Beveiliging van persoonsgegevens

1. Algemeenheden, definities, begrippen

1.1. Beveiliging van informatiesystemen

Vandaag kan geen enkel overheids- of privébedrijf zijn doel bereiken zonder in stijgende mate informatie te verzamelen en te verwerken.

Het **informatiesysteem** van een onderneming omvat alle technologieën waarvan een onderneming gebruik maakt, waaronder systemen voor applicaties en ondersteuning om gewild en op een gekozen ogenblik de nodige informatie verwerken, te verzamelen, op te slaan, te verzenden en aan te bieden aan diegene die er recht op heeft, en ten slotte ook om op het gepaste tijdstip die informatie te vernietigen.

Informatie is van kapitaal belang en is zoals alle andere belangrijke activa noodzakelijk voor de activiteiten van iedere organisatie. Daarom moet zij ook op een gepaste manier worden beschermd.

In welke vorm zij ook bestaat of met welke middelen zij ook werd verstrekt of bewaard, informatie moet altijd voldoende beschermd worden.

In normatieve context wordt informatiebeveiliging als volgt omschreven[1]: alle aspecten die betrekking hebben op vertrouwelijkheid (verkrijgen en bewaren van informatie), integriteit, beschikbaarheid, toerekenbaarheid, authenticiteit, betrouwbaarheid en onweerlegbaarheid van de informatie en op de installaties voor informatieverwerking.

Deze verschillende aspecten (hierna beschreven) worden dikwijls beveiligingsattributen of beveiligingskenmerken genoemd. Zij verwijzen naar de toestand van de betrokken entiteit, of het nu gaat over informatie, processen, systemen of personen. De beveiliging geeft dus de staat van bescherming weer, die het resultaat is van alle getroffen maatregelen en ingezette middelen om de beveiligingskenmerken van de entiteiten tegen mogelijke risico's te vrijwaren.

Met die definitie wordt informatiebeveiliging een van de primordiale eigenschappen van de intrinsieke kwaliteit van die informatie.

[1] ISO/IEC 13335-1:2004 – *Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for information and communications technology management*

1.2. De verschillende attributen van informatiebeveiliging

Vertrouwelijkheid is een informatie-eigenschap waardoor alleen gemachtigde personen, entiteiten of processen toegang hebben tot informatie en waardoor informatie alleen kan worden doorgegeven aan gemachtigde personen, entiteiten of processen.

De mogelijkheid om informatie selectief toegankelijk te maken, moet gegarandeerd worden zolang de informatie bestaat, d.w.z. gedurende de verzameling, bewaring, verwerking en mededeling ervan.

In de praktijk krijgen alleen personen die een functie of professionele activiteit uitoefenen die toegang tot persoonsgegevens rechtvaardigt hiervoor een machtiging.

Integriteit dekt twee verschillende aspecten: integriteit van de informatie en integriteit van systemen en processen.

De integriteit van informatie is de eigenschap waardoor die informatie niet opzettelijk of onopzettelijk kan worden veranderd of vernietigd.

De integriteit van een systeem of proces is de eigenschap om de gewenste functie volledig en volgens de verwachtingen te verwezenlijken, waarbij het zonder een gemachtigde tussenkomst niet mogelijk is opzettelijke of onopzettelijke veranderingen aan te brengen.

Beschikbaarheid: dankzij deze eigenschap zijn informatie, systemen en processen toegankelijk en bruikbaar op verzoek van een gemachtigde entiteit.

Toerekenbaarheid is de eigenschap waarmee de handelingen van een entiteit opspoorbaar zijn en enkel aan die entiteit toegeschreven kunnen worden.

Toerekenbaarheid garandeert dat alle bewerkingen die personen, systemen of processen uitvoeren, geïdentificeerd kunnen worden (identificatie) en dat het spoor naar de auteur en de bewerking worden bewaard (opspoorbaarheid).

Onweerlegbaarheid betekent dat een bewerking of gebeurtenis daadwerkelijk plaatsvond en niet nu noch later ontkend kan worden. Bij e-mailverkeer bijvoorbeeld, wordt onweerlegbaarheid gebruikt om zowel te garanderen dat de ontvanger niet kan ontkennen dat hij het bericht heeft ontvangen als om te garanderen dat de afzender niet kan ontkennen dat hij het bericht verstuurde.

Onder **authenticiteit** wordt verstaan dat een entiteit diegene is die ze beweert te zijn.

Authenticiteit wordt toegepast op personen (gebruikers) maar ook op elke andere entiteit (applicatie, processen, systeem, enz.). Het is een identificatie, d.w.z. een herkenning van een benaming waardoor een entiteit zonder enige twijfel kan worden aangewezen.

Betrouwbaarheid is de eigenschap waardoor het verwachte resultaat wordt verstrekt.

1.3. Het belang van informatiebeveiliging

Omdat ondernemingen meer en meer afhankelijk zijn van hun informatiesysteem, is de informatie zelf voor hen van doorslaggevend belang. Dit betreft niet alleen alle informatie die de onderneming in het kader van haar activiteiten verwerkt, maar ook alle andere informatie die voor de onderneming noodzakelijk is om haar activiteiten op een gepaste manier en in alle omstandigheden verder te kunnen uitoefenen.

Tot voor kort betrof de beveiliging van informatiesystemen vooral gesloten informaticanetwerken, die werden ontworpen rond op zichzelf staande systemen met een beperkte capaciteit. Die systemen konden gemakkelijk beveiligd worden met slechts enkele maatregelen voor de fysieke en logische beveiliging, en informatiebeveiliging. Maar door de snelle verspreiding van de pc, internettoegang voor het grote publiek en de snelle verspreiding van nieuwe informatie- en communicatietechnologieën, is het profiel van de menselijke activiteiten vandaag grondig veranderd. Bovendien zijn de informatie en de verschillende betrokken processen kwetsbaarder dan ooit omdat alle netwerken met elkaar verbonden zijn, omdat informatie steeds toegankelijker wordt en de systemen steeds complexer. Om commerciële activiteiten met succes te kunnen realiseren of om de burger een goede dienstverlening te garanderen, zijn gepaste beheersmaatregelen onontbeerlijk om tegen voortdurend wijzigende gevaren gewapend te zijn.

Beveiliging van informatiesystemen moet vandaag dus meer zijn dan een verzameling noodoplossende maatregelen om technische gebreken te verhelpen, nl. een gedragscode die alle betrokken partijen naleven om te beantwoorden wat essentieel en fundamenteel-menselijk is.

1.4. De beveiliging van persoonsgegevens

Het begrip persoonsgegevensbescherming verschilt gedeeltelijk van het begrip informatiebeveiliging. Persoonsgegevens zijn immers geen informatie zonder meer, die als zodanig kan worden beschermd. Door hun specifieke aard moeten deze gegevens en de verwerkingen ervan beantwoorden aan de kenmerken die in de Wet Verwerking Persoonsgegevens (WVP) werden gedefinieerd:

De persoonsgegevens dienen:

- eerlijk en rechtmatig te worden verwerkt;
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die onverenigbaar is met die doeleinden;
- toereikend, ter zake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;
- nauwkeurig te zijn en zo nodig te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om gegevens die onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren;
- in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer te worden bewaard dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder worden verwerkt.

De organisatie moet technische en operationele maatregelen en beheersmaatregelen treffen om:

- de verwerkingen bij de Commissie voor de bescherming van de persoonlijke levenssfeer aan te geven als die een aangifte vereisen;
- de rechten van de betrokkenen te eerbiedigen, met name toestemming, verificatie, wijziging en schrapping;
- de gegevens bij te werken, of onjuiste, onvolledige of irrelevante gegevens te verbeteren of te verwijderen;
- er zich van te vergewissen dat de verwerkingen gebeuren overeenkomstig de doeleinden en de wettelijke voorschriften;
- toegang tot de gegevens te beperken tot die personen die ze nodig hebben voor de uitoefening van hun functie of dienst;
- de personen die gemachtigd zijn de gegevens te raadplegen in te lichten over hun plichten krachtens de wet en hen desgevallend een vertrouwelijkheidsverklaring laten ondertekenen;
- de bescherming van de persoonsgegevens in de tijd te behouden;
- indien een beroep wordt gedaan op een verwerker, via een contract de verplichtingen van de verantwoordelijke voor de verwerking aan hem over te dragen.

Daarnaast moeten die maatregelen een passend beschermingsniveau waarborgen, waarbij enerzijds rekening wordt gehouden met de stand van de techniek en de kosten om die maatregelen toe te passen en anderzijds met de aard van de te beveiligen gegevens en de potentiële risico's.

Er kan dus gesteld worden dat bescherming van persoonsgegevens een fundamenteel recht is waarvan de uitvoering afhangt van bepaalde beheersmaatregelen of, anders gezegd, dat een benadering vanuit beveiligingsoogpunt noodzakelijk is voor een goede bescherming van persoonsgegevens.

2. Hoe wordt een beveiligingsproces opgesteld ?

2.1. Algemene beveiligingsprocessen

Een doeltreffende beveiliging zonder disproportionele maatregelen vergt een gestructureerde en rigoureuze benadering.

Er zijn verschillende methodes om de bestaande beveiliging te beheersen. Ze bestaan over het algemeen uit drie grote categorieën van processen:

- **risicobeheer** identificeert de belangrijkste risico's, waarbij een onderscheid wordt gemaakt tussen de risico's die moeten worden aangepakt en de aanvaardbare risico's. Het zet beveiligingsmiddelen in die de gevaren die persoonsgegevens kunnen lopen volgens een prioriteitenschaal behandelen. Het risicobeheersproces vormt een cyclus die herhaald wordt afhankelijk van de bijzondere kenmerken van de systemen en de geïdentificeerde risico's. Risicobeheer mondt uit in eindprocessen en updating van het informatiebeveiligingsbeleid en dikwijls ook in aanpassingen in de organisatie en procedures zodat beter rekening wordt gehouden met nieuwe risico's en getroffen maatregelen;

- **dagelijks beveiligingsbeheer** dat bestaat uit activiteiten zoals administratie van beveiligingsvoorschriften, beheer van machtigingen, analyse van ontdekte incidenten;

- **managementsysteem** dat de beveiliging permanent verbetert; er bestaan verschillende modellen voor managementsystemen inzake informatiebeveiliging (ISMS – Information Security Management System). Het meest gekende systeem is gebaseerd op een PDCA-structuur (Plan-Do-Check-Act). De voortdurende verbetering van de beveiliging is gelinkt aan evolutieve factoren, bijvoorbeeld wijzigingen van de organisatie en de daarmee verbonden risico's, wijzigingen in het informatiesysteem, technologische nieuwigheden zowel voor operationele systemen als voor beveiligingsvoorschriften.

2.2. De risicoketen

De verschillende elementen van een beveiligingsproces zijn:

Het vermogen van de organisatie

Het vermogen (patrimonium, activa of bezit) van een organisatie is alles wat voor haar waarde heeft of anders gezegd alles wat de organisatie waardevoller maakt of nog, alles wat bij verlies de waarde of de doeltreffendheid van de organisatie zou doen verminderen.

In het kader van de beveiliging van persoonsgegevens worden persoonsgegevens en alle noodzakelijke hulpmiddelen om ze correct te verwerken als bezit beschouwd:

- materiële bezittingen waarin de gegevens zijn ondergebracht (gebouwen, machines, informaticamaterieel, enz.);
- de noodzakelijke software voor de gegevensverwerking (de gebruikte toepassingen en programma's, de besturingssystemen enz.);
- de gebruikte informatie bij die gegevensverwerkingen, die onder verschillende vormen kan worden opgeslagen: in de databank, op papieren drager, enz.);
- de infrastructuur (de basisdiensten die noodzakelijk zijn voor de organisatie opdat ze haar doel zou bereiken; elektrische energie, verlichting, communicatie, transport, liften, enz.);
- het personeel (de werknemers van de organisatie, tijdelijk personeel, enz.);
- het niet-tastbare bezit (reputatie, merkimago, ethische waarden, enz.);
- de noodzakelijke financiële middelen voor de goede werking van de organisatie.

De dreiging

Een dreiging is elke onverwachte of onverhoopte gebeurtenis die aan een van de activa van de onderneming schade kan toebrengen en dus de bescherming van de persoonsgegevens kan schaden.

Het kan gaan om omgevingsdreigingen (brand), technische dreigingen (systeemdefecten) of menselijke dreigingen.

Menselijke dreigingen kunnen toevallig zijn (vergissingen, vergetelheid, ongeschikte procedures) of opzettelijk (boos opzet, indringing, diefstal), intern (verspreiding van informatie) of extern (industriële spionage).

Kwetsbaarheid

Kwetsbaarheid is de zwakke schakel van een bezitting of een groep bezittingen die door een of meerdere dreigende gevaren kan worden uitgebuit (ontwikkelingsfout, verkeerde installatie). In de meeste gevallen is kwetsbaarheid, eerder dan aan de bezitting zelf, te wijten aan het feit dat een bezitting te weinig bescherming geniet.

Kwetsbaarheid op zich berokkent de organisatie geen enkele schade. Alleen wanneer een dreigend gevaar bij toeval gebruik kan maken van de kwetsbaarheid en van eventuele bijzondere omstandigheden, kan zich een incident voordoen dat mogelijkerwijze schade berokkent.

Incidenten

Een incident is een onverwachte en onverhoopte gebeurtenis die ernstige gevolgen kan hebben.

Een informatiebeveiligingsincident is elke onverwachte of onverhoopte gebeurtenis die een activiteit of de informatiebeveiliging van een organisatie kan aantasten (disfunctie of overbelasting van een systeem, menselijke vergissing, abnormale of ongewone werking van een software of apparaat). Een incident op zich is noch goed noch slecht.

De impact

De impact zijn de gevolgen van een incident op een of meerdere activa (bijvoorbeeld persoonsgegevens die niet langer exact zijn).

Bij informatiebeveiliging wordt meestal een onderscheid gemaakt tussen het rechtstreekse gevolg (schade aan het informatiesysteem, zoals de wijziging van een bestand, van de toegankelijkheid tot een vertrouwelijk gegeven of een ongepaste stopzetting van het systeem) en de onrechtstreekse impact (de schade die de organisatie of derden hebben geleden, zoals misbruik van vertrouwelijke informatie, verkeerde beslissingen ten gevolge van onjuiste gegevens).

Er bestaat niet altijd een onmiddellijk verband tussen de rechtstreekse gevolgen en de onrechtstreekse impact van een incident op een organisatie of op derden: het verlies van een elementair gegeven kan enorme gevolgen hebben voor de betrokken persoon terwijl een volledig gewist systeem al hersteld kan worden aan de hand van een correct uitgevoerde back-up.

Risico

Een risico is een bepaald gevaar dat de kwetsbaarheden van een activa of een groep activa uitbuit en dus de organisatie schade berokkent (bijvoorbeeld een virus dat een bestand wist). Het risico wordt bepaald door de waarschijnlijkheidsberekening van een gebeurtenis, te combineren met de gevolgen ervan.

Een risico wordt dus gekenmerkt door twee factoren: de waarschijnlijkheid dat zich een incident voordoet en de ernst van de potentiële rechtstreekse gevolgen en onrechtstreekse impact.

Het risico kan ook afhangen van een tijdsfactor: de situatie kan na een incident verergeren als er niet bijtijds bijsturingsmaatregelen worden genomen (bijvoorbeeld fout in de software die de databank aantast, spyware die paswoorden, versleutelde codes of pincodes binnenhaalt). Zo kan een op onschuldig incident catastrofale gevolgen hebben.

Beheersmaatregelen

Beheersmaatregelen, ook "beschermingsmaatregelen" of "beveiligingscontrole" genoemd, zijn procedures of beslissingen die de risico's verkleinen. Beveiligingsmaatregelen kunnen op verschillende manieren doeltreffend zijn: door de mogelijke gevaren te verminderen, kwetsbaarheden te corrigeren of door de mogelijke rechtstreekse gevolgen of onrechtstreekse impact te beperken. Het is ook mogelijk om op de tijdsfactor te werken. Door incidenten beter en vroeger op te sporen, kan er immers opgetreden worden vooraleer de situatie verergert.

Het restrisico

Restrisico's zijn de risico's die blijven bestaan na de risicobehandeling of, anders gezegd, nadat beschermingsmaatregelen werden ingevoerd.

2.3. Probleemstelling

Utopie van het nulrisico

Zoals reeds eerder gemeld, is beveiliging de toestand van een systeem waarin de zeven beveiligingskenmerken behouden blijven, nl. vertrouwelijkheid, integriteit, beschikbaarheid, toerekenbaarheid, authenticiteit, betrouwbaarheid en onweerlegbaarheid.

Beveiliging is dus een toestand van blijvende valabele informatie met een infrastructuur die de integriteit van de gegevens perfect waarborgt en waar het altijd mogelijk is om kwaadwillige acties op te sporen en te verijdelen.

Een dergelijke beveiligingstoestand is natuurlijk een onbereikbaar ideaal. Talrijke factoren maken dit onrealistisch, waaronder onbekende en onzekere factoren, menselijke fouten, toenemende erosie van bepaalde beschermingsmaatregelen, onvoorzienbare veranderingen, kwaad opzet dat zich meestal daar voordoet waar het het minst verwacht wordt. Meer nog, een ideale dekking tegen risico's, vereist financiële en menselijke middelen die meestal buiten het bereik van de capaciteiten van de organisatie liggen.

Risico's behandelen

Er blijft dus altijd een risico waarmee men moet leren leven. De enige parameter waarop kan worden gewerkt, is het restniveau van dit risico.

In dit opzicht is beveiliging dus de kunst om risico's te beheren en wordt beveiligingsbeheer risicobeheer. Hierbij komt het erop aan de drempel te bepalen voor een onaanvaardbare overschrijding van die drempel en een aanvaardbare, d.i. wat uitgaande van de mogelijke beschikbare middelen, geaccepteerd zal moeten worden.

Omdat iedere organisatie uniek is, spreekt het vanzelf dat een aanvaardbaar risiconiveau verschilt naargelang van de organisatie. Dit aanvaardbare risiconiveau moet de hoeksteen worden bij de ontwikkeling en organisatie van het beveiligingssysteem dat specifiek aan iedere organisatie werd aangepast.

Precies daarom er bestaat geen wonderformule die voor alle organisaties minimale standaardbeveiligingsmaatregelen kan waarborgen voor een gepast beveiligingsniveau.

Iedere organisatie moet dus voor zichzelf de noodzakelijke, specifieke en individuele beveiligingsmaatregelen ontwikkelen zodat zij haar eigen beveiligingsdoelstellingen kan verwezenlijken.

Om tot een optimaal risicobeheer te komen moet iedere organisatie dus een methode ontwikkelen die strikt aan haar eigen context is aangepast.

Risicobeheer vergt niet alleen een methodisch kader maar ook gezond verstand. Er moet immers ook nog met andere elementen rekening worden gehouden.

Een totale beveiliging is zo sterk als het zwakste punt van de organisatie. Beveiliging moet dus gezien worden als een globaal probleem en moet homogeen ontworpen worden voor het gehele informatiesysteem.

Beveiliging bestaat slechts uit een geheel van compromissen. Immers, hoe hoger het gewenste beveiligingsniveau, hoe zwaarder en complexer de controles zijn, hoe ingewikkelder de administratie wordt en hoe moeilijker het is de informatie te gebruiken.

Die compromissen houden niet alleen rekening met mogelijke problemen maar ook met de financiële last van de voorgestelde oplossingen. De kost van de geplande beheersmaatregelen moet

vanzelfsprekend worden afgewogen tegenover de waarde van de te beschermen activa en aan de mogelijke gevolgen van een beveiligingsincident door een gebrek aan bescherming.

Risicobeheer opzetten moet dus gebeuren zoals een goede huisvader dat zou doen.

Risicobehandeling van persoonsgegevensverwerkingen

Bij de verwerking van persoonsgegevens worden de vereisten van de WVP omgezet in operationele en concrete beveiligingsvoorschriften.

Daarvoor moeten persoonsgegevens geïnventariseerd worden en moeten de volgende vragen beantwoord worden voor iedere groep persoonsgegevens:

- *Vertrouwelijkheid*: welke personen, systemen of processen hebben toegangsrecht tot de gegevens? Wanneer en onder welke voorwaarden ?
- *Integriteit en betrouwbaarheid*: hoe worden de gegevens ingezameld? Welke personen, systemen of processen zijn gemachtigd om die gegevens te wijzigen of te verwerken en onder welke voorwaarden?
- *Beschikbaarheid*: binnen welke termijn en via welke uitwisseling moeten die gegevens toegankelijk zijn voor de gemachtigde personen, systemen of processen?
- *Bewijzen* (authenticatie, toerekenbaarheid en onweerlegbaarheid) welke bewijzen moeten desgevallend worden geproduceerd?

2.4. Risicobeheer

Goed risicobeheer vergt een opeenvolging van verschillende activiteiten.

Beveiligingsdoelstellingen bepalen

Het is van wezenlijk belang dat de organisatie, volgens de prioriteiten van haar opdracht of volgens haar ethische waarden, klaar en duidelijk haar beveiligingsbehoeften identificeert en de prioriteiten bepaalt die zij noodzakelijk acht om aan deze behoeften te voldoen.

Identificatie, inschatting en evaluatie van het risico

Voor de *identificatie van het risico* worden de gevaarlijke situaties bepaald die, bij gebrek aan beveiliging, kunnen leiden tot een schending van de beveiligingsvoorschriften. Het gaat om situaties

die afhankelijk van de gebeurtenis schade kunnen berokkenen aan de organisatie of een derde kunnen benadelen.

Om een *risico in te schatten* wordt berekend hoe groot de kans is dat een incident gevolgen heeft. Daarbij wordt rekening gehouden met de eigen situatie van de organisatie, zoals mogelijke dreigingen of technologische kwetsbaarheden. De inschatting gebeurt systematisch en kan op verschillende manieren worden aangepakt, soms via formele methodes met een systematische en nauwgezette aanpak maar. Uitgaande van de situatie zijn die methodes soms echter te zwaar of te duur. Andere, meer eenvoudige methodes, doen een beroep op referentieniveaus inzake beveiliging. Iedere organisatie moet de oplossing kiezen die voor haar het meest geschikt is.

Voor de *evaluatie van het risico* wordt het ingeschatte risico vergeleken met de criteria van de organisatie (bijvoorbeeld haar sociale prioriteiten, haar financieel beleid of haar ethiek) en ook met de verschillende wettelijke voorschriften. Aan de hand van een evaluatie kunnen de risico's worden vastgesteld die *in abstracto* prioritair moeten worden behandeld.

Het risico behandelen

Eens de risico's geëvalueerd, moet er worden beslist of ze behandeld dan wel geaccepteerd worden.

Bij een risicobehandeling moet geopteerd worden voor een of meerdere beheersmaatregelen waarmee de risico's kleiner worden, de gevolgen minder ernstig zijn of helemaal verdwijnen. Het is een zoektocht naar de meest geschikte beheersmaatregelen op basis van een kosten-batenanalyse.

Sommige risico's kunnen worden overgedragen door ze bijvoorbeeld te verzekeren.

Bij een beslissing om risico’s te behandelen, wordt een prioriteitenlijst opgesteld. De risico's die prioritair moeten worden behandeld, zijn die die door de wet of een andere dwingende regel worden opgelegd (bijvoorbeeld toegang tot persoonsgegevens beperken). Vervolgens komen de risico's aan bod die tegen een minimale kost maximaal verminderd kunnen worden. Tot slot wordt de laagste prioriteit toegekend aan de "kleine" risico's, waarvoor de kans klein is dat ze voorkomen of die geen grote gevolgen zullen hebben.

Bepaalde risico's aanvaarden

Bepaalde risico's kunnen niet behandeld worden omdat het technisch onmogelijk is of de kostprijs onredelijk hoog ligt. Voor die risico's moet de algemene leiding van de organisatie een aanvaardingsbesluit nemen waarin de niet-behandeling van de risico's wordt verantwoord.

Voor nog andere risico's blijkt het voordeliger om, in geval van onverwacht onheil, de gevolgen ervan te dragen eerder dan het risico zelf vooraf te behandelen. Een voorbeeld: een grote databank die maar weinig veranderingen ondergaat kan makkelijker worden beveiligd met een kopie waarin maar zelden informatie van de opeenvolgende wijzigingen wordt aangevuld dan met een kopie die vaak en volledig werd aangevuld.

Beheer van restrisico's

Restrisico's moeten voortdurend worden opgevolgd. Het is mogelijk dat een beslissing tot behandeling zich opdringt wanneer waardoor de restrisico's als gevolg van bepaalde omstandigheden onaanvaardbaar worden en de behandeling ervan denkbaar of verantwoord wordt. Ook door een nieuwe wettelijke verplichting kan behandeling noodzakelijk worden.

Communicatie over de risico's

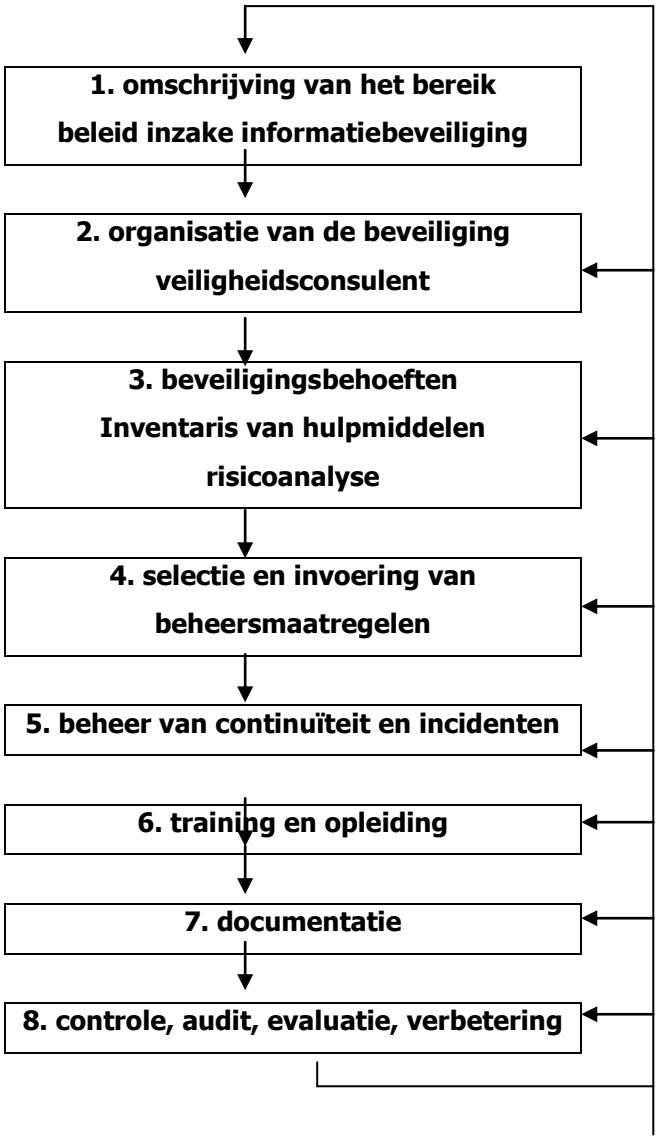
Er moet vanaf de start van het beveiligingsplan communicatie zijn over de risico's en het risicobeheer en dat moet zo blijven bij elke nieuwe stap in het ontwerp, de opmaak, de invoering en onderhoud ervan. Binnen elke organisatie moet iedere werknemer op de hoogte zijn van de risico's die aan zijn werkzaamheden verbonden zijn en vooral over de risico's voor persoonsgegevens. Eenieder die in het kader van zijn werkzaamheden met een beveiligingsrisico geconfronteerd kan worden, moet ingelicht worden over dit risico, de toepasselijke beheersmaatregelen en de op te volgen regels, zodat de doeltreffendheid van die maatregelen bewaard blijft.

De opvolging controleren

De organisatie moet tijdens haar activiteiten de beheersmaatregelen opvolgen en controleren. Het is immers noodzakelijk erover te waken dat beschermingsmaatregelen hun doeltreffendheid bewaren, dat nieuwe omstandigheden geen veranderingen teweeg brengen voor een of ander aspect van de bestaande risicobeoordeling en dat incidenten zo goed mogelijk worden opgespoord. Daarnaast moet worden nagegaan of alle beslissingen tot bijsturing of verbetering binnen de verwachte termijn in daden werden omgezet.

3. Algemene benaderingswijze voor informatiebeveiliging

3.1. Algemene benaderingswijze



1. Regelmatig het informatiebeveiligingsbeleid herzien en verspreiden binnen de organisatie. Het bereik van dit beleid moet worden vertaald in organisatie, lokalisering en hulpmiddelen.
2. De organisatie van de beveiliging aanpassen aan de behoeften en evoluties en een duidelijke omschrijving van de verantwoordelijkheden, taken en bevoegdheden.
3. De nodige hulpmiddelen voor de beveiliging bepalen die binnen het bereik liggen van het beveiligingsbeleid, een inventaris van de hulpmiddelen en een risicoanalyse opmaken.
4. De beheersmaatregelen om risico's te voorkomen kiezen en invoeren.
5. Voorzien in de voortzetting van de essentiële activiteiten van de organisatie bij rampen, beheer van beveiligingsincidenten.

6. De noodzakelijke maatregelen nemen zodat elke betrokken persoon voortdurend en voldoende wordt ingelicht over zijn plichten en verantwoordelijkheden en correct geïnformeerd wordt over de uitoefening van zijn functie en zijn verantwoordelijkheden inzake beveiliging.
7. De documentatie samenstellen die nodig is voor een goed beveiligingsbeheer.
8. Voortdurend toezicht op de ingevoerde beheersmaatregelen om na te gaan of ze nog geschikt zijn om de daadwerkelijke risico's te voorkomen en eventueel voorzien in bijsturingsmaatregelen.

3.2. Taken en verantwoordelijkheden

Wie is binnen de organisatie verantwoordelijk voor de informatiebeveiliging?

Informaticabeveiliging was lange tijd een zaak van het technisch departement en het informaticadepartement. Het volstond dat elk op zijn gebied de technische middelen inzette die noodzakelijk waren om de systemen te beschermen.

De evolutie in de beveiliging en in de verschillende beschikbare middelen vergt vandaag een veel globalere aanpak, vooral waar het bescherming van persoonsgegevens betreft. Iedere persoon die de beveiliging van een element van het informatiesysteem kan beïnvloeden tijdens het ontwerp, de ontwikkeling, de installatie maar ook en vooral bij het gebruik ervan, draagt een eigen verantwoordelijkheid opdat de vereiste beschermingsmaatregelen doeltreffend zouden zijn. Vandaag betekent dat vrijwel iedere persoon die tot de organisatie behoort.

Een globaal en coherent beveiligingsplan voor een informatiesysteem is dus een permanente opdracht waarbij ieders medewerking vereist is. Het is maatwerk waarin de bedrijfscultuur verweven zit en waarmee een evenwicht moet worden gevonden tussen belangen die meestal tegengesteld zijn aan beveiliging, operationele voorschriften, technische eisen, gebruiksvriendelijkheid en toegekende budgetten.

Een dergelijk plan waarbij elk lid van de organisatie betrokken is, vergt bijgevolg een actief en totaal engagement:

- *van de algemene leiding van de organisatie* om het beveiligingsbeleid te bepalen en uit te voeren, om de individuele taken te regelen en te verdelen, om de nodige middelen te verschaffen, om een risicobeheersproces in te voeren, om te besluiten de belangrijkste risico's te behandelen en de aanvaardbaar geachte risico's te aanvaarden; om beveiligingsregels- en instructies te verspreiden en op te leggen aan het personeel van de organisatie en aan de verwerkers voor opvolging van incidenten en evolutie in de beveiligingsgraad, zodat het noodzakelijk beschermingsniveau wordt behouden en ten slotte om eventuele inbreuken op de beveiliging te onderzoeken en te bestraffen;

- *van het operationeel personeel van de organisatie* (de gebruikers van het systeem) en *de betrokken derden* om de regels en instructies na te leven en om actief bij te dragen aan de bescherming van persoonsgegevens;
- *van de technici* die het informatiesysteem en de specifieke beveiligingsmaatregelen ontwerpen, ontwikkelen, installeren en instaan voor administratie en onderhoud op een zodanige wijze dat de persoonsgegevens voortdurend het vereiste beschermingsniveau genieten.

In dit beveiligingsorganogram is het nuttig bepaalde taken nader te omschrijven:

Verantwoordelijke voor de verwerking

Dit is de rechtspersoon die belast is met de gegevensverwerking en ook verantwoordelijk is voor de toepassing van de WVP. Die verantwoordelijkheid behoort toe aan de algemene leiding van de organisatie, de raad van bestuur of naargelang van het geval de directieraad.

Organisatie van de informatiebeveiliging

De veiligheidsconsulent is de bouwheer van de beveiliging van de organisatie en verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid binnen de organisatie.

Hij bepaalt welke doelstellingen bereikt moeten worden, hij coacht de verschillende partijen die tussenkomen in de installatie van het beveiligingssysteem ongeacht het niveau ervan, en hij verifieert ten slotte de resultaten.

Als veiligheidsconsulent moet hij rechtstreeks rapporteren aan de algemene leiding van de organisatie, over voldoende middelen beschikken (tijd, personeel, uitrusting en budget) en vrijuit toegang hebben tot de informatie die noodzakelijk is voor de uitoefening van zijn functie voor zover hij binnen het kader van het beveiligingsbeleid blijft.

Hij heeft de nodige competenties verworven en opleidingen gevolgd, en kan geen functie uitoefenen noch verantwoordelijkheden dragen die onverenigbaar zijn met die van veiligheidsconsulent.

Hij ziet erop toe dat de verschillende verantwoordelijkheden inzake beveiliging (preventie, toezicht, opsporing en verwerking) duidelijk in kaart zijn gebracht en dat de personen belast met de beveiliging in alle onafhankelijkheid kunnen handelen en ervan gevrijwaard blijven dat ze voor persoonlijke of tegengestelde belangen onder druk worden gezet.

Hij moet meer bepaald:

- de initiatiefnemer en de drijvende kracht zijn achter het informatiebeveiligingsbeleid en de omzetting ervan in diverse strategieën en ook worden betrokken bij de bepalingen van de behoeften en middelen (personele, financiële en materiële, enz.);
- de gangmaker zijn van de "beveiligingscultuur";
- voor alle niveaus (van de algemene leiding tot de gebruikers) de belangrijkste raadgever zijn inzake informatiebeveiliging en voor alle verschillende bestanddelen ervan (fysieke beveiliging van goederen en personen, informaticabeveiliging, interne organisatie, enz.);
- erop toezien dat de geldende wettelijke en reglementaire verplichtingen worden vertaald in concrete oplossingen zowel op personeelsgebied, als op organisatorisch en technologisch gebied;
- in beveiligingszaken de belangrijkste contactpersoon zijn voor derden;
- de nodige schikkingen treffen inzake risicobeheer, de geïdentificeerde risico's valideren en evalueren. Hij staat de leiding bij in haar beslissingen over aanvaardbare risico's, de behandeling van risico's (de beste beheersmaatregelen kiezen) en de aanvaarding van bepaalde risico's;
- de vereisten inzake informatiebeveiliging omzetten in een gedetailleerde opgave zodat alle bestanddelen van het informatiesysteem (materieel, software, human resources, enz.) concreet kunnen ontwikkeld, geïnstalleerd, gebruikt, onderhouden, veranderd en verwijderd worden;
- de ingevoerde beveiligingsmaatregelen valideren door de doeltreffendheid ervan te waarborgen;
- de inzameling van gegevens en de verwerkingen ervan dagelijks opvolgen om na te gaan of het informatiebeveiligingsbeleid goed wordt nageleefd;
- informatiebeveiligingsincidenten opsporen en analyseren, onmiddellijk bijsturen, eventueel maatregelen treffen en op lange termijn verbeteringen aanbrengen,
- eventuele inspecties en audits uitvoeren.

De aangestelde voor de gegevensbescherming

De WVP voert de aangestelde voor de gegevensbescherming in en definieert die aangestelde als de persoon die op onafhankelijke wijze zorgt voor de toepassing van deze wet en van haar uitvoeringsmaatregelen[2].

Een nog op te stellen koninklijk besluit moet heel precies de plichten en verantwoordelijkheden van de aangestelde voor de gegevensbescherming omschrijven, evenals de manier waarop hij zijn functie zal uitoefenen.

[2] WVP, artikel 17*bis*

3.3. Het beveiligingsbeleid

Doelstellingen

Het beveiligingsbeleid is een zaak van de algemene leiding en bevat de gedragscode die de organisatie zichzelf wil opleggen om vaste greep te hebben op de informatiebeveiliging en meer in het bijzonder op de beveiliging van persoonsgegevens.

Het beveiligingsbeleid moet worden neergeschreven in een document, zodat het nauwgezet aan iedere betrokken persoon binnen de organisatie kan worden verstrekt, maar ook aan betrokken derden.

Het beleid omschrijft het beveiligingsniveau dat bereikt moet worden. Het beschrijft in detail de rechten en plichten van alle betrokken personen en kan verder aangevuld worden met procedures die de manier van werken beschrijven en instructies geven die gevolgd moeten worden in specifieke gevallen.

Inhoud

Het beveiligingsbeleid moet ten minste bestaan uit de volgende elementen:

- de basisprincipes van de organisatie inzake informatiebeveiliging, waarin de wettelijke verplichtingen en eigen missies van de organisatie verweven zitten. Het beveiligingsbeleid omschrijft met name de principes die de bescherming van persoonsgegevens regelt;
- de beveiligingsvereisten die moeten worden nageleefd op gebied van vertrouwelijkheid, integriteit, beschikbaarheid, toerekenbaarheid, authenticiteit, betrouwbaarheid en onweerlegbaarheid van informatie;
- verschillende elementen met als doel sensibilisering voor de argumenten en de inhoud zelf van dit beleid dat de organisatie uitstippelde;
- beschrijving van de verschillende taken, verantwoordelijkheden en organisatorische regels voor toepassing van het beveiligingsbeleid;
- opzetten van een door de organisatie goedgekeurd risicobeheer, zodat de risico's volgens vastgelegde criteria kunnen worden opgespoord en beoordeeld en de modaliteiten kunnen worden bepaald voor de behandeling ervan. Zo kunnen ze worden teruggebracht tot een aanvaardbaar risiconiveau;
- de beschrijving van het organisatorisch kader voor beheersprocessen bij beveiligingsincidenten;
- de algemene beheersmaatregelen voor informatiebeveiliging, met name inzake bescherming en voorzienbaarheid;

- de maatregelen waarvoor de organisatie opteerde om het informatiebeveiligingsbeleid te integreren in ontwikkelings- onderhouds- en veranderingsprocessen;
- de maatregelen voor toezicht, evaluatie en actualisering van het informatiebeveiligingsbeleid en de verschillende ingestelde beveiligingsbestanddelen.

Het is meestal nuttig dat de volgende elementen in het beleid worden uiteengezet:

- de prioritaire risico's die beheersmaatregelen vereisen en die de noodzakelijke doeltreffendheid hebben;
- de werkwijze voor sensibilisering, informatieverstrekking en opleiding voor en over het informatiebeveiligingsbeleid, in werking gestelde beveiligingsprocedures en –maatregelen;
- de werkwijze voor het onderhoud van het informatiebeveiligingsbeleid , met name de aanpassingen die werden voorgesteld en de analyse van beveiligingsincidenten of om zich in overeenstemming te brengen met recente wetten;
- de werkwijze om de ingevoerde beheersmaatregelen te controleren, met name dagelijkse inspectie of periodieke audits;
- bepaalde gedragsregels die de beveiligingscultuur opbouwen en bevorderen en die hun weerspiegeling vinden in de dagelijkse activiteiten van het personeel van de organisatie.

Dit beleid moet constant worden bijgewerkt.

4. Referentiemodellen

Een beveiligingsplan opstellen is een complexe aangelegenheid die een systemische aanpak vergt. Er bestaan verschillende referentiemodellen die als gids kunnen dienen bij het ontwerp van het plan.

De OESO-richtlijnen[3]

Om beter gewapend te zijn tegen de nieuwe uitdagingen en risico's verbonden aan de dreigingen die vandaag wegen op de informatiesystemen en –netwerken, deed de Raad van de OESO[4] ten behoeve van de lidstaten op 25 juli 2002 een aanbeveling[5] ter aanmoediging van een daadwerkelijke beveiligingscultuur. Om die te bereiken is het noodzakelijk dat alle beveiligingsprocessen voldoen aan negen algemene principes.

[3] Terug te vinden op volgend adres : http://www.oecd.org/dataoecd/16/22/15582260.pdf

[4] De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) is een internationale organisatie die 30 lidstaten verenigt. De opdracht van de OSOE bestaat erin de economie van haar lidstaten te versterken, de doeltreffendheid ervan te verbeteren, de markteconomie te bevorderen, de vrije handel te ontwikkelen en bij te dragen aan de groei van zowel de geïndustrialiseerde landen als de ontwikkelingslanden. De Commissie van de Europese Gemeenschappen neemt deel aan haar werkzaamheden.

[5] Aanbeveling van de Raad van OESO, 1037ste zitting van 25 juli 2002: "OESO-richtlijn *tot regeling van de beveiliging van informatiesystemen en –netwerken*."

Volgens de OESO zijn de negen grondbeginselen: sensibilisering, verantwoordelijkheid, respons, ethiek, democratie, risico-evaluatie, ontwerpen en invoeren van beveiliging, informatiebeveiligingsbeheer, herevaluatie.

De ISO/IEC 13335 normen[6]

ISO/IEC TR 13335 – *Information Technology – Guidelines for the Management of IT Security* (GMTS) wil een gids zijn voor het management om hen bij te staan in hun keuze van mogelijke beveiligingsmiddelen afhankelijk van de karakteristieken van hun informatiesysteem.

De ISO/IEC 27002 norm[7]

ISO/IEC 27002 norm (vervangt de norm IDO/IEC 17799 sinds 1 juli 2007) – "*Code of Practice for Security Management*" biedt een modelcatalogus met goede praktijken inzake beveiliging, die bij de opmaak van een beveiligingsproces zeer nuttig kan zijn als basisreferentie.

Het spreekt echter vanzelf dat een dergelijke gids, in algemene zin en op internationaal niveau opgesteld, geen gedetailleerde en definitieve oplossingen kan aanreiken voor alle mogelijke beveiligingsproblemen, noch rekening kan houden met de cultuur of wetgeving van ieder land of elke activiteitensector.

Toch kan deze norm beschouwd worden als een betrouwbare gids en goede controlelijst waarin een reeks veel voorkomende goede praktijken worden opgesomd die, willen ze een passende bescherming bieden, natuurlijk telkens moeten worden aangepast aan wettelijke of andere specificiteiten en aan de reële behoeften van de organisatie.

Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens

De Commissie publiceerde "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens" om de verantwoordelijke voor de verwerking te helpen bij de beveiliging van de persoonsgegevens die hij wil gebruiken, verwerken of van plan is te verwerken. Dit document bevat een lijst met actiedomeinen die verband houden met de beveiliging van informatie waarvoor iedere verantwoordelijke voor de verwerking maatregelen moet nemen en die hij vanzelfsprekend moet aanpassen aan zijn eigen context en specificiteiten.

---

[6] Kan gratis geraadpleegd worden of aangekocht bij de bibliotheek van het BNB (Belgisch Normalisatiebureau : http://www.ibn.be) of gekocht worden via de site van de ISO : http://www.iso.org

[7] Kan gratis geraadpleegd worden of aangekocht bij de bibliotheek van het BNB (Belgisch Normalisatiebureau : http://www.ibn.be) of gekocht worden via de site van de ISO : http://www.iso.org

5. Conclusie : de belangrijkste principes

Een beveiligingsprocedure opzetten volgens de belangrijkste principes :

- ***Beveiliging is een essentiële eigenschap van de intrinsieke kwaliteit waarnaar een organisatie streeft***

  Zonder beveiliging is het voor een organisatie onmogelijk een afdoende kwaliteitsvol(le) product of dienst aan te bieden. In zekere zin bepaalt het kwaliteitsniveau dat een organisatie wil bereiken het beveiligingsniveau dat binnen die organisatie noodzakelijk is.
- ***Beveiliging is een cultuur***

  Dit vergt een fundamentele verandering in de bedrijfscultuur, en dit met name in de manier waarop die organisatie omgaat met de informatie die ze verwerkt.
- ***Beveiliging vraagt een systemische aanpak***

  Beveiliging is een geheel. Het is niet voldoende om een reeks formules of specifieke voorschriften toe te passen. De beveiliging van informatiesystemen gaat veel verder dan de simpele invoering van technische oplossingen of de aankoop van bepaalde producten. Het gaat om een probleem dat in zijn geheel moet worden gezien en waar iedere oplossing totaal en coherent moet worden uitgewerkt.
- ***Beveiliging vergt een "bewuste" aanpak***

  Het is van groot belang dat elke beveiligingsoplossing wordt gekozen met volledige kennis van zaken. Het is energieverspilling om in het wilde weg te kiezen voor bepaalde oplossingen. Zelfs wanneer het risico aan derden wordt overgedragen, moet de beveiliging die deze derde realiseert volledig door de organisatie in rekening worden gebracht.
- ***Beveiliging heeft een doel***

  Er wordt niet beveiligd omdat het moet of om een trend te volgen. Er wordt beveiligd omdat bepaalde specifieke doelen willen bereikt worden. Die doelen moeten nauwkeurig worden omschreven in het beveiligingsbeleid van de organisatie.
- ***Beveiliging is in de eerste plaats een zaak van de directie***

  Wanneer een beveiligingsproces doeltreffend wil zijn, is het noodzakelijk dat de leiding en de verschillende verantwoordelijken, met name de verantwoordelijke voor de verwerking, zich ten volle bewust zijn van hun cruciale rol bij de beveiliging binnen de organisatie, maar ook dat zij zich toeleggen op de voorgestelde beveiligingsdoelstellingen en dat zij daaraan actief meewerken.
- ***Daarna is beveiliging een zaak van iedereen***

  Alle leden van de organisatie, ongeacht hun functie, maken vroeg of laat deel uit van de beveiligingsketen en daardoor kunnen zij op een dag de zwakke schakel zijn. Eenieder moet van zijn eigen rol in die keten bewust worden gemaakt en verantwoordelijkheidsbesef worden bijgebracht; elk lid van de organisatie moet daarom worden voorbereid, opgevoed en opgeleid.
- ***Totale beveiliging is een illusie***

Het heeft geen zin om paranoïde te zijn over een 100% sluitende beveiliging. Die bestaat niet. Er moet eerder geopteerd worden voor een systeem dat voldoende ontmoedigt, bestaande uit verschillende risiconiveaus, waarvan elk niveau is aangepast aan de verschillende graden van dreigende risico's zoals die binnen de organisatie werden waargenomen.

- ***Beveiliging is een permanent proces***

  Beveiliging is een nooit voltooide aangelegenheid. Ze moet voortdurend worden onderhouden, in twijfel worden getrokken en aangepast aan veranderingen in de omgeving, aan economische veroudering en aan technologische evoluties.

Maar vooral met een flinke portie gezond verstand:

- ***Er moet net voldoende beveiligd worden, maar ook niet meer***

  Alleen wanneer er werkelijk een risico bestaat voor de organisatie moet er beveiligd worden. Er moet niet beveiligd worden voor het plezier. Zoals overal elders is overijver ook hier verdacht. Beheersmaatregelen treffen die nutteloos zijn omdat er geen risico bestaat of omdat ze in die omgeving onbetekenend zijn, veroorzaakt kosten en een logge organisatie.
- ***Beveiliging moet proportioneel zijn***

  De ingezette middelen moeten "redelijk en proportioneel" zijn in verhouding tot wat beschermd moet worden. Er moet dus een compromis worden gesloten tussen de waarde van het te beschermen goed en de kost voor die bescherming.
- ***Beveiliging is 20% techniek en 80% gezond verstand***

  De beveiliging is nog eerder een organisatorisch dan een technisch probleem. En zonder de 80 % gezond verstand zal die 20% techniek tot niet veel dienen. Het is dus misschien wijzer om eerst de goedkopere organisatieproblemen op te lossen vóór de technische problemen worden aangepakt.
- ***De wet van Pareto[8] geldt ook voor de beveiliging***

  80% van de nagestreefde beveiliging kan reeds worden verkregen met slechts 20% van de totale noodzakelijk inspanning, terwijl de resterende 80% van de totale inspanning moet gebruikt worden om er slechts 20% bijkomende beveiliging aan toe te voegen.
- ***Meer eenvoudige maatregelen zijn even doeltreffend als één logge en ingewikkelde maatregel***

  Zoals de stelling van Bayes[9] aantoont, geeft de combinatie van meer eenvoudige beschermingsmaatregelen, die minder performant en goedkoop zijn, een even goed resultaat als één enkele hyperperformante maatregel die werkelijk erg duur is en zeer moeilijk te installeren (bijvoorbeeld, 4 doeltreffende maatregelen aan 70% zijn gelijkwaardig aan een tot 99 % doeltreffende maatregel).
- ***Het gevaar schuilt binnenshuis***

[8] Vilfredo Pareto (1848-1923) Italiaanse econoom.
[9] Thomas Bayes (1702-1761) Engelse theoloog en wiskundige.

Zoals in alle studies werd aangetoond, komt slecht 10% van de aanvallen van buiten de organisatie en wordt 90% veroorzaakt door de organisatie zelf.

- ***De zwakste schakel in het beveiligingssysteem is de mens***

  Als het personeel de procedures of de geheimhouding niet eerbiedigt, kan zelfs het meest complexe beveiligingssysteem niet baten.

- ***Zich informeren en opleiden komt op de eerste plaats***

  Beveiliging is geen statisch gegeven, daarom zijn permanent informatie en opleiding noodzakelijk om nieuwe uitdagingen te allen tijde het hoofd te kunnen bieden.

En met integratie van de noodzakelijke gegevensbeschermingsprincipes

- ***De bescherming van de privacy is een grondrecht en de uitvoering ervan is afhankelijk van de beveiliging***

  Elk beveiligingsinitiatief moet in die perceptie worden verkend, gestuurd en ervan doordrongen zijn.

  Daarvoor moeten doelstellingen voor privacybescherming die inherent zijn aan de organisatie vanaf het begin deel uit maken van haar beveiligingsbeleid en van eenieder dezelfde toewijding krijgen, dezelfde ruchtbaarheid, dezelfde behandeling en dezelfde ondersteuning als de andere doelstellingen van dit beleid.

  Daarnaast moeten bij het beveiligingsinitiatief, simultaan met de andere behandelde beveiligingsproblemen, alle maatregelen worden getroffen om de integriteit, de vertrouwelijkheid en de beveiliging van de betrokken persoonsgegevens te waarborgen.