bediening				
			omgang met passwords				
	R3	Opzettelijke fouten (ook derden)	negeren voorschriften				
			schending privacy				
			ongeautoriseerde toegang (hacken)				
Apparatuur	R11	Spontaan technisch falen	veroudering, slijtage, gebrekkig onderhoud				
			storing				
			fouten in geleverd product				
	R12	Oorzaak omgeving	uitval nutsvoorziening				
			storing nutsvoorziening				
			temperatuur, vochtigheid, vuil, stof				
	R13	Oorzaak mens	remote werken				
			bring your own device				
			opzettelijke verandering functie apparatuur				
			beschadiging, vernieling, diefstal				
Programmatuur	R21	Programmatuur-fouten	bij ontwikkeling of onderhoud				
			bij beheer				
	R22	Programmatuur-	virus, malware				
			illegale software van derden				
			illegaal gebruik van software				
Gegevens	R31	Via gegevensdragers	onopzettelijk verlies				

MAPGOOD	#	Dreiging	Detail	Kans	Impact	Risico	Risicoomschrijving
			(nalatigheid)				
			diefstal (fysiek)				
			diefstal (digitaal)				
			crash				
			onzorgvuldige vernietiging				
	R32	Via programmatuur	foutieve of gemanipuleerde software (ook malware)				
	R33	Via personen	foutieve gegevensmutatie				

Organisatie	R41	Door afspraken en procedures, wet- en regelgeving	Niet voldoen aan wet- en regelgeving, privacyregels				
	R42	Door personen	Functiescheiding, niet houden aan regels				
Omgeving	R51	Door personen	Clean desk, niet naleven regels, diefstal				
	R52	Door fysieke omgeving/ gebouw	Ontoereikende toegangsbeveiliging, werkplek beveiliging,				
Diensten	R61	Door leveranciers	Onderhoudsfouten,				
	R62	Intern	Onderhoudsfouten, verstoringen				

In een sessie met de verantwoordelijke managers kan deze lijst in een dagdeel doorgewerkt worden. Aan zowel de kans als de impact wordt de kwalificatie laag, middel of hoog toegekend. Op grond hiervan wordt het objectieve risico geclassificeerd via het onderstaande schema.

	Laag	Middel	Hoog
Laag	1	1	2
Middel	1	2	3
Hoog	2	3	4

Interpretatie van de risicoanalyse

Het getal kan gebruikt worden in het stoplichtmodel, zoals beschreven is in ‘Managementrapportage risicoprofiel informatiebeveiliging ISO 27001 of 27002’.

Bekend is dat in dergelijke sessies risico’s vaak te hoog worden in geschat. Daarom is de volgende vuistregel van belang. Een sessie mag leiden tot maximaal 10 gebieden met een risico van 3 of 4. Als dit niet gehaald wordt in één sessie, moet de sessie met de proceseigenaar geëvalueerd worden en moet worden vastgesteld hoe een herhaling van de sessie wel tot het gewenste resultaat kan leiden. Oorzaak is vaak dat de kroonjuwelen niet scherp genoeg zijn afgebakend of dat de bescherming van de kroonjuwelen toch door de

discussie loopt. Ook kan het streven naar 100% veiligheid (wat per definitie onmogelijk is) de sessie beïnvloeden. (Zie ook ‘ISO 27001 of 27002 ‘lean en mean’ implementeren als security management systeem’.)

Het gevaar is dat u voor uzelf de lat te hoog legt. Zowel ISO 27001 als NEN 7510 kennen een verbetercyclus waar u gebruik van kunt maken. Leg de lat eerst op een hoogte die u aan kunt en leg in de volgende cyclus de lat hoger. Want één ding is onvergeeflijk: dat u niet voldoet aan de norm die u zelf heeft vastgesteld. Daar komt u absoluut niet mee weg als het gaat om bestuurdersaansprakelijkheid of certificering.