Inleiding

Gezien de gedefinieerde probleemstelling hebben we ervoor gekozen een organisatie, waarin een zogenaamde Computer Security Incident Response Team (CSIRT) opgenomen is, als uitgangspositie te nemen. Gezien de taakstelling en de hieraan gerelateerde verantwoordelijken, bevoegheden en concrete werkzaamheden van een CSIRT, kan ons inziens een CSIRT een essentiële bijdrage leveren bij de totstandkoming van forensische gegevens, oftewel digtaal bewijs. Natuurlijk dienen dan wel een aantal aanpassingen of maatregelen genomen te worden, met name op het organisatorische en juridische vlak, voordat een CSIRT geschikt en bevoegd is om forensische gegevens te kunnen aan leveren aan de diverse (externe) instanties.

Hieraan worden de verschillende aandachtsgebieden beschreven die inzichtelijk moeten maken waarmee rekening moet worden gehouden en welke concrete maatregelen in de organisatie genomen moeten worden die uiteindelijk leiden tot een "forensische" ingerichte CSIRT-organisatie. Het betreft de volgende aandachtgebieden:

- *Inventarisatie van de standaard verantwoordelijkheden, bevoegdheden en takenpakket van een CSIRT;*
- *Omschrijving van het begrip digitaal forensisch onderzoek en bewijs;*
- *Beschrijving van de toegevoegde waarde van een CSIRT in het kader van digitaal forensisch onderzoek c.q. de aanlevering van digitaal bewijs;*
- *Proces-technische aspecten;*
- *Juridische aspecten;*
- *Technische aspecten.*

Verantwoordelijkheden, bevoegheden en taken van een CSIRT

Het waarborgen van de beschikbaarheid, integriteit en exclusiviteit van de ICT-infrastructuur binnen een organisatie en de daarin opgenomen informatie vereist een specifieke deskundigheid. Deskundigheid die enerzijds in staat is interne en externe dreigingen te onderkennen en te vertalen in concreet te nemen maatregelen, anderzijds het op effectieve en efficiënte manier reageren op manifest geworden dreigingen en de hieraan gerelateerde incidenten. Deze moeten worden gepositioneerd in een zich continu wijzigend geheel aan ICT-infrastructuurcomponenten, hun individuele instellingen en beheer- en controle maatregelen die daarbij in samenhang zijn en een zich steeds wijzigend dreigingsbeeld. In een CSIRT is de noodzakelijke expertise en ervaring aanwezig om hieraan te kunnen voldoen. Hiermee wordt uiteindelijk bereikt dat:

- *de verantwoordelijkheid voor het vroegtijdig onderkennen en analyseren van dreigingen op de beschikbaarheid, exclusiviteit en integriteit van de ICT-infrastructuur is toegewezen en belegd binnen een organisatie;*
- *een gespecialiseerd team is geformeerd dat gevraagd en ongevraagd voorstellen doet over uit te voeren oplossingen in relatie tot beveiligingsrisico's en daadwerklijke voorgedane incidenten in de ICT-infrastructuur.*

Naast het op basis van dreigingsbeelden en risico-inschattingen permanent auditen van de ICT-infrastructuur en het nemen van maatregelen ter voorkoming van het manifest worden van dreigingen is het CSIRT tevens de vraagbaak en adviseur voor de organisatie op het gebied van de informatiebeveiliging.

Taakstelling forensisch georiënteerde CSIRT

De taakstelling van CSIRT kan worden omschreven als het zorgdragen dat de beschikbaarheid, exclusiviteit en integriteit van de werking van de ICT-infrastructuur vanuit de optiek van veiligheid in alle gevallen is gewaarborgd.

Deze taakstelling is daarbij in een aantal deeltaakstellingen onder te verdelen, te weten:

- *Het ontwikkelen, inrichten en instandhouden van voorzieningen waarmee de ICT-infrastructuur actief kan worden beschermd en worden gevrijwaard tegen aanvallen/handelingen van buitenaf en van binnenuit die tot doel of als resultaat de ondermijning van de werking van de ICT-infrastructuur kunnen hebben dan wel (vastgelegd in beleid) als ongewenst wordt beschouwd.*
- *Het aanwenden van bovenstaande voorzieningen voor het monitoren, onderzoeken, detecteren en (zo mogelijk) het voorkomen van bedreigingen op de ICT-infrastructuur.*
- *Het (doen) opheffen van eenmaal geconstateerde bedreigingen in de ICT-infrastructuur en het (doen) melden van bedreigingen en uitbrengen van adviezen ter opheffing aan daartoe bevoegde instanties indien dit buiten het eigen verantwoordelijkheidsgebied ligt.*
- *Het voorbereiden van preventieve maatregelen ter beheersing van de onderkende bedreigingen en de hieraan gerelateerde mogelijke risico´s en schade.*

Ter realisatie van deze taakstelling voert CSIRT onder andere de volgende activiteiten uit:

- *Het door preventief onderzoek in een vroegtijdig stadium onderkennen van potentiële informatiebeveiligingrisico's voor de ICT-infrastructuur betreft en het voorstellen van passende maatregelen.*
- *Het proactief optreden ter voorkoming van het manifest worden van deze beveiligingsrisico's.*
- *Het intern, namens de directie, sturend optreden in geval van acute dreigingen en het ongevraagd correctief optreden bij het manifest worden van beveiligingsrisico's.*
- *Het opstellen en ter hand stellen van rapportages inzake het voorkomen van beveiligingsincidenten aangaande de ICT-infrastructuur en genomen acties naar aard en soort aan de daartoe geëigende functionarissen intern, alsmede over genomen acties ter voorkoming van beveiligingsincidenten aangaande de ICT-infrastructuur.*
- *Het op nationaal en internationaal niveau verzamelen, bestuderen en analyseren van informatie, maatregelen en methodieken op het terrein van het waarborgen van de beschikbaarheid, exclusiviteit en integriteit van ICT-infrastructuren.*
- *Het adviseren/mede opstellen/ontwikkelen over/van beleid, informatie, maatregelen en methodieken waarmee de beschikbaarheid, exclusiviteit en integriteit van de defensie-ICT-infrastructuur beter kan worden gewaarborgd.*
- *Het gevraagd en ongevraagd adviseren van klanten over de opzet en inrichting van (informatie)systemen ter voorkoming (beveiliging)dreigingen bij gebruik.*

CSIRT diensten

Een CSIRT kan een veelheid van diensten leveren. Een dienst is het meest opvallend en daar wordt dan ook onmiddellijk aan gedacht als men het over CSIRT diensten heeft: het op afroep leveren van hoog specialistische diensten voor onverwachte gebeurtenissen op het gebied van de informatie beveiliging.
In de praktijk kan men de diensten van een CSIRT echter groeperen in drie categorieën te weten:

- *reactieve diensten*
- *proactieve diensten en*
- *beveiligingsbeheer- en beveiligingskwaliteit diensten.*

Reactieve diensten
Deze diensten worden op afroep gestart door een gebeurtenis of een verzoek, bijvoorbeeld een virusmelding, een rapport uit een Intrusion Detection System (IDS) of na het vaststellen van ongeoorloofde toegang op een systeem. De reactieve diensten vormen vaak de hoofdtaak van een CSIRT.

Proactieve diensten
Deze diensten leveren assistentie en informatie bij een veelheid van geautomatiseerde informatiediensten met als doel het veiligstellen van de exclusiviteit, integriteit en beschikbaarheid van systemen en netwerken.

Beveiligingsbeheer- en beveiligingskwaliteit diensten
Deze diensten ondersteunen bestaande ondersteunende bedrijfsprocessen oftewel verhogen het kwaliteitsniveau van deze diensten. Het meest opvallende aan beveiligingsbeheer- en beveiligingskwaliteit diensten is, dat ze niet in bestaande ontwikkel, test, beheerprocedures en werkzaamheden vallen. Typisch is dit het gebied waar de informatiebeveiliging sterk kan worden verbeterd door het inzicht en de expertise van een CSIRT. Vaak gaat het hier om het vaststellen en identificeren van risico's, bedreigingen, systeemzwakheden en kwetsbaarheid van samengestelde systemen.

In de onderstaande tabel wordt een totaaloverzicht gegeven.

tabel 1: Overzicht CSIRT diensten

Reactieve diensten	*Proactieve diensten*	*Beveiligingsbeheer- en beveiligingskwaliteit diensten*
Alarmeren en waarschuwen	*Mededelingen (informatie)*	*Risico analyse*
Incident afhandeling	*Technologie bewaking*	*Calamiteiten en continuïteitsanalyse*
Kwetsbaarheids afhandeling	*Beveiligingsaudits of onderzoeken*	*Beveiligingsadvies*
Besmetting afhandeling	*Ontwikkeling van beveiligingshulpmiddelen*	*Beveiligingsbewustwording*
	Intrusion Detection diensten	*Cursus en training*

Voor de bovenstaande diensten geldt dat er zowel reactieve- als proactieve componenten in zitten. Kwetsbaarheidanalyses bijvoorbeeld, kunnen proactief worden gedaan voordat een systeem wordt ingezet, maar een kwetsbaarheidanalyse wordt vaak ook uitgevoerd bij het constateren van een inbreuk.
rapporten over hardware en software kwetsbaarheden. Mogelijke activiteiten zijn:

Mandatering CSIRT
Het mandaat van een CSIRT wordt binnen een organisatie door de directie bepaald en formeel bekrachtigd. Gezien de ervaringen omvat de mandatering standaard de volgende punten:

- *Het CSIRT verricht haar werkzaamheden aan de hand van de vigerende wet- en regelgeving;*
- *Het CSIRT heeft het mandaat om binnen de organisatie beheerde omgevingen alle noodzakelijke onderzoek- en rapportagewerkzaamheden uit te voeren die in het kader van een CSIRT noodzakelijk zijn, met name het onderzoeken en rapporteren van geconstateerde afwijkingen van het vastgelegde beveiligingsniveau;*
- *Het CSIRT heeft het mandaat om binnen de beheerde omgevingen direct corrigerende acties uit te (laten) zetten in samenspraak met de verantwoordelijke informatiemanager;*
- *Het CSIRT heeft het mandaat om, voor wat betreft alle externe koppelingen, te handelen conform de separaat gedefinieerde regelgeving en instructies;*

- *Het CSIRT heeft geen mandaat voor de zogenaamde opsporingsbevoegdheid. In voorkomende gevallen worden altijd via de directie de geëigende instanties gewaarschuwd, waarna CSIRT hooguit om ondersteuning kan worden gevraagd.*

Proces forensisch onderzoek door CSIRT

Gezien de relevantie wordt dit onderwerp separaat in de weblog beschreven.

Inbedding CSIRT in de organisatie

Naast de manier waarop de processen ten aanzien van forensisch onderzoek en vastlegging worden ingericht is het ook van belang de betreffende processen op een correcte wijze in te bedden in de organisatie, derhalve de integratie van de CSIRT-organisatie in de bestaande organisatie.

Zoals uit het bovenstaande is gebleken zijn voor het goed doorlopen van het forensisch onderzoek en vastlegging van digitaal bewijs veel verschillende specialisaties nodig. Zo is er behoefte aan technisch geschoolde functionarissen voor het onderzoek naar de oorzaken en oplossingen van incidenten, aan functionarissen met kennis van de betreffende bedrijfsprocessen, aan juridische medewerkers en aan informatiebeveiligingsspecialisten.

Bij de inbedding in de organisatie komt men al snel uit op en zogenaamde matrix-organisatie. Bij een dergelijke organisatievorm worden functionele teams samengesteld uit functionarissen uit de verschillende afdelingen. Gezien de overwegend technisch georienteerde taakstelling van een CSIRT, zullen de meeste functionarissen uit de reguliere IT-afdeling afkomstig zijn.

Juridische aspecten

Inleiding
In het kader van deze scriptie is het niet doenlijk om alle juridische aspecten te behandelen en zal er dus een afbakening gemaakt moeten worden. Deze scriptie handelt over incident response en forensisch of digitaal onderzoek, zodoende worden de meest relevante juridische onderwerpen nader uitgewerkt die hiermee het meest verwant zijn.

Afbakening
Het beschouwingsgebied wordt afgebakend door de scope te beperken tot handelingen die gepleegd worden met geautomatiseerde middelen. Daarbij wordt ook enige aandacht besteed aan fraudehandelingen gepleegd door het eigen personeel, aangezien uit onderzoek is gebleken dat veelal deze doelgroep hierbij betrokken is.

Binnen het proces van incident response zijn er twee fasen die juridisch karakter kennen:
- *Opsporing;*
- *Afhandeling.*

Bij het opsporen van incidenten kan de vraag gesteld worden wat het juridisch kader is waarmee rekening gehouden moet worden indien bewijsmaterlaal verzameld wordt nadat geconstateerd is of vermoed wordt dat een persoon frauduleuze handelingen heeft gepleegd. Deze vraag is van cruciaal belang omdat onrechtmatig verkregen bewijs door de rechter terzijde wordt gelegd en dus niet wordt meegenomen bij de bewijsopbouw. Dit kan betekenen dat er te weinig bewijs overblijft waardoor de zaak verloren is.

Welke middelen staan de werkgever nu ter beschikking om bewijs te verzamelen inzake een (vermeend) incident? In dit kader is het interessant te onderzoeken welke mogelijkheden er bestaan dat naar aanleiding van de uitgevoerde controles ontoelaatbare handelingen van een medewerker geconstateerd worden. Dan speelt de vraag welke wegen bewandeld moeten worden om de medewerker te kunnen vervolgen. Dit leidt tot de tweede onderzoeksvraag: Op welke wijze dient de werkgever (potentiële) incidenten af te handelen zodat, indien gewenst, de verdachte ook daadwerkelijk strafrechtelijk vervolgd kan worden.

Ten eerste zal derhalve nader uitgewerkt worden welke wegen de werkgever moet bewandelen om van het vermeende incident aangifte te doen. Hierbij zal specifiek aandacht worden besteed aan de middelen die hiervoor in het algemeen binnen elke organisatie beschikbaar zijn.

Forensisch of digitaal onderzoek.
Het onderwerp forensisch of digitaal onderzoek wordt in de huidige literatuur hoofdzakelijk gepresenteerd als een technisch vakgebied waarin met behulp van tools en operating systeem commando's bepaalde informatie uit systemen wordt geëxtraheerd. In de literatuur wordt bijvoorbeeld veelvuldig in deze context verwezen naar de door Schiffman beschreven twintig scenario's van incidenten en de wijze waarop de betreffende systeembeheerders hiermee zijn omgegaan. Daarnaastgaan Mandia en Prosise in eerste instantie in op de organisatorische aspecten van digitaal onderzoek maar vervallen vervolgens snel in een technische behandeling van onderzoeken in diverse operating systemen en netwerk omgevingen. In de praktijk blijkt echter dat de puur technische invalshoek van incident response in het algemeen en digitaal onderzoek in het bijzonder te beperkt is.

De echte toegevoegde waarde van een goed incident response proces blijkt in de praktijk te liggen in de integratie van de organisatorische, juridische en technische aspecten die een rol spelen in een dergelijk proces. Digitaal onderzoek kan niet los worden gezien van het incident response proces waarin het is ingebed, zoals correct wordt weergegeven in de inleiding van Schiffman. Wij zullen dan ook een topdown benadering hanteren waarbij de afhandeling van incidenten vanuit de organisatorische inrichtng en processen zal worden bekeken.

Vanuit de organisatorische invalshoek zullen vervolgens juridische en technische verbijzonderingen worden aangebracht in het model.

Digitaal onderzoek wordt door het Nederlands Forensisch Instituut (hierna te noemen NFI) formeel gedefinieerd als het onderzoeken op informatiesystemen om uit de aanwezige data bewijs te extraheren.

Voor gebruik binnen een organisatie is de definitie van het NFI zeer beperkt. Zo wordt de term onderzoeken niet verder uitgewerkt en blijft het doel waarvoor het bewijs wordt geëxtraheerd onduidelijk. Dientengevolge hebben wij ervoor gekozen een andere definitie te hanteren:

Het doen van onderzoek door middel van al dan niet geautomatiseerde zoekslagen in geautomatiseerde systemen of gegevensverzamelingen naar het onbevoegd gebruik van systemen dat kan leiden tot schade voor de ondememing. Het bewijs dat gedurende het onderzoek wordt vergaard dient zowel voor mogelijke vervolging als ter beperking van de schade.

Uit de hier genoemde definitie komt naar voren dat gedurende het onderzoeksproces handmatig of met behulp van tools systemen worden doorzocht. Het onderzoek kan betrekking hebben op als zodanig gedefinieerde gegevensverzamelingen, zoals een bijvoorbeeld een database, of op onderliggende gegevensverzamelingen zoals bijvoorbeeld het filesysteem van een server. Daarnaast dient het onderzoek in onze definitie een tweeledig doel. In de eerste plaats zal de organisatie de schade als gevolg van het incident zoveel mogelijk willen beperken. Over het algemeen is hiervoor een goed inzicht nodig in de aard van het incident en de oorzaak van de totstandkoming hiervan. In de tweede plaats dient uit het onderzoek bewijsmateriaal te worden geéxtraheerd voor de mogelijke vervolging van de aanstichter van het incident.

Incident response
Incident response in de breedste zin kan worden gezien als de wijze waarop organisaties omgaan met incidenten. Een dergelijke brede definitie wordt gehanteerd in, waar incident response wordt gedefinieerd als “actions taken to deal with an incident that occurs”.

Merk bij deze definitie op dat het incident response proces onafhankelijk wordt gedefinieerd van enige vorm van automatisering. Deze definitie omvat zowel de traditionele als de computergerelateerde incidenten. Mandia definieert incident response veel specifieker in termen van de doelen die met het proces bereikt dienen te worden:

- *Confirms or dispels whether an incident occurs;*
- *Promotes the accumulation of accurate information;*
- *Establishes controls for proper retileval and handling of evidence;*
- *Protects privacy rights established by law and policy;*
- *Minimizes disruption to business and network;*
- *Operations;*
- *Aflows for legal or citdi recriminations against perpetrators;*
- *Provides accurate reports and useful recommendations.*

Bij deze laatste vorm zien we dat het proces al veel strakker wordt gedefinieerd en in wezen al de basiselementen bevat van de activiteiten die gedurende het proces moeten worden uitgevoerd.

Hierna zullen wij echter de eerste definitie van incident response hanteren, uitgaande van computer gerelateerde incidenten. Incident response behelst alle noodzakelijke activiteiten voor de afhandeling van een incident.

Bewijsvergaring
In deze paragraaf wordt nader ingegaan op de eerste vraag: welke middelen staan de werkgever ter beschikking om bewijs te verzamelen inzake een (vermeend) incident.

In een aantal wetten zijn de regels opgenomen die gehanteerd moeten worden om op rechtmatige wijze de handelingen van personen te mogen controleren. De belangrijkste wetten in dit kader zijn de Grondwet, de WOR (Wet op Ondernemingsraden), de Wet Bescherming Persoonsgegevens (WBP) en de Wet Computer Criminaliteit II.

In tegenstelling tot de wetgeving in de Verenigde Staten is in de Europese wetgeving de bescherming van de privacy veel stringenter vastgelegd. Zoals reeds gesteld, wordt onrechtmatig verkregen bewijs afgestraft met bewijsuitsluiting. Veelal zal in dit geval de privacy zijn geschonden. Aangezien het controleren van de handelingen van medewerkers een inbreuk op de privacy kan betekenen (en dus uitmond in onrechtmatig verkregen bewijs) wordt onderstaand eerst uitgebreid ingegaan op de juridische aspecten van het begrip privacy.

Privacy wetgeving algemeen
Privacy is een grondrecht en is vastgelegd in de Grondwet en in internationale verdragen als het Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) en het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR). De Wet Bescherming Persoonsgegevens (WBP) is rechtstreeks afgeleid uit artikel 10 van de Grondwet.

In werktijd geniet men niet dezelfde vrijheden als daarbuiten. De arbeidsverhouding brengt zekere beperkingen met zich mee voor de grondrechten van werknemers. Voor het loon dat een werknemer ontvangt verplicht hij zich werkzaamheden te verrichten waarbij de aanwijzingen van de werkgever dienen te worden opgevolgd. Dit betekent dat de werknemer in zekere mate beperkt wordt in zijn bewegings-, handelingsvrijheid en in zijn vrijheid van meningsuiting. Dit geldt ook voor zijn recht op privacy. Dit houdt echter niet in dat een werkgever alles van zijn medewerkers mag verlangen en de medewerker geen beroep meer kan doen op zijn grondrechten. Dit geldt ook voor de controle van het email- en internetgebruik van werknemers. Een werkgever moet volgens de wet, bij het nastreven van zijn belang zich gedragen als goed werkgever (art. 7:611 van Burgerlijk Wetboek). Dit houdt onder andere in dat de werkgever de rechtsbeginselen van de subsidiariteit en proportionaliteit dient toe te passen.

Art. 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) bepaalt dat een ieder recht heeft op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. De verzamelterm voor deze niet duidelijk te scheiden rechten is het "recht op privacy". Werknemers hebben een gerechtvaardigd belang om ook gedurende het uitvoeren van bedrijfsmatige activiteiten relaties met andere mensen aan te kunnen gaan, zonder dat inmenging van de werkgever plaatsvindt. Een zekere mate van vrijheid om met anderen al dan niet persoonlijk te kunnen communiceren is in dat kader onontbeerlijk. Artikel 8 EVRM beschermt het individu niet alleen tegen inbreuken op dergelijke privacyaanspraken door de overheid maar ook wanneer deze afkomstig zijn van particulieren en werkgevers. Bovendien zijn de verdragsstaten verplicht om het recht op privacy zo goed mogelijk te waarborgen in hun wetgeving, rechtspraak en bestuur. Voor ieder afzonderlijk geval dient te worden vastgesteld of het recht op privacy is aangetast. De kernvraag is of er sprake is van een inbreuk op de privacy indien iemand dit beweert. Dit is met name van belang wanneer er elektronisch onderzoek naar een individu wordt ingesteld.

Bij het uitvoeren van e-mail controles wordt de vrijheid om met anderen te communiceren aangetast. Indien gegevens worden vastgelegd die inzicht bieden in de activiteiten van de werknemer, raakt dit niet alleen diens persoonlijke levenssfeer maar ook de arbeidsverhouding in het algemeen; het kan in zekere zin de handelingsvrijheid van de werknemer beperken om de werkzaamheden naar eigen inzicht uit te voeren.

De werkgever dient een goede reden te hebben om dergelijke vrijheden in te perken en dient zo terughoudend mogelijk te zijn bij de implementafie van maatregelen (de reeds genoemde beginselen van proportionaliteit en subsidiariteit. Uit de jurisprudentie op artikel 8 EVRM is eveneens duidelijk dat de inbreuk kenbaar moet zijn voor de betrokkene. Heimelijke controle waaraan geen waarschuwing aan vooraf is gegaan of als uitvoering van een geldende gedragscode is in stiijd met deze regels.

De volgende juridische kenmerken zijn van toepassing op het begrip privacy:
1. Privacy is een relatief recht, d.w.z. als je denkt dat je privacy geschaad is hoeft de rechter nog niet zo te oordelen. De rechter weegt de belangen van partijen af bij de vaststelling van zijn oordeel.

2. Privacy is een individueel recht, d.w.z. dat de meerderheid de minderheid niet kan wegdrukken. Indien bijvoorbeeld de meerderheid van de werknemers geen bezwaar heeft tegen het plaatsen van een TV-circuit op hun afdeling mag een werkgever hiertoe niet overgaan indien een minderheid (dh kan ook één medewerker zijn) wèl bezwaar heeft.

3. Privacy is niet ruimtelijk begrensd, d.w.z. privacy geldt niet alleen in huis maar ook op het werk en in het publieke domein (op straat).

Privacybescherming via formele wetgeving
De bescherming van de privacy is zowel in het privaatrecht als het publiekrecht verankerd. De privacy wordt geschonden indien aangetoond kan worden dat de wettelijke norm overschreden is. Het overschrijden van de wettelijke norm is de juridische grondslag om de vermeende schending van de privacy te beëindigen of om een schadevergoeding toegewezen te krijgen.

Prlvaatrechtelijke grondslagen
In het privaatrecht, ook wel burgerlijk recht of civielrecht genoemd, wordt de rechtsverhouding geregeld tussen (natuurlijke- en rechts-) personen onderling. In toenemende mate wordt er wet- en regelgeving ontwikkeld die de privacyproblematiek in arbeidsverhoudingen regelt. Indien een persoon meent dat zijn privacybelangen geschonden zijn moet hij zeifl actie ondernemen om zijn gelijk te krijgen en kan hij zich beroepen op drie privaatrechtelijke grondslagen, te weten Aansprakelijkheidsrecht, Wet op de Ondernemingsraden (WOR) en het Arbeidsrecht.

Hierna worden de drie privaatrechtelijke grondslagen besproken.

Aansprakelijkheidsrecht
In art. 6:162 BW wordt de onrechtmatige daad geregeld. Onder een onrechtmatige daad wordt onder meer een inbreuk op het recht van een ander verstaan.
De inbreuk kan zowel betrekking hebben op een vermogensrecht of het recht op privacy. Indien iemand een beroep doet op dit recht moet hij schade hebben geleden. In het geval van een inbreuk op de privacy zal er veelal sprake zijn van immateriële schade.

Wet op de Ondernemingsraden (WOR)
Op 4 maart 1998 is de herziene Wet op de Ondernemingsraden (WOR) in werking getreden. De voor ons van belang zijnde wijzigingen in de WOR hebben voomamelijk betrekking op zogenaamde personeelsvolgsystemen (o.a. videocameratoezicht, toegangsregistratiesystemen, personeelsbestanden en digitale telefooncentrales). Een aantal onderdelen van de gewijzigde WOR zijn van belang:

- *In Hoofdstuk IV (Bijzondere bevoegdheden van de Ondernemingsraad) wordt in art. 25 het adviesrecht beschreven. Dit adviesrecht heeft o.a. betrekking op besluiten die kunnen leiden tot de invoering van geautomatiseerde systemen die de werkzaamheden of het toezicht hierop in belangrijke mate kunnen veranderen.*

- *In hetzelfde hoofdstuk wordt in art. 27 WOR het instemmingsrecht van de ondernemingsraad geregeld voor een tweetal regelingen:*
  - *Het instemmingsrecht omtrent "het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen".*
  - *Het instemmingsrecht "inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag en prestaties van de in de onderneming werkzame personen". Dit artikel betreft niet alleen specifiek voor dit doel ontwikkelde systemen (personeelsvolg- en informatiesystemen) maar ook de bedrijfsmiddelen die als zodanig gebruikt kunnen worden, bijvoorbeeld het loggen van uitgaande telefoongesprekken bij een digitale telefooncentrale.*

Voor de algemene regeling die de ondernemer wil treffen inzake de verwerving van persoonsgegevens is de instemming van de ondernemingsraad vereist. Indien de werkgever een individu wil controleren omdat deze verdacht wordt van bijvoorbeeld het privé bellen naar het buitenland is geen instemming van de Ondernemingsraad vereist.

De werkgever moet dus in overleg treden met zijn medewerkers indien hij regelgeving wil opstellen die mogelijk de privacy kunnen aantasten. De ondernemingsraad zal het instemmingsrecht gebruiken om over de condities te onderhandelen. Indien beide partijen overeenstemming bereikt hebben moeten de afspraken worden vastgelegd. De afspraken kunnen de volgende onderdelen betreffen:

- *Doelstelling van de maatregel;*
- *Wijze waarop de maatregel wordt toegepast - Waarborgen ter voorkoming van misbruik;*
- *Hoe de geheimhouding geregeld wordt;*
- *Welke gegevens worden vastgelegd;*
- *Welke sancties kunnen worden opgelegd.*

Nadat in goed overleg de afspraken zijn vastgelegd kan een datum vastgesteld worden waarop de regeling van kracht wordt. Indien echter een individuele medewerker Vindt dat zijn privacy belangen geschaad worden door de regeling kan deze alsnog naar de rechter stappen. Zoals in het voorgaande gesteld is privacy immers een individueel recht.

Arbeidsrecht
Nadat de herziene WOR in werking is getreden zijn de bepalingen over arbeids- of bedrijfsreglement in het Burgerlijk Wetboek geschrapt. Het arbeids- of bedrijfsregiement wordt veelal - in de vorm van een personeelsgids - als onderdeel van de arbeidsovereenkomst opgenomen. Om als werkgever flexibel te kunnen blijven handelen werd in de arbeidsovereenkomst opgenomen dat de werkgever het recht had het arbeids- of bedrijfsregiement eenzijdig te kunnen veranderen. Sinds de inwerkingtreding van de herziene WOR is dit niet meer mogelijk. In het arbeidsrecht zijn geen specifieke privacybepalingen vastgelegd. In zijn algemeen geldt dat de werkgever zich als goed werkgever dient te gedragen (art. 7:611 van Burgerlijk Wetboek). Dit houdt in dat de hij verplicht is datgene te doen en na te laten, wat een goed werkgever in gelijke omstandigheden behoort te doen en na te laten.

Publiekrechtelijke grondslagen
In het publiekrecht wordt de verhouding tussen natuurlijke- en/of rechtspersonen en de overheid geregeld. De overheid ziet er op toe dat de wetten en regelingen op een juiste wijze worden toegepast. De belangrijkste wetten met betrekking tot de privacy zijn de wetten waarin de regels zijn vastgelegd inzake het verzamelen, vastleggen en het gebruik van persconsgegevens.

Wetgeving over het verzamelen, vastleggen en gebruik van persoonsgegevens
Naar aanleiding van de richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens is in Nederland op 1 september 2001 de wet Bescherming Persoonsgegevens (WBP) in werking getreden.

Er geldt een overgangsregeling van 1 jaar. Dit betekent dat reeds bestaande zaken vanaf 1 september 2002 aan de nieuwe privacy wet moeten voldoen. De WBP is de opvolger van de wet Persoonsregistratie (WPR) die op 1 juli 1989 van kracht werd.

Wetboek van Strafrecht
]n het Wetboek van Strafrecht is een aantal gedragingen strafbaar gesteld die de privacy kunnen aantasten. De belangrijkste strafbaar gestelde gedragingen zijn:

- *Het heimelijk opnemen van gesprekken;*
- *Het aftappen of opnemen van gegevens;*
- *Het in het bezit hebben van een medium waarop gegevens staan die heimelijk zijn verkregen;*
- *Het opzettelijk bekend maken van gegevens aan derden waarvan men weet of vermoedt dat deze wederrechtelijk zijn verkregen.*

De strafbepalingen hebben met name betrekking op situaties waarin bij betrokkene niet bekend is dat zijn privacy geschonden wordt. Een werkgever moet zich realiseren dat dit kan leiden tot onrechtmatig verkregen bewijs.

Onrechtmatig verkregen bewijs kan op zich betrouwbaar zijn maar vanwege de wijze waarop dit bewijs verkregen is kan dit leiden tot bewijsuitsluiting. Bij de afhandeling van een incident is het dus van uiterst belang dat het verzamelen van bewijsmateriaal op rechtmatige wijze geschiedt.

Wet Bescherming Persoonsgegevens
Gezien het belang van deze wet voor deze scriptie hebben wij echter besloten een separate paragraaf aan dit onderwerp te wijden.

De WBP heeft betrekking op persoonsgegevens en bevat voorschriften van dwingend recht hetgeen wil zeggen dat het niet is toegestaan bepalingen in een contract op te nemen die in strijd zijn met de WBP. Dit betekent dat er voor de werkgever vrijwel geen mogelijkheden zijn om eigen beleid te ontwikkelen op de WBP.
De WBP is voor digitaal onderzoek met name van belang indien, met behulp van geautomatiseerde systemen, gegevensverzamelingen over personen worden aangelegd en indien er digitaal beeld- en geluidsfragmenten worden opgeslagen. Tevens is de WBP van belang indien er naar aanleiding van een incident een medewerker wordt ontslagen. In sommige gevallen is de reden voor ontslag op staande voet evident (bijvoorbeeld greep uit de kas). In andere gevallen echter hoeft een afzondertijk incident niet van een dusdanige zwaarte te zijn dat ontslag op staande voet gerechtvaardigd is. Bij het herhaald voorkomen van incidenten kan dit echter wel het geval zijn. In de jurisprudentie is terug te vinden dat een goede registratie van incidenten noodzakelijk is. Uit de registratie moet blijken om welke incidenten het betrof en dat de betrokkene hiervoor een officiële waarschuwing heeft gekregen.

Verwerking van Persoonsgegevens
Zoals reeds aangegeven richt de WBP zich op de verwerking van persoonsgegevens. In de zin van de wet is een persoonsgegeven een gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon. Hierbij kan onderscheid gemaakt worden in direct of indirect identificeerbare persoonsgegevens. Voorbeelden van direct identificeerbare persoonsgegevens zijn: naam, geboortedatum adres, vingerafdruk. Voorbeelden van indirect identificeerbare persoonsgegevens zijn de stem en het kenteken van een motorvoertuig. In dit geval zijn een aantal handelingen noodzakelijk om de gegevens van een persoon te kunnen afleiden. In de wet wordt aangegeven dat indien er te veel moeite moet worden gedaan om de gegevens van een persoon te achterhalen er geen sprake is van een persoonsgegeven. Deze vage regelgeving maakt het in sommige gevallen moeilijk om de WBP in de praktijk correct toe te passen.

Bij de WBP is het van belang of persoonsgegevens geheel of gedeeltelijk geautomatiseerd verwerkt worden. Indien de persoonsgegevens niet geautomatiseerd verwerkt worden, geldt de wet alleen indien de persoonsgegevens in een bestand worden opgenomen. In dit verband is alleen sprake van een bestand indien er aan een aantal criteria wordt voldaan, te weten:

- *de persoonsgegevens moeten onderdeel uitmaken van een gestructureerd geheel;*
- *het bestand moet volgens bepaalde criteria toegankelijk zijn;*
- *het bestand moet betrekking hebben op verschillende personen.*

Naar aanleiding van de definitie van een bestand is de conclusie gerechtvaardigd dat indien een groot aantal gegevens over één persoon worden opgeslagen er in de zin van de wet geen sprake is van een bestand. Indien de samenhang van verschillende dossiers ontbreekt en dus in feite elke dossier op zich staat is er ook geen sprake van een bestand. Analoge videocamerasystemen vallen ook niet onder het begrip bestand omdat de mogelijkheid om het camerasysteem systematische toegankelijk te maken ontbreekt.

Onder verwerking van persoonsgegevens wordt verstaan het verzamelen, het vastleggen, het ordenen, het bewaren, het raadplegen, het ter beschikking stellen en het met elkaar in verband brengen van persconsgegevens. In relatie tot digitaal onderzoek betekent dit dat het "digitaal" observeren (o.a. in- en uitloggen van de werknemer, het tracen van een medewerker m.b.v. een audit trail, het monitoren van e-mail berichten) in principe onder de werking van de WBP vallen. Het is dus noodzakelijk dat de gegevensverwerking voldoet aan de algemene beginselen van gegevensverwerking. Bij de verwerking van persoonsgegevens geldt te allen tijde dat de gegevens alleen mogen worden verwerkt indien dat noodzakelijk is voor de behartiging van een gerechtvaardigd belang (noodzaakscriterium). In art. 7 WBP wordt de zogenaamde doelbinding beschreven. Dat wil zeggen dat persoonsgegevens alleen mogen worden verzameld voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen.

In artikel 8 WBP wordt dit in relatie gebracht met het recht op privacy en wordt gesteld dat persoonsgegevens slecht mogen worden verwerkt indien:

> *".. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert".*

Volgens de wet dient er formeel een verantwoordelijke aangesteld te worden die bevoegd is het doel van de verwerking van persoonsgegevens vast te stellen. De verantwoordelijke kan de verwerking van de persoonsgegevens overdragen aan een derden, de "verwerker". De verantwoordelijke blijft echter aansprakelijk voor het na komen van de algemene beginselen van gegevensverwerking. Naast deze zorgplicht heeft de verantwoordelijke ook een meidingsplicht bij het College Bescherming Persconsgegevens (voorheen Registratiekamer). Tevens dient de verantwoordelijke de persoon waarover gegevens worden vastgelegd hierover te informeren. Indien de verantwoordelijke in gebreke blijft kan het College hem een bestuurlijke boete opleggen van ten hoogste EUR 4.500,--.

Een (digitaal) onderzoek zou feitelijk niet uitgevoerd kunnen worden als te allen tijde aan de informatieplicht moet worden voldaan. In artikel 43 WBP wordt aangegeven dat niet aan de informatieplicht hoeft te worden voldaan indien dit in het belang is van:
a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;
c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn;
e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Het bovenstaande geldt ook voor het recht van inzage dat de betrokkene normaal heeft.

Internationale aspecten
In art. 76 t/m 78 WBP wordt het gegevensverkeer met landen buiten de Europese Unie behandeld. Een van de beginsels die hierbij gehanteerd worden is dat persoonsgegevens niet zonder toestemming van de betrokkene doorgegeven mogen worden naar een land buiten de Europese Unie waar geen passend beschermingsniveau geldt. Informatie-uitwsseling tussen landen van de Europese Unie is zonder meer mogelijk. De vestigingsplaats van de multinational bepaalt of do Nederlandse wet of de wetgeving van een derde land van toepassing is. De plaats waar het informatiesysteem zich bevindt is dus niet van belang.

Forensich digitaal bewijs
Indien iemand meent dat hem onrecht is aangedaan moet er bewijs verzameld worden waarmee de rechter overtuigd kan worden van het gestelde aangedane onrecht. Ten aanzien van het aandragen van elektronisch bewijsmatertaal wordt door Franken en Kemna in gesteld, dat:

"….in Nederland is er niets op tegen om elektronisch bewijsmateriaal in juridische procedures aan te dragen. Dit vloeit voort uit het vrije bewijsstelsel dat hier ter lande wordt gehanteerd. Het bewijs van gestelde feiten kan in Nederland volgens arlikel 179 lid 1 Rv met alle middelen worden geleverd tenzij de wet anders bepaalt. De rechter zal vervolgens bepalen wat de waarde is van het geleverde bewijs."

Het is frustrerend indien er veel moeite gedaan is om vermeende frauduleuze handelingen van een verdacht persoon te achterhalen en vervolgens het verkregen bewijsmateriaal door de rechter ter zijde wordt gelegd omdat dit onrechtmatig verkregen zou zijn. Vandaar dat in deze paragraaf aandacht wordt besteed aan de wijze waarop deugdelijk bewijsmaterlaal kan worden verkregen. In het voorgaande is uitgebreid aandacht besteed aan de Wet Bescherming Persoonsgegevens aangezien het in de praktijk nog al eens blijkt dat, wegens het schenden van de privacy, de rechter oordeelt dat het bewijsmaterlaal onrechtmatig verkregen is.

In Nederland is de rechter vrij in de waardering van het door beide partijen ingebrachte bewijsmateriaal. Het is dus zaak de rechter ervan te overtuigen dat de gedaagde de gestelde strafbare feiten ook daadwerkelijk gepleegd heeft. Voor een werkgever gelden de volgende belangrijke uitgangspunten voor het verkrijgen van deugdelijk bewijsmateriaal zijn:

- *Voer de handelingen m.b.t. het vergaren van digitaal bewijsmateriaal uit binnen het hiertoe wettelijk gestelde kader (m.n. Wet Bescherming Persoonsgegevens);*
- *Handel in de geest van een goed werkgever;*
- *Zie erop toe dat de basisprincipes van subsidiaritelt en proportionalitelt worden toegepast;*
- *Bouw een dossier op en geef de medewerker een officiële waarschuwing indien hij zich niet aan de regels houdt.*

Voorts kan het in sommige gevallen nuttig zijn een overeenkomst af te sluiten voordat een zakelijke relatie wordt aangegaan. Franken definieert een bewijsovereenkomst als een afspraak tussen contractspartijen met betrekking tot hun bewijspositie in geval van een eventueel proces

Technische aspecten

Inleiding

Wanneer een incident heeft plaatsgevonden en binnen de onderneming is geëscaleerd zullen de betrokkenen zoveel mogelijk bewijs en informatie gaan verzamelen. Ook hierin kunnen technische hulpmiddelen een rol spelen, derhalve welke technische hulpmiddelen staan de organisatie ter beschikking bij het analyseren en onderzoeken van een incident.

Bij het vergaren van informatie kan globaal onderscheid worden gemaakt tussen informatievergaring op systeemniveau en op netwerkniveau. Hierna zal alleen het forensisch onderzoek op systeemniveau beschreven worden.

Systeemonderzoek

In deze paragraaf zullen wij de verschillende mogelijkheden behandelen voor het doen van onderzoek binnen systemen waarop of waarmee (vermoedelijk) een incident heeft plaats gevonden, oftewel digitaal forensische onderzoek. Door het hierin gespecialiseerde bedrijf Fox-IT wordt een digitaal forensisch onderzoek gedefinieerd als:

> *"…het onderzoeken en analyseren van digitale informatie of digitale sporen van informatie in welke vorm dan ook, met als doel digitale delicten zoals fraudes op te lossen."*

Eén van de belangrijkste aspecten bij het onderzoeken van systemen is de bewijsvoering. Technische is het haalbaar om heel veel informatie uit systemen te halen. Wanneer de informatie echter forensische doeleinden dient (met andere woorden wanneer de informatie als bewijs in een rechtszaak gebruik wordt worden), zullen bepaalde zekerheden moeten worden ingebouwd. De juridische aspecten van deze bewijsvergaring zijn eerder al behandeld.

Bij de uitvoering van systeemonderzoeken kunnen verschillende hulpmiddelen worden gebruik te weten:

- *Disk-cloning software;*
- *Integriteitsgarantie;*
- *Zoekprogrammatuur;*
- *Geïntegreerde programmatuur.*

Deze verschillende hulpmiddelen zullen in het vervolg van deze paragraaf verder worden toegelicht.

Disk-cloning software

Om uit systemen verkregen gegevens als bewijsmateriaal te kunnen opvoeren moet men beschikken over een exacte weergave van de originele informatie. Eén van de kenmerken van moderne systemen is echter dat de betreffende informatie (bijvoorbeeld configuratie-informatie en loggegevens) continu worden aangepast door het systeem. Voor het doen van forensisch onderzoek is het dus noodzakelijk een systeem voor onbepaalde tijd te bevriezen, waarna men opzoek kan gaan naar de noodzakelijke informatie. Ook dit zoeken zelf kan echter de informatie op het betreffende medium al veranderen. Om dit te voorkomen wordt over het algemeen gebruik gemaakt van zogenaamde disk-cloning software. Dergelijke programmatuur maakt bit-voor-bit een exacte kopie van een bepaald medium, waarna onderzoek kan plaatsvinden op de kopie en niet op het originele systeem. Eventueel kan hiervoor ook gebruik worden gemaakt van standaard back-up programmatuur hoewel hierbij geen garantie bestaat dat een 100% exacte kopie wordt gemaakt, welk feit bij een rechtszaak mogelijk problemen op kan leveren.

Een bekend voorbeeld van disk-cloning software welk een exacte kopie van een medium kan maken is SafeBack van het bedrijf NTI.

Integriteitsgarantie
Zoals hierboven besproken is het essentieel om een integere kopie te maken van gegevens op systemen. Voor de rechter kan het echter ook noodzakelijk blijken om aan te tonen dat de betreffende gegevens niet zijn veranderd of aangepast. Hiervoor kan gebruik worden gemaakt van cryptografische checksums die over de originele gegevens worden uitgerekend. De uitkomsten van deze berekening kunnen vervolgens bij een vertrouwde partij in bewaring worden gegeven.

Een voorbeeld van software voor het uitvoeren van dergelijke checksum berekeningen is het programma CRCMD5, wederom van het bedrijf NTI.

Zoekprogrammatuur
Moderne harde schijven bevatten een veelheid aan informatie (grootte van 30 GB of meer zijn meer regel dan uitzondering), wat betekent dat het zoeken naar een bepaald stukje informatie zeer lang kan duren. Om dit probleem op te lossen zijn verschillende zoek-tools beschikbaar.

Bij het zoeken naar gegevens op media zijn twee aspecten van belang, te weten:
- *Bepalen naar welke informatie gezocht moet worden;*
- *De wijze van zoeken.*

Om te weten naar welke informatie gezocht moet worden zal eerst inzicht moeten bestaan in de aard van het incident. Vervolgens kunnen de meest waarschijnlijke scenario's voor de uitvoering van het incident worden opgesteld, aan de hand waarvan kan worden bepaald naar welke specifieke informatie het CSIRT-team moet gaan zoeken.

Om de grote hoeveelheid informatie efficiënt te doorzoeken is een goede zoek-tool onmisbaar. Naast het zoeken op standaard strings zou een dergelijke tool ook geavanceerdere opties moeten bevatten, bijvoorbeeld zoeken aan de hand van reguliere expressies en het gebruik van wildcards. De bekendste tool op dit gebied is DiskSearchPro, wederom geleverd door het bedrijf NTI.

Geïntegreerde programmatuur
Verschillende commerciële leveranciers hebben geconstateerd dat digitaal forensisch onderzoek vaak plaatsvindt met een verzameling losse programmaatjes waartussen geen of weinig verband te onderkennen valt. Een dergelijke werkwijze komt de efficiency van onderzoeken niet ten goede. De oplossing hiervoor is gevonden in het ontwikkelen van geïntegreerde suites waarin de meest voorkomende technische handelingen zijn geïntegreerd. Twee bekende voorbeelden van dergelijke suites zijn DriveSpy van het bedrijf Digital Intelligence en Byte Back van Tech Assist. Geïntegreerde software suites bevatten over het algemeen een verzameling van de hierboven genoemde functionaliteit voor het kopiëren van gegevens, het digitaal tekenen van deze gegevens, het zoeken binnen deze gegevens en het terugzetten van kopieën op schone systemen. Hieraan hebben de verschillende leveranciers nog specifiek, vaak platform afhankelijke, functionaliteit toegevoegd. DriveSpy bevat bijvoorbeeld functionaliteit voor het benaderen van de gegevens van veel verschillende filesystemen en biedt bijvoorbeeld de mogelijkheid om verborgen bestanden op te sporen.

Normenkader (een eerste aanzet)

Inleiding
In de voorgaande hoofdstukken is de theorie van incident response en forensisch c.q. digitaal onderzoen en bewijsvergaring de revue gepasseerd, ingedeeld naar organisatorische, juridische en technische aspecten. Op basis van deze theorie wordt in dit hoofdstuk voor ieder van deze drie aspecten een normenkader opgesteld. Deze normenkaders stelt een organisatie in staat de status van incident response en forensisch onderzoek binnen een organisatie vast te stellen.

Organisatorische normenkader
1. *De organisatie beschikt over een geaccepteerd en geaccordeerd informagebeveiligingsbeleid.*

2. *De functie informatieboveiliging is belegd in do organisatie waarbij onderscheid wordt gemaakt tussen werkzaamheden op strategisch, tactisch en operationeel niveau.*

3. *De werkwijzen van de informatiebeveiligingsfunctie zijn vastgelegd informele procedures en werkinstructie.*

4. *De organisatie beschikt over een standaard methodiek voor het uitvoeren van risico-analyses.*

5. *Voor ieder nieuw informatiesysteem en voor belangrijke aanpassingen aan bestaande informatiesystemen wordt een risico-analyse uitgevoerd.*

6. *De onderneming heeft een CSIRT-organisatie opgezet, inclusief de richtlijnen en procedures voor escalatie.*

7. *De CSIRT-organisatie werkt conform een standaard methodiek die is vastgelegd in procedures en werkwijzen.*

8. *Er is een standaard rapportage structuur gedefinieerd met betrekking tot incidenten.*

9. *De organisatie beschikt over een intern- en extern communicatieplan waarin de omgang met incidenten specifiek wordt behandeld.*

10. *Er wordt voldoende aandacht besteed aan de opleiding van medewerkers.*

11. *Alle noodzakelijke documentatie (inclusief vakliteratuur) is beschikbaar voor de CSIRT-organisatie.*

Juridische normenkader
1. *Bij de inrichting en de uitvoering van het incident response proces dient de werkgever zich te houden aan de wet en regelgeving. In dit verband wordt met name gewezen op de Europese richflijnen, de Wet Bescherming Persoonsgegevens en de regelgeving van de toezichthoudende instanties.*

2. *De werkgever dient zich als goed werkgever te gedragen. Dit houdt o.a. in dat de principes van subsidiariteit en proportionaliteit toegepast dienen te worden.*

3. *Er dient een dossier te worden opgebouwd van de incidenten die zich in het verleden hebben voorgedaan. In vele gevallen is het plegen van meerdere incidenten noodzakelijk alvorens verregaande disciplinaire maatregelen kunnen worden genomen. Om incidenten uit het verleden te kunnen aantonen is het opbouwen van een dossier noodzakelijk.*

4. *De medewerker dient na het plegen van een incident, dat niet zwaar genoeg is voor het nemen van verregaande disciplinaire maatregelen, een officiële waarschuwing te krijgen. Indien het tot een rechtszaak komt is het voor de rechter van belang te weten of de verdachte officieel gewaarschuwd is voor het plegen van incidenten.*

Technisch normenkader

1. *Zowel op systeem als op applicatieniveau worden van alle relevante events loggingsgegevens bijgehouden.*

2. *Er is een systeem aanwezig om do gegevens uit de logbestanden op eenduidige wijze te ontsluiten en toegankelijk te maken. Hierbinnen kan onderscheid worden gemaakt tussen standaard queries en ad-hoc vraagstellingen.*

3. *De organisatie heeft een intrusion detection systeem geïmplementeerd en de signalen uit dit systeem worden op adequate wijze gecommuniceerd met CSIRT-organisatie.*

4. *Kritieke informatiesystemen beschikken over een eigen signaleringsfunctie met betrekking tot mogelijke incidenten, waarmee afwijkend gedrag kan worden gesignaleerd.*

5. *De organisatie beschikt over hulpmiddelen voor het uitvoeren van systeemonderzoeken. Mogelijke onderdelen hiervan zijn disk-cloning software, integriteitsgarantie software en specialistische zoekprogrammatuur.*

6. *De organisatie beschikt over hulpmiddelen voor het uitvoeren van netwerkonderzoeken.*

7. *Op kritische externe verbindingen worden bijvoorbeeld honeypots gebruikt om aanvallers te misleiden en informatie te verzamelen over de aanvaller en het type aanval.*