More-Secure®
IT Security Architecture

WHITE PAPER

Informatiebeveiliging: hype of noodzaak?

COLOFON

Titel	Informatiebeveiliging: hype of noodzaak?
Ondertitel	-
Versie, datum	Definitief versie 1.2, 19 februari 2007
Referentie	White paper Informatiebeveiliging MS def 1.2
Auteur	Frans M. Kanters
Opdrachtgever	More-Secure BV
Laatste versie bewerkt door	Ernst J Mellink op 19 februari 2007
Bestandsnaam	White paper Informatiebeveiliging MS def 1.2
Contactadres voor deze publicatie	More-Secure b.v. Mailto: info@More-Secure.nl

INHOUDSOPGAVE

FIGUREN

1 INTRODUCTIE

Informatiebeveiliging kan zich de afgelopen jaren verheugen in een toenemende belangstelling van organisaties. De vraag “Informatiebeveiliging: hype of noodzaak?” doemt dan ook snel op. Is deze vraag legitiem? More-Secure beantwoordt deze vraag met een volmondig “Ja, informatiebeveiliging is een noodzaak!”. Als argument voor dit antwoord hoeft u alleen maar een landelijk dagblad te raadplegen of een nationaal of internationaal journaal op televisie te bekijken. Elke dag verschijnen korte en lange berichten die te maken hebben met informatiebeveiliging. De berichtgevingen variëren van geheime lijsten van politieke leiders tot het hacken van de Website van een Europees veiligheidsinstituut. Kortom, voorbeelden te over. Nu zijn dit wel een heel voor de hand liggende argumenten. Door middel van een aantal stellingen wil More-Secure aangeven dat de argumentatie veel dieper gaat. Dieper dan menig individu denkt. Deze stellingen zijn wellicht arbitrair, toch maakt het duidelijk waarom informatiebeveiliging zo belangrijk is of zou moeten zijn: onze maatschappij is namelijk zeer afhankelijk geworden van Informatie en Communicatietechnologie, kortweg ICT.

De stellingen luiden als volgt:

1. **Uitval van ICT door beveiligingsincidenten veroorzaken directe en indirecte kosten.**
   ICT neemt een niet te onderschatte rol in binnen organisaties. Primaire bedrijfsprocessen leunen zwaar op ICT. Organisaties ontlenen hun bestaansrecht aan ICT, het vormt een van de hoekstenen voor organisaties. Deze rol wordt almaar belangrijker voor organisaties.

2. **Het Internet wordt steeds vaker gebruikt voor gegevensuitwisseling tussen organisaties.**
   Als drijfveer is het Internet er de oorzaak van dat organisaties steeds vaker externe digitale relaties aan gaan met instanties en bedrijven in de omgeving waarin organisaties opereren.

3. **Organisaties hebben hun wettelijke verplichting en maatschappelijke verantwoordelijkheid als het gaat om het vastleggen van gegevens.**
   Vanuit zowel wettelijk verplichting als maatschappelijk oogpunt zijn organisaties verplicht bepaalde zaken rondom de digitale verwerking van gegevens vast te leggen in procedures, richtlijnen en maatregelen.

4. **Globalisering leidt tot nieuwe inzichten en bruikbare toepassingen, maar levert ook valkuilen op.**
   Technologische ontwikkelingen veroorzaken ongekende mogelijkheden als het gaat om afstanden en tijdsverschillen: het fenomeen “24-uurs economie” is aan een niet te stoppen opmars begonnen.

5. **Organische groei van organisaties genereert nieuwe beveiligingsbedreigingen.**
   Organische groei van organisaties leidt tot het niet inzichtelijk hebben van interne computernetwerken. Externe koppelingen met bijvoorbeeld analoge modems leiden tot ongewenste situaties.

6. **Nadenken over beveiliging verdient de voorkeur boven "quick & dirty".**
   Beveiliging is in. Het "even" snel implementeren van een oplossing na een beveiligingsincident kan tot nieuwe beveiligingsincidenten leiden. Het ageren tegen op zichzelf staande beveiligingsincidenten geeft geen garantie voor de totale beveiliging.

7. **Het aantal beveiligingsincidenten stijgt explosief.**
   Het aantal beveiligingsincidenten is het afgelopen jaar schrikbarend gestegen. Organisaties hebben veelal slechts het topje van de ijsberg scherp op het netvlies. Uit onderzoek is gebleken dat het gros van de beveiligingsincidenten zijn oorsprong binnen de organisaties zelf heeft.

8. **Steeds veranderende toepassingen vragen continue aandacht voor informatiebeveiliging.**
   Fenomenen en toepassingen als E-commerce en electronic banking staan volop in de belangstelling. Inherent hieraan ontstaan nieuwe beveiligingsvraagstukken en -problemen.

9. **De vergaande digitalisering roept om regelgeving.**
   Elke dag worden meer computernetwerken aan elkaar geknoopt. Het digitaliseren van informatie neemt hand over hand toe. De rechtsgeldigheid van digitale informatie staat volop in het voetlicht, en ter discussie. Binnen onafzienbare tijd zal de digitale maatschappij haar intrede doen.

10. **Huidige identificatiemethoden bieden onvoldoende houvast bij beveiligingsincidenten.**
    De identiteit van gebruikers van elektronische diensten is niet altijd bekend. Hierdoor kan men ingeval van een incident een digitale transactie niet of nauwelijks herleiden tot een natuurlijk persoon. Nieuwe technologische ontwikkelingen zoals bijvoorbeeld biometrie kunnen hier verandering in brengen.

Op basis van deze tien stellingen willen wij dieper ingaan op gevolgen en gerelateerde problemen bij het manifest worden van beveiligingsincidenten.

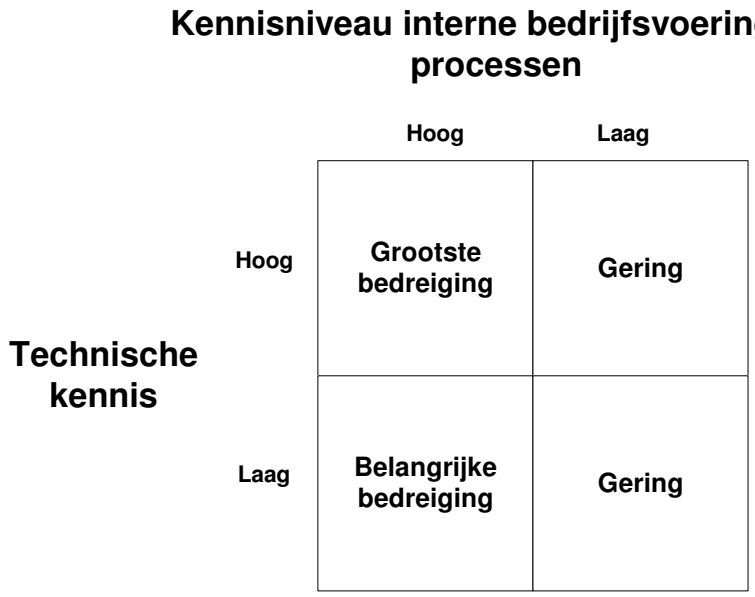
In een aantal stellingen wordt gesproken over de van afhankelijkheid van ICT. Uitval van deze ICT is desastreus. Wat zijn de gevolgen voor organisaties en maatschappij als de commerciële stroomvoorziening langdurig zou wegvallen? Beveiligingsmaatregelen zouden moeten voorzien in oplossingen op dit vlak.

Wettelijke kaders nopen organisaties tot het nemen van maatregelen. Het aanmaken en bewerken van persoonsgegevens legt automatisch een aantal verplichtingen bij de eigenaar van die gegevens. Denk bijvoorbeeld aan een gemeentelijke instantie die uitkeringen regelt, maar ook een bedrijf dat profielen van klanten bijhoudt ten behoeve van marketingdoeleinden.
Kortom maatregelen ter voorkoming van dreigingen of maatregelen die de gevolgen van deze dreigingen kunnen verhelpen zijn van eminent belang.

Een ander probleem vormt de identiteit van de gebruiker. Misschien is dit wel het belangrijkste argument om informatiebeveiliging door te voeren.

De huidige stand van de techniek maakt het mogelijk dat een gebruiker van elektronische diensten meerdere identiteiten aan kan nemen. Hierbij kan de elektronische transactie zelf volledig legitiem zijn; de gebruiker zelf heeft alleen een onjuiste identiteit, zonder dat dit uiteindelijk fout is. Op deze wijze kan het gebeuren dat een gebruiker met frauduleuze bedoelingen bijvoorbeeld een banktransactie initieert met een gestolen account, vervolgens een volslagen legitieme transactie uitvoert, en tot slot het geldbedrag op een "verkeerde" rekening laat terecht komen. Doordat de identiteit van een ander wordt aangenomen, en dus in feite misbruikt wordt, kan de daadwerkelijke pleger niet meer worden achterhaald.

Tot slot de kennis omtrent ICT zelf. Dit is een fors probleem. ICT is een zeer kennisintensief vak. Organisaties maken veelvuldig gebruik van externe specialisten als het gaat om het oplossen van ICT vraagstukken. Ziehier een potentieel gevaar. De combinatie van deze twee factoren laat namelijk een interessante uitkomst zien: medewerkers met veel kennis van de interne organisatie alsmede veel technische bagage zijn bij uitstek in staat om beveiligingsincidenten te veroorzaken. Het is niet de eerste keer dat een externe medewerker zich toegang verschaft tot vertrouwelijke bedrijfsinformatie. De hieronder staande figuur ontleend aan de Gartner Group onderstreept deze uitspraak.



Figuur 1.1 *Risico's beveiligingsincident versus kennisniveau pleger.*

In de twee navolgende hoofdstukken wordt stilgestaan bij de organisatorische en technische kant van informatiebeveiliging. "Hoe komt de vorming van beveiligingsbeleid tot stand?" en "Biedt een firewall afdoende bescherming tegen ongewenst dataverkeer vanaf het Internet?" zijn zomaar wat vragen die in deze white paper beantwoord worden. In de beiden hoofdstukken passeert een aantal onderwerpen de revue, zonder dat hierbij diep wordt ingegaan op de feitelijke materie. Een aantal onderwerpen, bijvoorbeeld *intrusion detection* of het uitvoeren van een risicoanalyse biedt namelijk genoeg stof voor een apart white paper.

2 ORGANISATIE

2.1 Inleiding

Informatiebeveiliging kent zowel een organisatorische als een technische invalshoek. Alvorens men bepaalde maatregelen kan gaan implementeren, moet men informatiebeveiliging goed en doordacht organiseren. “Waarom wil ik beveiliging in gaan voeren?” of “Wat wil ik nu precies beveiligen?” zijn vragen die beantwoord moeten worden. In dit hoofdstuk wordt ingegaan op een aantal organisatorische aspecten van informatiebeveiliging.

2.2 Definitie en doelstelling

Wat is nu precies informatiebeveiliging, en wat wil men ermee bereiken?
Een gangbare definitie luidt:

Informatiebeveiliging betreft alle maatregelen die gericht zijn op het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van gegevens.

In plaats van “informatie” wordt hier gesproken over “gegevens”. Dit komt omdat de term “informatie” generiek van aard is, en op diverse manieren geïnterpreteerd kan worden. De term “gegevens” is meer gerichter. Gegevens vormen de drager van “informatie”.

De doelstelling van informatiebeveiliging is tweeledig:

1. Waarborging van de continuïteit van de interne bedrijfsvoering en primaire processen binnen organisaties.
2. Minimalisatie van de schade en de eventuele gevolgen voor organisaties als gevolg van beveiligingsincidenten.

In de definitie wordt tevens gesproken over beschikbaarheid, integriteit en vertrouwelijkheid. Dit zijn de zogenaamde betrouwbaarheidseisen van gegevens.

2.3 Betrouwbaarheidseisen

De betrouwbaarheidseisen geven een verfijning van de doelstelling van informatiebeveiliging, namelijk een zo hoog mogelijke beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en bijbehorende ICT.

2.3.1 BESCHIKBAARHEID

De garantie dat gegevens en essentiële diensten op het juiste moment en in de juiste vorm beschikbaar zijn. Dit wordt ook wel continuïteit genoemd.

2.3.2 INTEGRITEIT

De garantie dat gegevens correct, juist en volledig is. Dit wordt ook wel exclusiviteit genoemd.

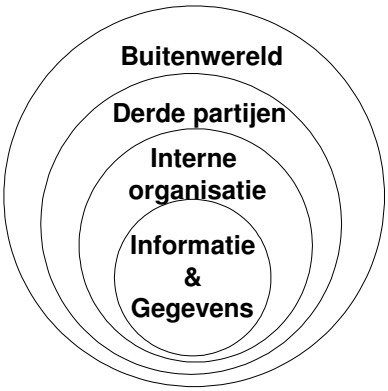
2.3.3 VERTROUWELIJKHEID

De garantie dat gegevens niet door onbevoegde is in te zien. Dit wordt ook wel exclusiviteit genoemd.

2.4 Bedreigingen

Binnen organisaties wordt de continuïteit van de primaire bedrijfsprocessen continue bedreigd door invloeden van zowel binnen als van buiten de organisatie. Bedreigingen zijn er in soorten en maten. Voorbeelden hiervan zijn technische storingen, fouten veroorzaakt door menselijk handelen, social engineering, maar ook computervirussen en allerhande technische trukendozen zoals IP Source routing attacks, TCP SYN floods en bijvoorbeeld Ping of Death.

Om de bedreigingen goed in kaart te kunnen brengen is het noodzakelijk dat men voor zichzelf een beschouwingsgebied formuleert. In dit beschouwingsgebied wordt onderscheidt gemaakt tussen gegevens, systemen, omgevingen en gebruikers. Door de structurele opzet helpt het organisaties de bedreigingen in kaart te brengen. Een mogelijke indeling voor een beschouwingsgebied is in onderstaand figuur weergegeven.



Figuur 2.1 *Beschouwingsgebied informatiebeveiliging.*

In dit voorbeeld is omwille van duidelijkheid een aantal schillen weggelaten. Men kan bijvoorbeeld inzoomen op de schil “Interne organisatie”, en deze vervolgens verder te verbijzonderen tot bijvoorbeeld aparte schillen voor informatiesystemen en netwerken.

2.5 Risico

Het risico of de kans dat zich een bepaalde bedreiging daadwerkelijk voordoet dient men vooraf vast te stellen. Dit is niet altijd even eenvoudig. Het simpele feit dat een geringe directe bedrijfsschade veel grotere gevolgschade kan hebben voor bijvoorbeeld het imago van een organisatie is niet ondenkbaar. Een inbraak op een computernetwerk van een energiebedrijf zonder dat gegevens zijn meegenomen kan in de media breed worden uitgemeten in de trend van “Bedrijfsnetwerk energieleverancier onveilig: hoe zit het met uw stroomvoorziening?”.

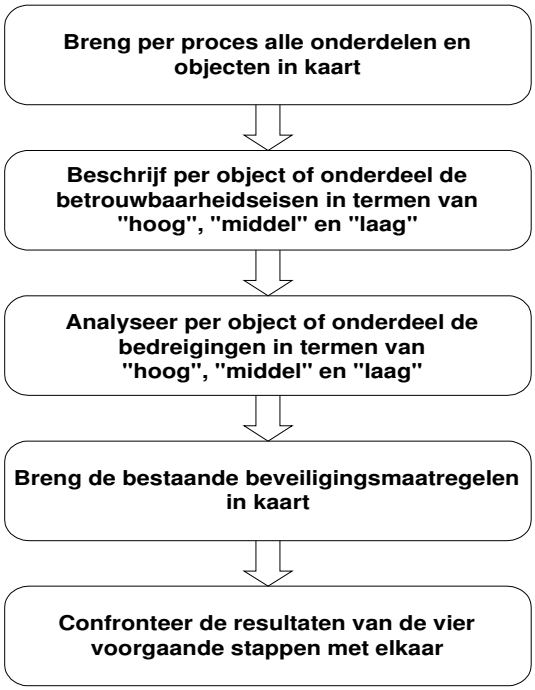
Het in kaart brengen van risico's kan op een aantal manieren. Men kan ofwel een risicoanalyse ofwel een afhankelijkheids - en kwetsbaarheidsanalyse uitvoeren. De hiermee vergaarde informatie is noodzakelijk voor het opstellen van maatregelen. Aan de hand van het beschouwingsgebied kan men vaststellen of deze analyse op macro - dan wel op microniveau moet worden uitgevoerd. Op macroniveau wordt risicobeleid geformuleerd, terwijl op microniveau op basis van dit geformuleerde risicobeleid de uiteindelijke analyse plaatsvindt.

2.5.1 RISICOANALYSE

Een risico analyse maakt het mogelijk vooraf een inschatting te maken van de eventuele gevolgen die een bepaalde bedreiging zou veroorzaken. Men berekent wat de (gevolg)schade in financiële zin is bij een bepaalde bedreiging. De risicoanalyse kent twee varianten, namelijk de kwantitatieve en de kwalitatieve. Bij de kwantitatieve variant wordt een aantal risico's onderzocht in termen van hoeveelheden bijvoorbeeld "duur uitval". De kwalitatieve variant onderzoekt de kans dat een bepaald risico zal optreden in termen van de classificatie "hoog", "middel" en "laag".

2.5.2 AFHANKELIJKHEIDS- EN KWETSBAARHEIDSANALYSE

Bij een Afhankelijkheids- en kwetsbaarheidsanalyse (ook wel afgekort tot A&K-analyse) brengt men eerst de processen is kaart die voor het functioneren van een organisatie, dus waar en organisatie van afhankelijk is, van belang zijn. Van deze processen worden de betrouwbaarheidseisen uitgewerkt. Vervolgens wordt per proces de kwetsbaarheid in kaart gebracht. Dit gebeurt stapsgewijs. Onderstaand figuur illustreert deze werkwijze.



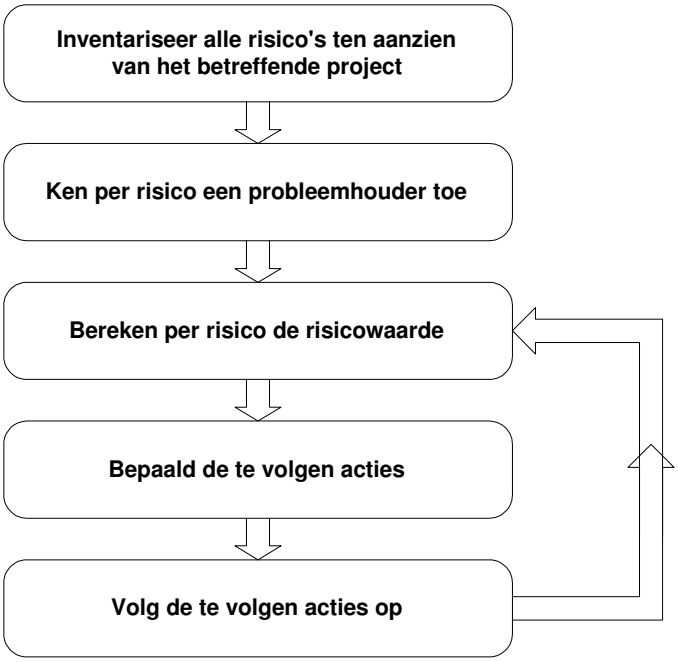
Figuur 2.2 *Stappen van een Kwetsbaarheidsanalyse.*

2.6 Risicomanagement

Als het gaat om informatiebeveiliging loopt elke organisatie bepaalde risico's. Het manifest worden van deze risico's heeft bepaalde gevolgen, en wordt normaliter op de juiste wijze ingeschat en afgewogen. Binnen grote organisaties is het managen van deze risico's, of anders gezegd de risicobeheersing, een aparte taak. De mate waarin deze taak is ingevuld is afhankelijk van een aantal factoren, bijvoorbeeld de mate waarbij men zich kan verzekeren tegen bepaalde risico's. Risicomanagement kent diverse methodieken, bijvoorbeeld de zogenaamde "projectaanpak".

2.6.1 Projectaanpak: Bepalen risicowaarde

Een andere vorm van risicomanagement is de zogenaamde "projectaanpak". Deze aanpak is gestoeld op het bepalen van de risicowaarde. Het vaststellen van deze risicowaarde komt steeds terug. De risico's die gedurende de loop van een bepaald project worden onderkend moeten worden gemanaged. Onderstaand figuur illustreert de te ondernemen stappen bij deze vorm van risicomanagement.



Figuur 2.3 *Stappen risicomanagement op basis van "projectaanpak".*

Deze sessie moet een vast onderdeel worden op de agenda van het projectgroep overleg. Periodiek moeten de risico's opnieuw in kaart worden gebracht.

RISICOWAARDE

De mate van inspanning die in de beheersing van de risico's moet worden gestoken is sterk afhankelijk van de risicowaarde. De risicowaarde wordt bepaald door drie factoren, namelijk “kans”, “impact” en “uncontrollability”. In onderstaande tabel worden deze factoren uitgewerkt.

Factor	Omschrijving
Kans	De waarschijnlijkheid dat de gebeurtenis zich voor zal doen
Impact	De ernst van de gevolgen indien de gebeurtenis zich voordoet
Uncontrollability	De mate waarin het voorkomen van de gebeurtenis en of het reduceren van de kans op het manifest worden van de gebeurtenis onbeïnvloedbaar is

Tabel 2.1 *Factoren risicowaarde.*

Van deze drie factoren wordt bepaald wat de waarde is. Er zijn drie mogelijkheden namelijk:

1. "Hoog" (waarde = 5)
2. "Medium" (waarde = 3)
3. "Laag" (waarde = 1)

Door deze waarden met hun wegingsfactoren te vermenigvuldigen en vervolgens de uitkomsten daarvan te sommeren wordt de risicowaarde berekend. De wegingsfactoren zijn:

1. "Kans"(waarde = 1)
2. "Impact"(waarde = 4)
3. "Uncontrollability"(waarde = 2)

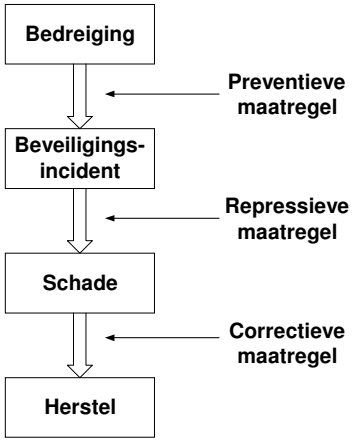
Op basis van de bovengenoemde gegevens ontstaat de volgende formule:

Risicowaarde = (kans x 1)+ (impact x 4) + (uncontrollability x 2)

De maximale risicowaarde komt hiermee op 35, en de minimale risicowaarde op 7. Risico's met een waarde die hoger is dan 20 hebben een hoge prioriteit en vragen onmiddellijke actie en of aandacht.

2.7 Maatregelen

Maatregelen vormen het antwoord op bedreigingen. Maatregelen kunnen zowel organisatorisch als technisch van aard zijn. In sommige gevallen is een combinatie mogelijk. Naast de bovengenoemde tweedeling vallen maatregelen uiteen in preventieve maatregelen, repressieve maatregelen en correctieve maatregelen.



Figuur 2.4 *Soorten maatregelen.*

2.7.1 PREVENTIEVE MAATREGEL

Een preventieve maatregel is bedoeld om het gevolg van een bedreiging te voorkomen. Een voorbeeld hiervan is antivirussoftware. De virusscanner controleert op virussen, bij detectie van een virus kan de software het virus elimineren.

2.7.2 REPRESSIEVE MAATREGEL

Een repressieve maatregel is bedoeld om de gevolgen van een beveiligingsincident te beperken. Een voorbeeld hiervan is een brandblusinstallatie.

2.7.3 CORRECTIEVE MAATREGEL

Een repressieve maatregel is bedoeld om de gevolgen van een beveiligingsincident te minimaliseren. Een voorbeeld hiervan is een backup systeem. Ingeval van een calamiteit waarbij gegevens verloren zijn gegaan kan men met een backup gegevens terugzetten.

2.8 Beleid en positionering

Informatiebeveiliging is gebaseerd op beleid. Het beveiligingsbeleid is afgeleid van het een drietal beleidsgebieden, namelijk informatiebeleid, automatiseringsbeleid en algemeen beleid. Beveiliging is onlosmakelijk verbonden met de informatiesystemen zelf. Aangezien de informatiesystemen de verantwoordelijkheid zijn van het management, betekent dit dat de beveiliging van deze systemen eveneens tot deze verantwoordelijkheid behoord. Binnen organisaties speelt informatiebeveiliging op diverse niveaus een rol. Op het strategisch niveau wordt beveiligingsbeleid geformuleerd. Beleid is per definitie richtingbepalend en sturend, echter op tactisch en operationeel niveau heeft men behoefte aan een hanteerbare vorm van dit beleid, het beveiligingsplan. Op tactisch niveau wordt dit beveiligingsplan uitgewerkt in de vorm van procedures en maatregelen, ook wel baseline of code genoemd.

Op operationeel niveau heeft men behoefte aan concreet uitgewerkte onderdelen. Een voorbeeld is een handleiding met instellingen of een guideline voor de inrichting van een firewall, of de inzet van routers om interne netwerken van elkaar te scheiden (bijvoorbeeld het productienetwerk van het financiële netwerk).

2.9 Menselijke factor

Beveiligingsbeleid en de uitwerking daarvan valt of staat met de vaststelling dat de menselijke factor in alle facetten rondom informatiebeveiliging centraal moet staan. Doet men dit niet, dan zijn alle initiatieven per definitie gedoemd te mislukken.

De mens, of beter gezegd de gebruiker van gegevens, moet in een vroegtijdig stadium betrokken worden bij informatiebeveiliging. Men kan zich voor stellen dat alleen zo een beveiligingsbewustzijn kan worden aangekweekt. Overigens wordt met gebruiker van gegevens zowel de eigenaar, de beheerder als diegene die gegevens bewerkt en veredeld bedoeld. Uiteindelijk zal in maatregelen, procedures en werkrichtlijnen verschil optreden tussen deze groepen.

2.10 Inbedding in organisaties

Informatiebeveiliging als tak van sport is veelal belegd bij een aparte functionaris, de security officer. Afhankelijk van het soort organisatie en de grootte daarvan kan tevens een aparte afdeling worden ingericht. Belangrijk aandachtspunt is dat informatiebeveiliging op het juiste niveau binnen organisaties voldoende aandacht krijgt. Dit betekent dat minimaal op het niveau van het MT een medewerker met verstand van beveiligingszaken mee moet praten.

2.11 Beveiligingsbewustwording en - bewustzijn

Het is al eerder aangehaald, informatiebeveiliging kan alleen slagen met medewerking van de interne medewerkers van organisaties. Informatiebeveiliging moet bekend zijn bij alle managers en medewerkers van organisaties. Het beveiligingsbeleid moet op brede steun kunnen rekenen van het management. Zonder commitment van het management en de medewerkers heeft informatiebeveiliging weinig zin, het werkt eerder problemen in de hand.

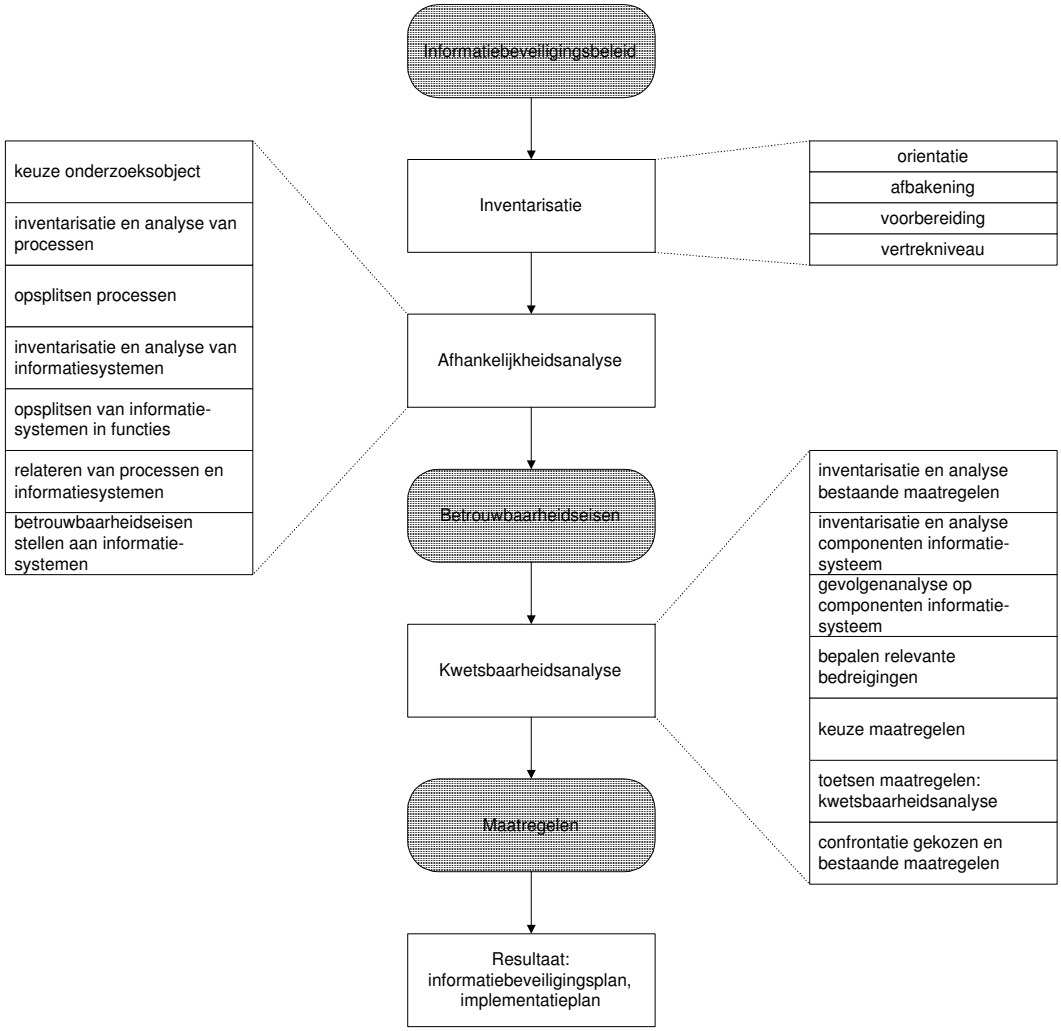
Een ander probleem vormt kennis. Men kan zich simpelweg niet bewust zijn dat bepaalde handelingen wat beveiliging betreft het noodlot tarten. Dit betekent dat alle medewerkers een instructie moeten krijgen over informatiebeveiliging. De geldende normen op dit vlak moet voor niemand onbekend zijn.

Door bewustwordingsprogramma's kunnen organisaties managers en medewerkers een handvat bieden om op een goede wijze met beveiliging om te leren gaan. In een dergelijk programma zou het niet misstaan een voorbeeld te stellen door een intern voorval. Uiteindelijk zal door bewustwording bewustzijn ontstaan. Het is van eminent belang dat dergelijke programma's frequent plaatsvinden. Het is namelijk een bekend fenomeen dat bepaalde gewoonten erg moeilijk zijn af te leren, waardoor bewustzijn snel omslaat in deze oude gewoonten. Er ontstaat een golfbeweging waardoor toekomstige initiatieven snel terzijde worden geschoven. Wij noemen dit ook wel het "haaientand principe".

2.12 Standaarden

Het organiseren van beveiliging is geen geringe opgave. Er is een aantal standaarden en richtlijnen opgesteld om organisaties in dergelijke trajecten terzijde te staan.

Een daarvan is de Code voor Informatiebeveiliging, afgeleid van de British Standard 7799 of kortweg BS7799. Met behulp van dit document kan een organisatie haar informatiebeveiliging stapsgewijs vormgeven. Tevens biedt het de mogelijkheid om een doorsnede van alle maatregelen uit dit document in te voeren. Deze zogenaamde "keycontrols" zijn de meest essentiële informatiebeveiligingsmaatregelen die elke organisatie zou moeten treffen. De Code is overigens recent aan een revisie onderworpen. Een ander "standaard" werk is het zogenaamde Orange Book 1995 van het Amerikaanse Ministerie van Defensie.
Binnen overheidsorganisatie wordt vaak gebruikt gemaakt van het in 1994 uitgegeven Voorschrift Informatiebeveiliging Rijksdiensten, kortweg VIR. Onderstaand figuur is ontleend aan het VIR, en geeft schematisch de werkwijze van deze methodiek weer.



Figuur 2.5 *Voorschrift Informatiebeveiliging Rijksdiensten.*

3 TECHNIEK

3.1 Inleiding

Vanuit het vormgegeven informatiebeveiligingsbeleid kan men maatregelen destilleren. Een aantal van deze maatregelen kunnen zijn gestoeld om techniek, bijvoorbeeld een firewall. Dit hoofdstuk beschrijft een aantal technische maatregelen. De het niet de bedoeling om in dit hoofdstuk een volledig overzicht te geven van alle technische mogelijkheden.

3.2 Beveiligingsarchitectuur

Net zoals bij de organisatie van informatiebeveiliging zou de technische invulling gebaseerd moeten zijn op een groter geheel. Het implementeren van losstaande oplossingen kan voor een enkel probleem goed werken, veelal is de invloed op andere reeds geïmplementeerde oplossingen negatief. Door nu en de organisatie en de techniek onderdeel te laten uitmaken van een al eerdere genoemd groter geheel ontstaat een "beveiligingsarchitectuur". Dit is een samenhangend geheel van maatregelen en technische invullingen op gebied van informatiebeveiliging.

3.3 Componenten

Een beveiligingsarchitectuur kent verschillende verschijningsvormen, en is sterk afhankelijk van het type organisatie en de mate van beveiliging. Het gevolg hiervan is dat het onmogelijk is een compleet overzicht te geven van beschikbare componenten. Een aantal veelvoorkomende componenten wordt hieronder weergegeven.

3.3.1 INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems, ook wel afgekort tot IDS, is een combinatie van hard- en software die het netwerk of informatiesystemen kunnen monitoren. De "ogen en oren" van het netwerk of informatiesysteem is misschien een betere benaming.

Er zijn verschillende IDS varianten:

1. host based systemen: hierbij wordt informatie van een los systeem gebruikt om inbreuken te detecteren
2. multihost based systemen: hierbij wordt informatie van verschillende systemen gebruikt om inbreuken te detecteren
3. network based systemen: hierbij wordt informatie over het netwerkverkeer in combinatie met een van de hierboven genoemde systemen gebruikt om inbreuken op het netwerk te detecteren

IDS kan realtime werken, dit betekent dat op basis van gedetecteerde inbreuken direct actie kan worden ondernomen. IDS werkt op basis van het vergelijken van vooraf geprogrammeerde patronen. Bij een verschil wordt een alarm gegenereerd.

Elke niet vooraf ingestelde handeling wordt vastgelegd. Het is zelfs mogelijk bepaalde handelingen op het interne netwerk te blokkeren.

3.3.2 Firewall

Een firewall is een combinatie van hard- en software waarmee een scheiding kan worden gemaakt tussen het interne, vertouwde netwerk, en het externe, niet-vertrouwde netwerk. De basisfunctie van een firewall is het controleren van datastromen op basis van regels, ook wel policies genoemd. Het controleren van datastromen kan op diverse niveaus binnen het OSI model plaatsvinden. Op protocolniveau kan bijvoorbeeld gelden dat alleen HTTP mag worden doorgelaten, terwijl FTP en Telnet moeten worden tegengehouden. Voor HTTP kan vervolgens worden vastgesteld dat alleen bepaalde systemen door interne medewerkers kunnen worden geraadpleegd.

Een firewall kent een aantal verschijningsvormen. De bekendste zijn:

1. De packetfiltering firewall
2. De proxy firewall
3. De statefull inspection firewall

3.3.3 In - en uitbelvoorziening

Een in - uitbelvoorziening vormt een potentieel gat in de beveiliging van bedrijfsnetwerken. Dit komt omdat het een concentratie van analoge (bijvoorbeeld standaard telefoonlijnen) en digitale (bijvoorbeeld ISDN) koppelvlakken biedt. Als de bij deze koppelvlakken corresponderende telefoonnummers bekend zijn, dan is het kinderspel om via deze koppelvlakken het netwerk te benaderen.

Beveiliging kan plaatsvinden op een aantal manieren, waarvan de bekendste zijn het werken met call back en het toepassen van een access list. Een extra beveiligingsniveau kan men creëren door toepassing het identificeren van de in- of uitbellende gebruiker met behulp van een token oplossing.

3.3.4 Routers

Routers vormen het hart van elk computernetwerk. Een router bevat een schat aan informatie over de topologie en typologie van een computernetwerk. Routers zijn vaak uitgerust met een extra analoog modem voor management.

3.4 Identiteit

Het nagaan of een persoon daadwerkelijk diegene is voor wie zij of hij zich uitgeeft is een van belangrijkste aandachtspunten binnen de maatregelensfeer van informatiebeveiliging. De identiteit van een gebruiker van elektronische diensten kan men veelal herleiden door het gebruik van wachtwoorden, pincodes of het bezit van iets tastbaars, bijvoorbeeld een token of smartcard. In toenemende mate is de combinatie van “iets weten”, bijvoorbeeld een wachtwoord, en het “bezit van iets”, bijvoorbeeld een token, onvoldoende. Een uitbreiding met een extra beveiligingsniveau is dan ook wenselijk. Biometrie, of identiteitsvaststelling op basis van menselijke kenmerken zoals iris of handpalm geometrie, voorziet in een dergelijke uitbreiding.

3.4.1 Authenticatiesystemen

Het vaststellen van de identiteit van een gebruiker op basis van “iets bezitten” wordt veelal geregeld met behulp van authenticatiesystemen. Een veeltoegepaste vorm is gebaseerd op de zogenaamde tokens. Deze tokens kunnen werken op basis van het challenge & response

principe. Andere vormen zijn time-based, password-based of address-based. Het gebruik van authenticatiesystemen vergt investering in administratie en beheer.
Bekende protocollen op dit vlak zijn RADIUS en TACACS.

3.4.2 BIOMETRIE SYSTEMEN

Het uitgangspunt van biometrie systemen zijn menselijke kenmerken. Door deze kenmerken op enige wijze op te slaan, en geschikt te maken voor hergebruik, kan men een controlemechanisme ontwikkelen op basis waarvan de identiteit van een persoon kan worden vastgesteld. Biometrie is een verzamelnaam voor een aantal toepassingen, en kent diverse verschijningsvormen. Een gangbare beschrijving:

Biometrie is een techniek waarbij identificatie van personen is gebaseerd op een uniek kenmerk van de mens, bijvoorbeeld een vingerafdruk, een deel van de iris of een bepaald gedrag. Door dit kenmerk in elektronische vorm op te slaan, kan men het vergelijken met een op een ander tijdstip vergaarde versie.

BIOMETRIE VORMEN

Om biometrie te kunnen toepassen is een aantal systemen beschikbaar. Grofweg kan men deze systemen opdelen in twee groepen. Allereerst zijn er systemen die betrekking hebben op fysiologische eigenschappen van de mens. Fysiologische systemen zijn ontwikkeld rondom een menselijk kenmerk, bijvoorbeeld een vingerafdruk, de kenmerken van het netvlies en iris, de vorm van een gezicht, stemherkenning, de vorm van de handpalm en ooggeometrie.
De tweede groep systemen is gebaseerd op het gedrag van de mens. Voorbeelden hiervan zijn systemen die werken met handschrift herkenning. In dit laatste geval speelt het tikken met vingers op een harde ondergrond en de wijze waarop een persoon zijn of haar handtekening plaatst een rol van betekenis.

Nieuwe ideeën ontstaan door met akoestische kenmerken biometrie systemen te gaan ontwikkelen. Dit is geen sciencefiction; een aantal systemen ontstijgt het R&D niveau.

FAR VERSUS FRR

Biometrie is gebaseerd op rekenregels of algoritmen die worden gebruikt om twee zogenaamde “templates” met elkaar te vergelijken. Een template is bijvoorbeeld een elektronisch opgeslagen vingerafdruk zijn. Door twee templates met elkaar te vergelijken kan de identiteit van iemand worden vastgesteld. Afwijkingen worden aangeduid met FAR (False Acceptance Rate) en FRR (False Rejection Rate). FAR betreft fouten waarbij een biometrie systeem mensen geaccepteerd terwijl dit niet zou mogen. In het geval van FRR worden mensen onterecht geweigerd, terwijl het biometrie systeem deze mensen juist moet accepteren. Elk biometrie systeem heeft en FAR en een FRR. Beiden zijn aan elkaar gerelateerd. Afhankelijk van het type toepassing worden FAR en FRR aangepast.

3.5 Mobile content

Mobile content is een verzamelnaam voor kleine programma’s die worden gebruikt om Web pagina’s te verfraaien. Door het gebruik van HTTP wordt, zonder dat men er weet van heeft, een aantal vormen van mobile content binnengehaald. Voorbeelden zijn Active-X code, Java applets en cookies. Deze code is een bron van zorg, omdat hiermee allerlei problemen kunnen worden binnengehaald zoals bijvoorbeeld computervirussen.

Het is mogelijk deze code te controleren alvorens de betreffende Web pagina wordt binnengehaald door een gebruiker. Een 100% waterdichte controle is echter niet mogelijk.

3.6 PKI, Encryptie, TTP, CA en certificaten

Indien bepaalde informatie dusdanig vertrouwelijk is, en men wil niet dat deze informatie leesbaar is voor onbevoegden, dan kan men besluiten om encryptie of versleuteling van informatie te gaan toepassen. Het voordeel is dat informatie alleen zichtbaar of beter gezegd leesbaar is voor bevoegde personen. Het nadeel is dat het geld kost in de vorm van techniek en beheer. Encryptie is op velerlei wijze beschikbaar, hetzij in de vorm van hardware hetzij in de vorm van software of een combinatie daarvan. Met encryptie technieken is het mogelijk via publieke netwerken zogenaamde “encrypted tunnels” op te zetten. Zo kan bijvoorbeeld via het Internet een veilige verbinding opzetten tussen twee financiële centra van een bank.

Encryptie technieken zijn gebaseerd op het gebruik van zogenaamde sleutels, algoritmen (bijvoorbeeld DES of RSA) die ervoor zorgen dat klare tekst veranderd in onleesbare tekst. Dit kunnen zowel publieke sleutels als privé sleutels zijn. Het gebruik van deze sleutels vereist administratie. Door sleutels te voorzien van een certificaat kan worden aangegeven of het gebruik ervan veilig is of niet. Het certificeren van sleutels wordt door een zogenaamde Certification Authority (CA) gedaan. Een voorbeeld van een CA is het Amerikaanse Verisign,.

Het voeren van administraties voor certificaten kan worden uitgevoerd door zogenaamde Trusted Third Parties, of TTP’s, zeg maar een notaris op gebied van ICT producten en diensten. In Nederland zijn onder andere PTT Post, Roccade en KPMG momenteel actief als leverancier van TTP producten en - diensten.

Een infrastructuur waarmee bovenstaande materie als complete dienst kan worden geleverd noemt men ook wel een Public Key Infrastructure of PKI.

3.7 Protocollen

Op het gebied van beveiliging is een aantal protocollen beschikbaar. Enkele voorbeelden van (netwerk)protocollen zijn IPSEC, SSL, S-HTTP (een “veilige” extensie van het bekende HTTP), S/MIME, PGP/MIME en SET.

SET is wat dat aangaat een mooi voorbeeld van samenwerking tussen diverse organisaties (zoals banken en creditcard maatschappijen) om te komen tot een veilige standaard voor gegevens uitwisseling via netwerken (bijvoorbeeld Internet).

4 AANBEVELINGEN

1. Geef informatiebeveiliging voldoende aandacht binnen uw organisaties. Maak dit onderwerp bespreekbaar op het hoogste niveau binnen uw organisatie.

2. Voer minimaal de 10 zogenaamde “keycontrols” van de Code voor Informatiebeveiliging door. Als men binnen uw organisatie niet of nauwelijks aan informatiebeveiliging wordt gedaan dan zijn deze 10 aandachtspunten het minste wat men zou moeten invoeren als het gaat om informatiebeveiliging. Enkele voorbeelden van “keycontrols” zijn:
   a.) opstellen van een beleidsdocument aangaande informatiebeveiliging
   b.) rapporteren van beveiligingsincidenten en controle op computervirussen
   c.) naleven van de wetgeving ten aanzien van de bescherming van persoonsgegevens

3. Stel een helder en duidelijk informatiebeveiligingsbeleid op. Maak van dit beleid een steeds terugkerend onderdeel op uw agenda van MT vergaderingen.

4. Formuleer duidelijke regels voor eindgebruikers ten aanzien van het gebruik van informatiebeveiliging. Het invoeren van een gecentraliseerd Internet koppelpunt heeft alleen nut indien de interne medewerkers er gebruik van maken, en niet met andere oplossingen (lees modems) gaan werken.

5. Zorg dat uw medewerkers zich bewustzijn van het nut van informatiebeveiliging. Elke beveiligingsmaatregel valt of staat met de betrokkenheid en het bewustzijn van uw interne medewerkers. Stel daarom de mens in uw organisatie centraal als het gaat om beveiliging. Voer tevens een bewustwordingsprogramma ten aanzien van informatiebeveiliging door.

6. Ontwikkel een sanctiebeleid. Binnen enkele organisaties staat het betrappen van een medewerker met een modem gelijk met ontslag op staande voet.

7. Voorkom de denkwijze “de voordeur zit op slot, dus ik ben veilig”. Het toepassen van bijvoorbeeld een firewall betekent niet dat uw netwerk veilig is. Het netwerk zelf moet worden gecontroleerd, de naleving op het gebruik van gecentreerde externe koppelingen moet plaatsvinden, het gebruik van modems moet aan banden worden gelegd. Dit zijn slechts enkele voorbeelden.

8. Ontwikkel een beveiligingsarchitectuur waarin u alle voor u belangrijk zijnde oplossingen in integreert.

9. Controleer dagelijks de werking van uw operationele informatiebeveiliging. Een voorbeeld hiervan zijn het controleren van de logfiles, deze worden niet voor niets aangemaakt.

10. Weeg kosten af tegen baten en de mate waarin uw primaire bedrijfsvoering gevaar loopt als het gaat om investeringen in beveiligingshulpmiddelen. Al is potentiële gevaar in de ogen van externe partijen nog zo groot, u zelf (eventueel met hulp) kunt het best inschatten wat de mogelijke gevolgen zijn van bepaalde beveiligingsincidenten.

5 LITERATUURLIJST

- NIVRA geschrift 53, Automatisering en controle, deel V Organisatorische maatregelen en controletechnieken voor de ontwikkeling van geautomatiseerde informatiesystemen
- NIVRA geschrift 43, Automatisering en controle, deel VII, Kwaliteitsoordelen over informatievoorziening
- Beveiligingsbeleid en beveiligingsplan, publicatie van het NGI , 1e druk, 2e oplage 1993
- Beveiligingsbewustzijn bij gegevensbescherming, publicatie van het NGI 1995
- Risico-analyse en risicomanagement, publicatie van het NGI 1992
- Bevordering van betrouwbaarheid van Informatiesystemen
- KPMG: 24 auteurs over EDP-auditing
- Network Security, Ch. Kaufman, 1995
- Firewalls and Internet Security, W.R. Cheswick & S.M. Bellovin., November 1997
- EDP-Auditing: automatisering onder controle
- Code voor Informatiebeveiliging; publicatie van NNI, versie 1, November 1994 (vertaling van de Engelse BS7799)
- Diverse publicaties en handboeken van Gemeenten en instanties
- Diverse OTB studies
- Publicaties uit Informatie en Automatiserings Gids
- Voorschrift Informatiebeveiliging Rijksdiensten, 1994
- Websites van diverse leveranciers van beveiligingsproducten

