Royal Belgian Academy Council of Applied Science

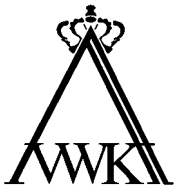
CAWET

Comité van de Academie voor Wetenschappen en Techniek

BEVEILIGING VAN DIGITALE INFORMATIE

Document van de CAWET-werkgroep 55

26 oktober 2007



Koninklijke Vlaamse Academie van België
voor Wetenschappen en Kunsten
Paleis der Academiën
Hertogsstraat 1, 1000 Brussel

INHOUDSOPGAVE

LIJST VAN AFKORTINGEN EN TREFWOORDEN

AES:	Advanced Encryption Standard (Rijndael cryptografisch algoritme)
ASP:	Application Service Providers
ATM:	Automatic Teller Machine
Botnets:	netwerken van geïnfecteerde computers, die gebruikt worden om bv. spam en phishing-mails te versturen of doelgericht diensten aan te vallen
BIPT:	Belgisch Instituut voor Post en Telecommunicatie
CA:	Certification Authority derde partij die publieke sleutels certificeert door ze te koppelen aan een gebruikersnaam
CERT:	Computer Emergency Response Team
CI:	Critical Infrastructure (kritische infrastructuur)
CII:	Critical Information Infrastructure (kritische informatie-infrastructuur)
Cookies:	kleine bestanden op de harde schijf van de gebruiker die gebruikt worden om surfen op het Internet meer gebruiksvriendelijk te maken; ze kunnen ook aangewend worden om gevoelige informatie over de gebruiker te verkrijgen
DDOSaanvallen:	Distributed Denial of Service aanvallen (aanvallen waarbij de dienstverlening van een server gehinderd wordt door duizenden gedistribueerde opdrachten)
DRM:	Digital Rights Management
EEMA:	the European Association for e-identity and security
end-to-end vercijferen:	vercijferen van het ene eind van de communicatie tot het andere uiteinde (in tegenstelling met linkvercijferen, die enkel een verbinding vercijfert)
ENISA:	European Network and Information Security Agency
EVRM:	Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden
EWS:	Early Warning System (systemen die waarschuwen voor virussen en wormen)
Hacker:	persoon die op een gedreven en effectieve manier een computerprobleem oplost. Dit kan zowel neutraal zijn als destructief in het kader van computercriminaliteit bij het inbreken in een computer
ICT:	Informatie- en Communicatietechnologie
IP:	Internet Protocol
IPR:	Intellectual Property Right
ISO:	International Organisation for Standardisation
ISP:	Internet Service Provider
Junkmail:	e-mail waar de ontvanger weinig waarde aan hecht zoals spam, virussen of kettingbrieven
Logische bom:	software die pas schade aanricht onder een vooraf bepaalde voorwaarde
MSSP:	Managed Security Service Providers (Verleners van Beheerde Beveiligingsdiensten)
PDA:	Personal Digital Assistant
PET:	Privacy Enhancing Technology Privacy verhogende technologie
PKCS:	Public Key Cryptographic Standards (Publieke sleutel cryptografische standaarden)
PKI:	Public Key Infrastructure
Phishing:	misleiden van een webgebruiker om gevoelige persoonlijke gegevens zoals paswoorden te bemachtigen

PIN code:	Personal Identification Number
RFID tag:	Radio Frequency Identification Tag
SCADA:	Supervisory Control And Data Acquisition het verzamelen, doorsturen, verwerken, en visualiseren van meet- en regelsignalen van complexe industriële processen of machines
RSA:	Rivest Shamir Adleman publieke sleutel cryptografisch algoritme
SLA:	Service Level Agreement
SIM-kaart:	Subscriber Identity Module kaart uit een GSM toestel
Spam:	ongevraagde elektronische boodschappen voor reclame of andere diensten
Spyware:	kwaadaardige software die binnendringt in de eindapparatuur van de gebruikers om informatie te verkrijgen
SSL:	Secure Socket Layer cryptografisch protocol voor internet
TCPA:	Trusted Computing Platform Alliance
TCP:	Trusted Computing Platform
TCG:	Trusted Computing Group
TLS:	Transport Layer Security cryptografisch protocol voor internet
TPM:	Trusted Platform Module is een identiteits- en beveiligingsmodule voor een PC.
Tijdbom:	is software die pas schade aanricht op een vooraf bepaald tijdsstip
Trojaanse paarden:	zijn programma's die ook andere vaak ongewenste opdrachten uitvoeren dan wat ze voorgeven
Virussen:	schadelijke software die zich in een bestand nestelt en zich voortplant naar andere bestanden bij het openen of uitvoeren van een bestand
VPN:	Virtual Private Network
Wormen:	zijn schadelijke software die zich direct over het netwerk verspreiden
WVP:	Wet Verwerking Persoonsgegevens
XML:	eXtensible Markup Language een standaardtaal voor het gestructureerd vastleggen van gegevens die zowel door de mens als door de computer kunnen gelezen worden

Samenvatting

Dit rapport brengt de actuele problematiek in kaart rond de beveiliging van informatie, zoals deze zich in onze huidige maatschappij stelt. Vooreerst wordt geargumenteerd dat het geheel van bescherming, vertrouwelijkheid, authenticiteit en integriteit van informatie meer dan ooit een belangrijke zorg vormt. De openheid van de communicatiesystemen en hun toepassingen, de snellere doorstroming van gegevens en informatie en het toenemende aantal gebruikers wereldwijd vereisen de aandacht van het totale netwerk en de ganse maatschappij. De rol van de diverse actoren, zoals de overheid, de bedrijven, de ICT- dienstverleners, de maatschappij en de burgers in dit geheel wordt geformuleerd. De juridische aspecten vormen een belangrijk onderdeel in deze thematiek. Vele diverse toepassingsdomeinen worden meer specifiek toegelicht. Ten slotte worden de actuele en relevante technologische methodieken besproken. De veiligheid van een informatiesysteem wordt immers, zoals de sterkte van een ketting, bepaald door de sterkte van de zwakste schakel.

De voornaamste aanbevelingen zijn:

– ruime aandacht in de media om de waakzaamheid en de zorg voor de beveiliging van informatie bij het bredere publiek blijvend te stimuleren,
– managers, bedrijfsleiders, diensthoofden en personeel verantwoordelijk voor diverse infrastructuren, bedrijven en diensten dienen terdege rekening te houden met de totale informatiebeveiliging zowel in het ontwerpproces als in de bedrijfsprocessen,
– creatieve ingenieurs, informatici en juristen met gedegen kennis van de beveiliging van informatie kunnen deze noden aan beveiligingsproducten en diensten aangrijpen voor relevant onderzoek, ontwikkeling en innovatie,
– een aangepaste aanpak is gewenst waarbij de jongeren een verantwoord gedrag, houding en ethisch bewustzijn worden aangeleerd vanaf een jonge leeftijd. Zowel de ouders, grootouders als het onderwijzend personeel moeten hiertoe geïnformeerd en opgeleid worden,
– meer aandacht in de wetgeving op internationaal niveau voor de cybercriminaliteit en de bescherming van de persoonlijke levenssfeer,
– betere coördinatie van alle aspecten van informatiebeveiliging op overheidsniveau. Ontwikkelen van een geïntegreerde onderzoeksstrategie op het vlak van informatiebeveiliging met extra aandacht voor de bescherming van kritische ICT-infrastructuur. Uitwerken van een incidentprocedure.
– in de mate van het mogelijke en redelijke moet beveiliging gebruik maken van standaarden en *best practices* die hun deugdelijkheid bewezen hebben,
– een internationale ethische gedragscode opstellen en bekendmaken voor de diverse betrokken groepen.

Executive Summary

This report describes the key issues related to the security of information as they are surfacing in our contemporary society. First it is argued that the realm of the protection, confidentiality, authenticity and integrity of information is more than ever an important item of concern. The wide access to information, the wide availability of ICT systems and their enormous applications, the fast transmission of data and information, and the ever increasing number of users worldwide, justify the attention of the entire network and society as a whole. The role of the different stakeholders, the government, the companies, the ICT service providers and the society and its citizens are situated within this framework. The juridical aspects constitute an important component. Many diverse application domains are specifically highlighted. Finally, actual and relevant technological methods are surveyed. The security of an information system is, like the strength of a chain, determined by the strength of its weakest link.

The report is making a few important recommendations:

– wide coverage in the media in order to stimulate the broad society's vigilance and caring for the protection of information
– managers, responsibles for diverse ICT and critical infrastructures, in companies and services should be concerned about global information security issues as well during the design of these systems as in the business processes themselves,
– creative engineers, informaticians and lawyers with a solid understanding of the issues of data security have opportunities to design and deploy security products and services through relevant research, development and innovation.
– an appropriate campaign is needed to stimulate youngsters to responsible behaviour and ethical conduct from an early age on. Parents as well as grandparents and teaching staff should be informed and trained for it.
– more legislative attention at an international level for the cyber criminality and the privacy protection.
– better coordination of all aspects of information security at the government level. Development of an integrated research strategy at the level of information security with special attention for the critical ICT-infrastructure. Development of an incident procedure.
– as far as possible and reasonable security should be based upon standards and best practices that have proven their soundness.
– an international ethical code of conduct should be laid down and communicated to the various concerned groups.

INLEIDING

In een vorig CAWET rapport: “Elektronisch zaken doen in een netwerkeconomie” [1, 2002] werd de problematiek van de informatiebeveiliging slechts gedeeltelijk behandeld. Bovendien is sindsdien het belang van elektronisch zakendoen, internet en digitale informatie in het algemeen nog sterk toegenomen en de beveiliging ervan is meer dan ooit een belangrijk aandachtspunt voor diverse gebruikers en verantwoordelijken. Talrijke veiligheidsproblemen zoals virussen, wormen, hackers en computerfraude komen regelmatig in de pers en alarmeren het grote publiek soms te veel en soms ook te weinig. In dit rapport wordt getracht een bondig leesbaar maar ook breed beeld te scheppen van deze problematiek, de omvang ervan en de middelen om beveiliging te realiseren. We sluiten af met een beperkt aantal besluiten en raadgevingen voor de diverse betrokkenen en hopen dat deze studie de aandacht voor deze belangrijke problematiek mag stimuleren.

1. DIMENSIES VAN DE BEVEILIGING VAN INFORMATIE

Het geheel van databescherming, -vertrouwelijkheid en -integriteit vormt meer dan ooit een belangrijke zorg voor overheden, bedrijven en burgers. De openheid van de communicatie- systemen en hun toepassingen, de snellere doorstroming van gegevens en informatie en het toenemende aantal gebruikers wereldwijd, zorgen ervoor dat de noodzaak van een adequate bescherming niet langer het probleem is van één enkele gebruiker of organisatie, maar van het totale netwerk en de maatschappij als geheel. Om de noodzakelijkheid van beveiliging aan te tonen is het nuttig rekening te houden met de perceptie van het veiligheidsgevoel. Vaak blijkt dat in dezelfde omgeving personen toch een ander gevoel van veiligheid hebben. Voorbeelden zijn legio: waarom wil de éne burger zijn ervaringen en foto’s delen via *blogs* en websites, en wil de andere deze gegevens angstvallig beschermen? Deze gevoelsmatige indruk is onlosmakelijk verbonden met personen, het tijdskader, de ruimte en de gegevens. Juist omwille van deze verschillende indrukken, die vaak tegenovergestelde reacties en denkwijzen binnen een organisatie uitlokken, is er een kader nodig dat burgers en organisaties beschermt. Een kader waarbij moet worden gezocht naar een gulden middenweg, die werkbaarheid en individuele eisen met elkaar combineert.

Maar er is meer: de noodzakelijkheid van bescherming van informatie is bovenal een kwestie van opvoeding. Vergelijk het met een wagen: die gaat toch zonder fout op slot als die achtergelaten wordt op de openbare weg? Hoe vaak echter wordt een computer onbeveiligd achtergelaten op de informatiesnelweg? Diefstal draait niet altijd rond de fysieke ontvreemding van goederen. Het verlies van waarde bij diefstal van elektronische gegevens wordt al te vaak onderschat. Bij een rondvraag bleek dat het illegaal binnenhalen van muziek– en filmbestanden niet wordt aanzien als diefstal, omdat de informatie vrij en gemakkelijk te vinden is op het internet.

Doorheen de eeuwen werd de beveiliging min of meer gedreven door vraag en aanbod, massaverspreiding en toenemende connectiviteit. Gegevens worden belangrijker naarmate de vraag ernaar of de exclusiviteit ervan toeneemt. Deze ontwikkelingen zorgen ook nu – in het informatietijdperk voor een grotere belangstelling bij individuen of organisaties die munt slaan uit het verhandelen van onrechtmatig verkregen gegevens. De snelle evolutie van het computertijdperk heeft deze ontwikkeling van vraag en aanbod niet vertraagd, integendeel. Door de uitbouw van wereldwijde netwerken, bereiken gegevens sneller dan ooit hun eindbestemming. Ook beslissingen nemen of anticiperen op veranderingen kan tegenwoordig razendsnel. Dat de informatiemaatschappij vandaag is wat ze is, heeft ongetwijfeld te maken met het feit dat we zo vlug en ook in alle vrijheid met elkaar kunnen communiceren en ontwikkelen. Aan de andere kant is de kost voor het beschikbaar stellen of dupliceren van informatie spectaculair gedaald. Maar deze ontwikkelingen hebben ook een belangrijke keerzijde: de verdere evolutie van onze informatiesnelweg dreigt elke dag meer en meer verstoord te worden door de onvolmaaktheden in de infrastructuur en door andere belanghebbenden die niet altijd koosjere bedoelingen hebben in deze tijd van mondialisering.

De problemen betreffende infrastructuur stellen zich vooral op het vlak van de grotere complexiteit. Een beheersysteem telt tientallen miljoenen lijnen code en ook software applicaties kunnen zeer uitgebreid zijn. Het is vrijwel onvermijdelijk dat software van deze omvang een aantal fouten bevat (“bugs”); een belangrijke fractie daarvan introduceert problemen in de beveiliging van het systeem. Op deze manier wordt het mogelijk om in te breken of om schade aan te richten. Ondanks alle beveiligingsinspanningen worden elk jaar nog duizenden nieuwe zwakheden geïdentificeerd die steeds sneller worden uitgebuit. Ook de netwerkinfrastructuur wordt steeds complexer en efficiënter en draagt een steeds groeiend multimedia verkeer (audio en film). Het is niet duidelijk of de huidige TCP/IP-infrastructuur voldoende robuust is en zal blijven geschaald worden, zeker niet als het aantal aanvallen toeneemt. Door het verschuiven van de economie naar de cyberwereld is deze ook een meer aantrekkelijk doelwit geworden. In de jaren 1980 en 1990 werden de belangrijkste problemen gecreëerd door hackers, die er vooral op

gericht waren hun kennis te tonen of schade aan te richten. Tijdens de laatste jaren zien we een verschuiving naar de georganiseerde misdaad, die economische motieven heeft voor computercriminaliteit. De uitgevoerde aanvallen worden meer en meer gesofisticeerd; dit is ten dele mogelijk door het groeiend aantal *online tools* dat het mogelijk maakt om complexe aanvallen uit te voeren met een paar muiskliks.

Die mondialisering en het wereldwijde internet zorgen voor een bijkomende uitdaging met betrekking tot beveiliging: namelijk die van de bescherming van de persoonlijke levenssfeer en van onze identiteit. Recente studies tonen aan dat het misbruik van persoonlijke gegevens een van de snelst groeiende plagen is van de komende decennia. Aan de hand van recente virus- en *phishing*technieken, wordt het straks zeer eenvoudig om de identiteit aan te nemen van een persoon die zich aan de andere kant van de wereld bevindt, en zich van geen kwaad bewust is. En het zijn niet enkel de individuen die hiervan het slachtoffer zijn, ook de overheden en bedrijven moeten waakzaam blijven. Informatiebeveiliging is dus meer dan alleen het elektronisch beschermen van gegevens. We moeten rekening houden met de individuele noden van de gebruikers, ervoor zorgen dat diezelfde gebruikers beschermd worden tegen zichzelf en anderen, maar vooral ook dat er werk wordt gemaakt van een goede opvoeding betreffende het omgaan met elektronische gegevens en media.
Het is merkwaardig dat de meeste mensen in cyberspace doof en blind blijven voor alle gevaren die er dreigen, terwijl men voor het vogelgriepvirus wel snel naar de dokter gaat. Preventieve maatregelen – organisatorisch en technisch – om onze computersystemen en netwerken te beveiligen worden door veel bedrijfsleiders en systeembeheerders nog steeds niet genomen. En toch vormen de cyberversies van virussen een even grote dreiging voor de gezondheid van onze ondernemingen en van onze maatschappij. Het is dus noodzakelijk om even stil te staan bij de fenomenen die de goede werking van onze computersystemen en netwerken bedreigen. Hiervoor moeten we ons verschillende vragen stellen. Welke zijn de trends in *cyberspace?* Wat is onze houding ten aanzien van *e-security*? Welke zijn de risico's en wat is de mogelijke schade?

Trends in cyberspace
Sommige dreigingen kunnen vaak al op voorhand voorspeld worden, enkel door de algemene trends te bestuderen. Welke zijn die trends in cyberspace die ons een beter inzicht kunnen geven op de groter wordende afhankelijkheid en kwetsbaarheid van computersystemen en netwerken in onze maatschappij? Goede zakenlui en bestuurders zien meestal wel de mogelijkheden en voordelen die geboden worden door de nieuwe informatie- en telecommunicatietechnologieën. Veel bedrijven en overheidsinstellingen verschuiven hun activiteiten deels of zelfs geheel naar cyberspace. De processen in de reële wereld die worden vervangen door hun cybervariant, verdwijnen geheel of gedeeltelijk. Onze computersystemen en netwerken staan voor steeds meer bedrijfsprocessen in: beheer van klantenrelaties, beheer van de toelevering, de boekhouding, de aan- en verkoop, enz. Daarnaast besluiten bedrijven over te schakelen op "virtueel private netwerken" VPN. De versleutelingtechnieken van deze VPN's maken het mogelijk om vertrouwelijke informatie te verzenden over het "publieke" internet zonder vrees dat de inhoud van het bericht ergens "onderweg" zal kunnen worden gelezen. Op deze manier kunnen bedrijven stoppen met het huren of leasen van "private" datacommunicatielijnen. Die internetverbinding maakt het bedrijven ook mogelijk om hun telefoonkosten te drukken door over te schakelen op de "voice over IP" technologie. Weg met die oude telefooncentrale...leve de internettelefonie! We zien ook meer en meer dat het beheer van deze geïnformatiseerde bedrijfsprocessen wordt uitbesteed, als het niet om de *'core business'* van de bedrijfszaken gaat. Om van al deze aangeboden diensten gebruik te kunnen maken, beschikken steeds meer particulieren en bedrijven over breedbandinternettoegang. Gezien deze abonnementen meestal tegen een vast maandelijks bedrag worden aangeboden, blijven deze aansluitingen vaak 24 uur per dag actief, ook al is de gebruiker niet aanwezig. De infrastructuur bij een eindgebruiker is bovendien in evolutie... Waar we enkele jaren geleden lokale netwerken enkel terugvonden in firma's, is een lokaal netwerk – in vele gevallen draadloos – een veelvoorkomende situatie geworden in huiselijke omgeving. Ook servers draaien meestal dagenlang zonder toezicht.

Houding ten aanzien van e-security
Hoe enthousiast de ondernemers ook zijn om hun activiteiten over te hevelen naar cyberspace, zo terughoudend zijn ze om ook te investeren in de beveiliging van hun nieuwe systemen. Een actief engagement van het management van het bedrijf betreffende *e-security* is niet zo evident. Velen zien *security* als een last, als een kostenfactor in het budget en niet als een noodzakelijkheid om hun zakelijke activiteiten vlot voort te kunnen zetten. Particulieren, maar ook al te vaak bedrijven, denken er niet aan dat hun ICT-infrastructuur en hun gegevens te maken zouden kunnen krijgen met een technisch falen, een veiligheidsprobleem of erger nog het doelwit zouden kunnen worden van (onzichtbare) cybercriminaliteit.

De risico's
Het spreekt voor zich dat veiligheidsmaatregelen verder moeten gaan dan het zich beschermen tegen criminaliteit alleen, ook **natuurlijke risico's** moeten in het oog gehouden worden. Hoe kan je onderneming verder draaien als

de ICT-infrastructuur beschadigd is door een blikseminslag? En hoe kun je verder werken na een grote stroompanne die de hele buurt gedurende een halve dag heeft platgelegd? Ook om de gevolgen van **technische risico's** zoveel mogelijk in te perken, moeten maatregelen voorzien worden. De **menselijke risico's** vormen echter de grootste en meest diverse groep.
Wat als uw secretaresse per ongeluk de enige versie van de financiële begroting voor uw nieuwe businessplan heeft gewist? Waarom hebt u gisteren geen *back-up* gemaakt? Dit is dan wel een *niet-intentionele fout*, maar de gevolgen ervan uiten zich in vele verloren werkuren. Indien er *intentioneel gedrag* aanwezig is, dan spreken we van "computercriminaliteit". Hierbij worden de zwakheden van een ICT-systeem of de organisatie ervan gebruikt of beter gezegd misbruikt om er geldelijk voordeel uit te halen of om schade aan het systeem toe te brengen. Een typisch voorbeeld hiervan is een ontslagen werknemer van een koerierbedrijf, die zich toegang verschaft, zes maanden na zijn ontslag, tot zijn oude kantoor en er bepaalde delen van het reservatiesysteem wegwist, waardoor het bedrijf meer dan een miljoen euro schade oploopt in één weekend tijd. Dit voorbeeld betreft een gevaar van binnen de firma. Het personeel vormt al te vaak de zwakke schakel in de veiligheid, ten eerste omdat net zij toegang hebben tot de gevoelige informatie, ten tweede omdat ze een bepaald vertrouwen genieten en dus weinig of niet gecontroleerd worden en ten derde omdat ze de zwakheden in het systeem kennen of deze eventueel zelf ingevoerd hebben. Een ander voorbeeld is een systeembeheerder, die in een internationaal bedrijf belast is met controle op de integriteit van kredietkaarttransacties, en die alle bruikbare informatie (magnetische stripdata en kredietlijn) verzamelt om deze door te spelen aan de gokmaffia bij wie hij schulden heeft. De dreiging kan echter ook *van buiten uit* komen, en opnieuw zijn motivaties vooral geldelijk gewin of het toebrengen van schade. Zo werd bvb. een Brits bedrijf, dat uitsluitend van zijn e-infrastructuur afhangt, afgeperst onder dreiging van DDOS-aanvallen (*Distributed Denial of Service*); in een dergelijke aanval wordt een server door duizenden machines belaagd met als gevolg dat de dienstverlening vertraagt of onbeschikbaar wordt. Computercriminaliteit kan echter ook gebruikt worden om bepaalde *verklaringen of boodschappen* kenbaar te maken. Begin 2006, gedurende de heisa over de Mohammed-cartoons, werden diverse websites gekraakt met boodschappen van zogenaamde islamitische verzetsstrijders. De geboekte verliezen waren aanzienlijk ten gevolge van de tijd dat deze sites buiten gebruik waren en de kosten voortvloeiend uit het nodige herstel. De dreigende gevaren voor gebruikers van ICT-systemen zijn talrijk en de impact ervan kan sterk variëren, gaande van de ontvangst van vervelende boodschappen tot de beschadiging of het verlies van belangrijke data. De meest frequente toepassingsvormen van *informaticacriminaliteit* zijn: *het verspreiden van virussen, het installeren van spionagesoftware (spyware), het inbreken in computers (hacking), het verspreiden van ongewenste commerciële mail (spam), het saboteren van een website of (chat)netwerk en het misbruik van allerhande betaalkaarten (informaticabedrog). Daarnaast vormen ook inbreuken op de persoonlijke levenssfeer en DDOS-aanvallen een belangrijke bedreiging. Bovendien vergroot de trend naar mobiele systemen en draagbare computers het gevaar voor verlies of diefstal van bedrijfsgegevens.*

De diverse niveaus
Naast de diversiteit op het gebied van verschillende toepassingsvormen is er ook een grote diversiteit inzake doelgroep. Indien men zich wenst te beveiligen, moet dit op verschillende niveaus gebeuren.
De **fysische veiligheid** is de eerste fundamentele stap. Is het gebouw, waarin het informatica- en telecommunicatiemateriaal zich bevindt, voldoende beveiligd? Maatregelen zoals veiligheidsbadges en een apart lokaal voor de server, kunnen hier een belangrijke basis vormen. Door de groei van het aantal laptops, PDA's, *smart phones* en *USB-disks* is het probleem ook uitgebreid naar het beveiligen van een mobiele infrastructuur tegen diefstal.
Indien de fysische veiligheid gegarandeerd is, kan de aandacht gaan naar de **eindgebruiker**. Elke gewone burger die gebruik maakt van een PC en breedbandinternet kan het slachtoffer worden van cybercriminaliteit. Door zijn gebrek aan kennis en vorming wordt hij als gemakkelijk, kwetsbaar doelwit uitgekozen. Deze eindgebruiker wordt dan vaak gebruikt als toegang tot hogere niveaus. Hoe kan dit in zijn werk gaan? Doordat een eindgebruiker zich met zijn geïnfecteerde PC begeeft op het netwerk van het bedrijf, krijgen ook de hackers toegang tot het bedrijfsnetwerk en kunnen ze er op los spioneren. Of door het inpluggen op het bedrijfsnetwerk van zijn geïnfecteerde PC maakt hij de verspreiding mogelijk van kwaadaardige software (bv.: virussen en Trojaanse paarden). Een infectie met *spyware* houdt in dat men als gebruiker bespioneerd wordt en/of bestookt wordt met reclame; het kan de machine ook zeer traag maken. Als de machine gekraakt wordt door een aanvaller, kan het een zombiemachine worden, gecontroleerd van op afstand door de georganiseerde misdaad. Dergelijke netwerken (*botnets* genaamd) worden online verhuurd door de georganiseerde misdaad voor het verzenden van spam en *phishingmails* en voor DDOS- aanvallen. Elke particulier en werknemer bewust maken van de bestaande risico's is dus essentieel. Men moet hierbij ook beroep doen op het individuele verantwoordelijkheidsgevoel: de gemiddelde gebruiker merkt amper op dat zijn machine een zombiemachine geworden is, en hij ondervindt niet altijd zelf de nadelige gevolgen van.

Op het niveau van de **organisatie** is het belangrijk de continuïteit in de bedrijfsprocessen te verzekeren. Een gespecialiseerde kracht als systeembeheerder is daarom noodzakelijk, maar de nodige voorzichtigheid is hier ook

geboden want het principe geldt steeds dat 'niemand onmisbaar is'. Ontdubbelen van de belangrijkste taken is daarom sterk aangewezen. Wat als de systeembeheerder omkomt in een verkeersongeluk en hij de enige was die bepaalde codes en paswoorden kende? Pas als ook iemand anders tot de essentiële informatie toegang heeft, kan de continuïteit gegarandeerd worden. Door de grote geografische spreiding van bedrijven en/of dochterbedrijven wordt meer en meer gebruik gemaakt van systeembeheer op afstand. Bij het overbruggen van deze afstand is er een groter risico op interceptie. Men heeft ook geen fysiek contact meer, men ziet niet met de eigen ogen wie wat doet. Een bijkomende risicofactor is dat bedrijven soms geen of een gebrekkige authenticatieprocedure toepassen. Een identificatie is immers niet voldoende, iedereen kan beweren dat hij deze of gene persoon is, een verificatie van die identificatie is daarom noodzakelijk; dit wordt meestal authenticatie genoemd (zie hoofdstuk 5). Dit kan aan de hand van bepaalde paswoorden en uiteraard mag niet éénzelfde paswoord of sleutelbestand gebruikt worden voor iedereen. Op basis van deze authenticatie wordt dan een autorisatie toegekend. Maar aandacht is steeds geboden, want zelfs in de best beveiligde omgeving kan een crimineel binnendringen als systeembeheerder met zijn gebruikersnaam en paswoord, indien de systeembeheerder dergelijke gegevens opschrijft en op een papiertje op zijn bureau of in zijn tas laat rondslingeren. Een aanbevolen methode om de werknemer ertoe te stimuleren zijn persoonlijke toegangscodes niet aan andere personen mee te delen, bestaat erin toegang tot bepaalde persoonlijke informatie hieraan te koppelen (vb. inzage persoonlijk dossier, inzage loonfiches, aanvragen verlof …). Daarnaast is het ook zeer belangrijk het personeel attent te maken op de risico's van "social engineering", waarbij indringers de naïviteit of behulpzaamheid van werknemers gebruiken om in een systeem binnen te dringen.

Op **nationaal** niveau zijn er enerzijds beperkingen en anderzijds verplichtingen op het gebied van *e-security*, wat soms tot spanningen kan leiden. Enerzijds moet er rekening gehouden worden met de wet op de bescherming van de persoonlijke levenssfeer (08-12-1992). Hieruit vloeit voort dat controle van e-mail en internetcommunicatie van werknemers alleen toegelaten is bij vermoeden van misbruik en dat gegevens niet zomaar bijgehouden mogen worden. Anderzijds moet er rekening gehouden worden met de regels betreffende behoorlijk bestuur (*corporate governance*), die opleggen dat bepaalde gegevens net wel bijgehouden moeten worden. Het is verder sterk aangewezen dat een bedrijf een regelgeving opstelt over het gebruik van e-mail en internet op het werk. Op die manier kunnen dubbelzinnigheden uitgesloten worden. De principes van CAO nr. 81 (26-04-2002) tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op elektronische online communicatiegegevens, kan hierbij zeker van nut zijn. De bevoegdheden van zowel systeembeheerders als gebruikers in een bedrijf moeten duidelijk vastgelegd zijn. Zoniet is er bij 'misbruik' of interne *hacking* mogelijks geen aanwijsbare bevoegdheidsoverschrijding, wat volgens de strafwet vereist is. Zonder duidelijk kader van toezicht is het mogelijk dat de maatregelen die het bedrijf nam tegen een werknemer, die bijvoorbeeld illegaal filmmateriaal afgeladen heeft op zijn PC van het werk, ongedaan worden verklaard door de arbeidsrechtbank. Daarnaast loopt het bedrijf zelf het risico op een veroordeling wegens het illegaal onderscheppen van internetverkeer van de werknemer.

Op **Europees niveau** zijn een aantal richtlijnen, o.a. Richtlijn 2002/58/EC over privacy and elektronische communicatie, uitgevaardigd waar ook verplichtingen en verboden betreffende de 'online werknemer'-materie in terug te vinden zijn. In deze richtlijnen wordt een bepaalde ruimte voor implementatie op nationaal niveau gelaten. Het gevolg is echter dat deze nationale implementatie vaak van land tot land verschillend is. Dit leidt soms tot verwarrende situaties voor organisaties die verspreid zijn over verschillende landen. Dit probleem stelt zich nog duidelijker als een organisatie zich zowel op Europees als op Amerikaans grondgebied bevindt. De Amerikanen hanteren immers verschillende criteria en regels op het gebied van elektronische controle van werknemers. Daarbij komt nog de belangrijke vraag: 'wie is de bevoegde autoriteit voor gerechtelijk onderzoek indien er sprake is van *cybercrime*?' Een Belgische firma die zijn computersysteem in het buitenland plaatst, zal vaak op zoek moeten gaan naar de politie en justitie in het land waar de server staat, indien deze gekraakt blijkt te zijn, tenzij er heel duidelijke aanwijzingen zijn dat de *hacking* vanuit België is gebeurd, wat in de meeste gevallen moeilijk aan te tonen is.

***e-Security* als strategie**

Binnen **de bedrijven** moeten het veiligheidsbewustzijn, de aandacht en de risicobeheersing een echt deel van de *strategie* worden, niet enkel voor de ICT-verantwoordelijken van een bedrijf, maar ook voor de bedrijfsleiders. Dit is immers noodzakelijk geworden om de bedrijfsactiviteiten vlot en ononderbroken te laten verlopen. Indien managers rekening houden met de hierboven beschreven natuurlijke, technische en menselijke risico's kunnen ze op een adequate manier de continuïteit van hun activiteiten verzekeren. Alle risico's uitsluiten zal nooit mogelijk zijn, maar anticipatie is wel mogelijk, zodat de potentiële schade tot een minimum herleid kan worden. *Tactisch* is het dus belangrijk om procedures te voorzien die enerzijds het dagelijkse reilen en zeilen op het gebied van ICT beschrijven, maar anderzijds ook voorzien wat moet gebeuren in geval van incidenten. Zo snel mogelijk terug operationeel zijn, is in het bedrijfsmilieu de hoofddoelstelling, maar men mag het belang van back-ups bij incidenten niet uit het oog verliezen. Op die manier blijft de informatie behouden om op zoek te kunnen gaan naar de *modus*

operandi en het doel van de dader. Ook als men er de politie wil bijhalen, doet men dit best zo snel mogelijk, zodat er nog fysische en digitale sporen te vinden zijn. De ICT-procedures moeten duidelijk gecommuniceerd worden naar alle werknemers. Zij moeten ook ingelicht worden over de mate waarin de systeembeheerder toegang heeft tot hun persoonlijke zaken. Goede procedures hebben niet veel zin als de toepassing ervan niet gecontroleerd wordt. De voorgeschreven procedures moeten dus *geoperationaliseerd* worden. Zo beveiligde een financieel bedrijf zijn kritisch cryptosysteem door dit te plaatsen in een lokaal met een badgecontrole. Tijdens een fraudeonderzoek bleek echter dat de beveiligde deur met een houten wig geblokkeerd was. De frisdrankenautomaat werd bij gebrek aan plaats in dit lokaal geplaatst. 'Voorkomen is beter dan genezen'... dit gezondheidsprincipe geldt ook voor de preventie en detectie van potentiële aanvallen op een ICT-systeem. Het installeren en nakijken van *logfiles*, te starten bij de perifere diensten (proxy, firewall, mail, VPN, ...) en daarnaast ook bij de interne diensten (file server, dhcp, loginprocedures, ...) zal helpen bij het detecteren van aanvallen op het systeem. Ook verdere informatie betreffende de *modus operandi* van de aanval is dankzij die *logs* mogelijk zodat de dader gestopt kan worden en de schade geschat. In een aantal gevallen kan het zelfs aangewezen zijn om een *intrusion detection* systeem (IDS) te installeren dat aanvallen "*live*" kan detecteren. De preventie of detectie hangt niet enkel af van deze *logfiles* of de installatie van zwaar beveiligde hardwaretoepassingen. De capaciteit van de medewerkers om de rapporten van dergelijke systemen te lezen en te begrijpen is onontbeerlijk. In het geval dat iemand is binnengedrongen in het systeem is het belangrijk na te gaan hoe deze persoon daarin geslaagd is. Bovendien is het essentieel om de bedoeling te achterhalen van deze indringer. De eerste reactie moet er altijd in bestaan om de aanvaller te 'begrijpen'. Het heeft geen zin om een dienst af te sluiten of een nieuwe regel in de *firewall* te creëren zonder begrip van wat is gebeurd. Op basis van de methode, gebruikt door de indringer, kan het objectief van de indringer duidelijk zijn, en kan dit beschermd worden met het adagio: "*Be the goalkeeper and don't run on the whole soccer field*". Vooraleer *servers* opnieuw geïnstalleerd worden is het belangrijk back-ups te nemen van de geïnfecteerde systemen. Speciale aandacht moet ook uitgaan naar de configuratiebestanden en de logbestanden. Het toenemend gebruik van *laptops*, *USB-sticks*, PDA's en *smart phones* stelt bijkomende uitdagingen, vooral omdat deze in toenemende mate gevoelige bedrijfsinformatie bevatten. Men moet rekening houden met de gevolgen van verlies of diefstal ervan en op deze manier kan zeer gevoelige informatie (bijvoorbeeld een klantenbestand of een top secret document) uitlekken. De markt van deze toestellen evolueert zeer snel en vaak is het ook zo dat deze toestellen door de werknemer zelf aangekocht en dus ook beheerd worden. Dit brengt de nood naar voor om duidelijke regels te stellen voor het gebruik ervan.

De laatste tijd is aandacht en bewustzijn i.v.m. beveiliging gegroeid, maar er is meer nodig en het is ook noodzakelijk om dit al in de **opvoeding en het onderwijs** te beklemtonen. Immers, vaak komt de echte aandacht, die gepaard gaat met acties, er pas na het ondervinden van zware beschadiging of gegevensverlies. Ondervinding is de beste leerschool. Er is geen enkele bedrijfsverantwoordelijke zo snel met het nemen van beslissingen en voorzien van budgetten betreffende *e-security* als diegene die geconfronteerd werd met de kosten voor herstel van een ICT-incident (als de schade al te herstellen viel). Het is daarom belangrijk te leren van ervaringen van anderen. De opvoeding over informatiebeveiliging zou moeten starten op school, want daar zou al een belangrijke inspanning geleverd moeten worden. Daarnaast zou elke professionele opleiding in ICT voldoende aandacht moeten besteden aan alle aspecten van informatiebeveiliging. Voorbeelden uit het verleden tonen aan dat de scholen en andere educatieve instellingen zelf vaak te weinig beveiligd zijn. Leraren in lagere en middelbare scholen hebben vaak te weinig kennis over dit domein. Hun studenten echter ontdekken de wondere wereld van de cyberspace...

Informatiebeveiligingsstandaarden worden ontwikkeld door een hele reeks organisaties wereldwijd. Zo zijn de meest bekende met vooral internationale werking en betekenis: ISO, ITU, NIST, ANSI, OASIS,.. en met vooral Europese werking en betekenis: ETSI, CEN/ISSS, ..
Er bestaan momenteel beveiligingsstandaarden voor zowat alle domeinen van de informatiebeveiliging waar oplossingen voor bestaan: cryptografie, chipkaarten en hun lezers, biometrie, web services, etc.. Vaak is het zelfs zo dat er sprake is van competitie tussen standaarden, die bijvoorbeeld afkomstig zijn van verschillende standaardisatieorganisaties, of waar, zij het meer sporadisch, dominante vendors hun marktpositie mee trachten te consolideren (bv. de PKCS standaarden van RSA en nu EMC). Verder zijn er nog sectorale standaarden, bijvoorbeeld de zeer bekende EMV-standaarden die Mastercard en VISA gezamenlijk opstelden en die het mogelijk maken dat beide types kredietkaarten op een veilige manier op dezelfde systemen kunnen gebruikt worden.

In de informatiebeveiliging kunnen open standaarden van belang zijn om uiteenlopende redenen:

- interoperabiliteitsstandaarden zorgen ervoor dat oplossingen afkomstig van verschillende leveranciers met elkaar kunnen samenwerken, wat voor de gebruikers een perspectief biedt op 'best of breed' totaaloplossingen. Voorbeeld: de "Crypto API" van Microsoft maakt het mogelijk dat andere vendors dan Microsoft gebruik kunnen maken van de cryptografische technologie die aanwezig is in Windows.

Hetzelfde soort standaarden zorgt er eenvoudigweg ook voor dat informatie aangemaakt met product A veilig verwerkt (gelezen, geverifieerd,..) kan worden met product B, wat een noodzaak is tenzij men in een strikte "*closed user group*" werkt. Zo kan een bestand dat vercijferd is met het AES-algoritme maar ontcijferd worden als ook de ontvanger AES met dezelfde parameters gebruikt;

- zelfs binnen gesloten gebruikersgroepen, waar met technologie van één leverancier zou gewerkt worden, is er nog behoefte aan kwaliteitsstandaarden, waardoor het ook voor niet-specialisten mogelijk wordt om in te schatten welk beveiligingsniveau behaald wordt mits gebruikmaken van een bepaalde technologie of *policy*. Voorbeelden: "*Common Criteria*" standaarden voor evaluatie van beveiligingsproducten en ISO17799 voor "organisatorische" beveiliging, bijvoorbeeld intern bij *managed security service providers*.

Gesloten systemen, zelfs geheime algoritmes, kunnen enkel in zeer beperkte gevallen verkozen worden, namelijk in besloten *top-secret* omgevingen, zoals militaire systemen. Naast standaarden dient ook het belang van "***best practices***" aangestipt te worden. Strikt genomen gaat het hier niet over standaarden, maar eerder over aanbevelingen voor goed beheer die typisch opgesteld worden door een gebruikersgemeenschap van een welbepaald type oplossing, bijvoorbeeld een *best practice* voor beveiliging van elektronische post. Bij de organisaties die hierin op Europees vlak een rol spelen horen onder andere EEMA en TeleTrusT.

In nagenoeg alle praktische toepassingen wordt een geheel van verschillende standaarden aangewend om een totaaloplossing tot stand te brengen. Bij complexe gehelen leidt dat automatisch tot het fenomeen dat om interoperabiliteit tot stand te kunnen brengen meerdere standaarden op elkaar moeten afgestemd worden. Ook binnen standaarden zélf geldt dit fenomeen: vaak laten ze zoveel keuzeopties open aan de implementatie dat er gewerkt moet worden met een "profiel" van de standaard d.w.z. een welbepaalde invulling voor de keuzes die opengelaten werden binnen één standaard.

Hoewel standaarden van zeer groot belang zijn, wordt hun belang soms ook overtrokken wat vaak leidt tot immobiliteit. Als men steeds gebruik wil maken van de allernieuwste standaard, raken de producenten allicht nooit helemaal bijgebeend met hun implementaties en kan de potentiële gebruiker de fout maken om toch nog maar even te wachten. Dit soort uitstel kan vervolgens leiden tot een permanent uitstel (want er komen steeds nieuwe standaarden bij); zo kan onoordeelkundig gebruik van standaarden ook contraproductief werken.
Dankzij het toponderzoek aan onze universiteiten levert ons land op standaardisatievlak zijn bijdrage, denk maar aan de selectie van het Rijndael algoritme als encryptiestandaard voor de Amerikaanse overheid "AES"; op dit moment is AES een wereldwijde *de facto* standaard geworden geïntegreerd in duizenden toepassingen en producten. Anderzijds dient er opgemerkt te worden dat het vaak de grotere landen zijn die deze scène domineren, waar het behalen van competitief voordeel allicht één van de drijfveren voor is. Zo is bijvoorbeeld bekend dat ook grotere EU-landen al eens proberen hun markt af te schermen via nationale standaarden. Een belangrijk element hierin is het ontbreken in België van een lab voor evaluaties t.o.v. de *Common Criteria* of de FIPS 140 standaard. Dit impliceert dat de Belgische industrie met haar producten naar een buitenlands lab moet, wat een aantal commerciële risico's meebrengt. Dergelijke labs kunnen ook een belangrijke rol spelen als expertisecentrum voor de overheid. Gezien de omvang en kostenstructuur van een dergelijk lab is het misschien aangewezen om samen te werken met een aantal andere kleinere Europese landen.

2. ORGANISATORISCHE ASPECTEN EN ROL VAN DE BETROKKENEN

Het waarborgen van de nodige informatieveiligheid kan niet enkel worden overgelaten aan de ondernemingen of instellingen die informatie al dan niet elektronisch verwerken. De **overheid** dient deze instanties door regelgeving doelstellingen betreffende informatieveiligheid op te leggen. Dit is geschied in verschillende regelgevingen, waarvan er een aantal verder in dit rapport worden besproken. Zo stelt artikel 16, § 4 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna genoemd Wet Verwerking Persoonsgegevens en afgekort als WVP) dat iedereen die persoonsgegevens verwerkt "de gepaste technische en organisatorische maatregelen moet treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's." Daarenboven kan de overheid organisatiestructuren opleggen of invoeren die de informatieveiligheid vorm dienen te geven. Zo zijn alle openbare en private instellingen van sociale zekerheid (RSZ, RVA, ziekenfondsen, arbeidsongevallen- verzekeraars, …) en de ziekenhuizen bijvoorbeeld wettelijk verplicht om een interne informatieveiligheidsconsulent aan te duiden. Ook zijn een aantal sectorale comités van

de Commissie voor de Bescherming van de Persoonlijke Levenssfeer ingesteld, die o.a. minimale veiligheidsnormen kunnen opleggen bij de omgang met persoonsgegevens in bepaalde sectoren, en de in deze sectoren actieve instanties regelmatig ondervragen over de naleving van deze normen. Tenslotte kan de overheid instrumenten instellen om de informatieveiligheid te bevorderen. De elektronische identiteitskaart, die de houder in staat stelt zijn identiteit elektronisch te bewijzen en een juridisch geldige elektronische handtekening te plaatsen, is een dergelijk middel.

Vermits de concrete maatregelen betreffende informatieveiligheid gebaseerd dienen te zijn op een degelijke risicoanalyse en erop gericht dienen te zijn om de risico's te reduceren en de gevolgen ervan te beperken, is een te precieze wettelijke regeling van de inhoudelijke maatregelen niet wenselijk. Wel kunnen domeinen worden aangegeven, bijvoorbeeld onder verwijzing naar internationale standaarden zoals de ISO-norm 17799, waarin maatregelen dienen te worden genomen. De Commissie voor de Bescherming van de Persoonlijke Levenssfeer heeft alvast in een document "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens" (beschikbaar op http://www.privacycommission.be/publicaties.htm) een aantal domeinen aangegeven waarop ze het wenselijk acht dat iedereen die persoonsgegevens verwerkt, gepaste maatregelen treft. Meer bepaald gaat het om het vastleggen van een informatieveiligheidsbeleid, het aanduiden van een informatieveiligheidsconsulent, het instellen van de nodige informatieveiligheidsorganisatie, de fysieke beveiliging van de omgeving, de netwerkbeveiliging, de logische toegangsbeveiliging, de *logging* van de toegangen en de analyse van de logbestanden, het onderhoud en het toezicht, het waarborgen van de continuïteit, het beheer van incidenten en het documenteren. De overheid zou verder een vorm van gecertificeerde zelfregulering kunnen stimuleren in bepaalde sectoren met een uitgebreid elektronisch informatiebeheer (zoals banken, verzekeringsmaatschappijen, distributie, gezondheidszorg, …). Dergelijke zelfregulering laat toe de maatregelen op het vlak van de informatieveiligheid en de bescherming van de persoonlijke levenssfeer optimaal af te stemmen op de specifieke situatie en risico's binnen de betrokken sector. Artikel 44, tweede en derde lid van Wet Verwerking Persoonsgegevens biedt hiertoe een eerste aanzet. Het stelt dat "beroepsverenigingen en andere organisaties die categorieën van verantwoordelijken voor de verwerking vertegenwoordigen, en die ontwerpen van gedragscodes hebben opgesteld of voornemens zijn bestaande gedragscodes te wijzigen of te verlengen, deze kunnen voorleggen aan de Commissie voor de bescherming van de persoonlijke levenssfeer. De Commissie vergewist er zich in het bijzonder van dat de haar voorgelegde ontwerpen in overeenstemming zijn met de wet en haar uitvoeringsbesluiten, en onderzoekt, voor zover dat mogelijk is, de standpunten van de betrokkenen of van hun vertegenwoordigers."

Bedrijven voeren activiteiten uit om hun bedrijfsdoelstellingen te realiseren, en in de meeste gevallen worden zulke doelstellingen bepaald door een raad van bestuur met vertegenwoordigers van aandeelhouders. Deze willen een return voor de door hen ter beschikking gestelde fondsen in de vorm van aandelen. Daarvoor zijn ofwel dividenden ofwel stijgende aandelenkoersen nodig, waarvoor op zijn beurt cashflow dient gerealiseerd te worden. Als nu de *cashflow* van een bedrijf negatief beïnvloed wordt door aanvallen op zijn ICT-infrastructuur, dan raakt dat het wezen van die bedrijfsvoering. Om die reden wordt het bedrijfsleven al vele jaren gewaarschuwd dat de nodige inspanningen vereist zijn om ervoor te zorgen dat dit niet te gemakkelijk of te goedkoop of te vrijblijvend kan gebeuren. Bij financiële instellingen leeft dit besef al heel lang. Dat heeft wellicht ook te maken met het zeer directe verband tussen elektronische transacties en mogelijke geldelijke verliezen, waardoor zij een aantrekkelijk doelwit vormen voor ICT-aanvallen. Ook meer indirecte gevolgen van computerfraude kunnen echter leiden tot lagere returns voor aandeelhouders bijvoorbeeld wanneer de integriteit van een bedrijfsvoering publiekelijk in vraag gesteld wordt omwille van een computerkraak. Het Europese agentschap ENISA analyseert trouwens sinds kort het verlies van reputatie als een afzonderlijk onderwerp. Om die reden wordt het gros van de inbreuken verzwegen en leeft de onterechte indruk dat het "risico overdreven wordt". Bedrijven dienen in essentie twee dingen te doen: a) de kans verminderen dat een inbreuk zich voordoet, b) de impact verminderen als een dergelijke inbreuk zich dan toch voordoet. Een typisch voorbeeld van het eerste is gebruik maken van beveiligingstechnologie, een typisch voorbeeld van het tweede zijn de dag- en weeklimieten op het afhalen van contanten met een bankkaart. In principe kunnen bedrijven zich verzekeren tegen geldelijk verlies dat het gevolg is van computerfraude, maar dat heeft de volgende beperkingen of nadelen:

- de kost van een verzekering is typisch in evenredigheid met het risico en de wellicht geleden schade bij voorval. Operationele & technologische oplossingen echter zijn niet evenredig en moeten in principe altijd goedkoper uitvallen dan een verzekering;
- ook verzekeringen manen hun klanten aan om te beveiligen, zoniet zijn de risico's onverzekerbaar of de premies zeer hoog.

De **dienstverleners van beheerde beveiligingsoplossingen (MSSPs)** zijn organisaties gespecialiseerd in de delocalisering van de ICT-veiligheidsoplossingen voor hun klanten. Dit kunnen zowel grote organisaties of middelgrote en kleine bedrijven zijn. Zij leiden, over veilige verbindingen en in een sterk beveiligd gegevenscentrum, één

of meerdere verschillende veiligheidsdiensten, zoals de beheerde firewall en een opsporingsdienst tegen binnendringen. Dit geschiedt tegen betaling van een abonnementsprijs die gewoonlijk in verhouding is tot het aantal en het type van apparaten en/of diensten die voor de klant worden beheerd. De diensten van "*Managed Security Service Providers*" (MSSPs) zijn goed georganiseerd en de schatting is dat deze sector wereldwijd zal groeien naar $2 miljard in 2007. Kleinere MSSPs verstrekken één of een beperkt aantal veiligheidsdiensten onder het ASP-model, terwijl de grotere specialisten wereldwijde *Secure Operating Centers* (SOCs) hebben die 24 uur op 24 werken en een uitgebreide gamma van beheerde veiligheidsdiensten aanbieden. Deze diensten omvatten perimeter- en extranetveiligheidstoepassingen en toepassingen zoals *firewalls*, VPNs, indringingsopsporing. Andere diensten variëren van preventieve diensten (zoals virus scannen, filteren van spam, mobiele gegevensveiligheid), tot en met diensten voor verrichtingenbeheer (zoals infrastructuurbeheer, beleidsbeheer, controle, analyse), en curatieve diensten (zoals herstel na incidenten). De redenen van de delocalisering van de ICT-beveiliging aan "*Managed Security Service Providers*", die kunnen gezien worden als een gespecialiseerde subcategorie van "*Application Service Providers*" (ASP), zijn divers, en vaak gesteund op het uitbesteden van taken andere dan kerntaken met als doel het reduceren van de kosten.

- Naast het zoeken naar de laagste totale operationele kost, zien velen een hoger beveiligingsniveau als de dominerende factor om MSSP te verkiezen boven eigen ICT-veiligheidsoplossingen. MSSP-klanten ervaren voordelen van de ervaring en efficiëntie van gespecialiseerde externe diensten *providers*.
- Initiële kosten zijn lager en de budgettering is beter voorspelbaar.
- De totale operationele kost kan lager zijn, zeker voor kleine of middelgrote ondernemingen.
- Minder zorgen over veiligheidscontroles en naleving van de verhoogde regelgeving, rapportage en eventuele sanering.
- De steeds stijgende complexiteit van het beheer van de ICT-beveiliging, zoals het opsporen van binnendringers en de behandeling van de vloed van valse alarmen vereist professionele aanpak.

MSSPs verstrekken de nodige controle, monitoring en controlehulpmiddelen, inclusief "*Service Level Agreements* (SLA)", zodat de klanten kunnen tevreden zijn en de controle over hun veiligheid en diensten niet verliezen. Integendeel, dergelijke hulpmiddelen, in combinatie met kwaliteits- en veiligheidsniveaus die te duur zijn om beheerd te worden "in huis", resulteren hoofdzakelijk in een hoger veiligheids- en controleniveau. MSSPs kunnen dus bijdragen tot de algemene beveiliging van onze industrie, door het verstrekken van hoge-kwaliteitsveiligheidsoplossingen tegen een redelijke prijs aan organisaties die anders een veiligheidsrisico vormen door het gebrek aan oplossingen en expertise in eigen huis.

Computernetwerken en het internet hebben vele nieuwe risico's binnengebracht in **onze maatschappij**. In de jaren 1980 en 1990 waren virussen en wormen de belangrijkste risico's. Deze aanvallen werden typisch gelanceerd op grote schaal en besmetten computers die aan het internet worden aangesloten; ze zijn nog steeds belangrijk, maar er duiken nieuwe varianten op die meer gericht zijn en minder visibiliteit creëren maar daarom niet minder schadelijk zijn. Nu zien wij dat de georganiseerde misdaad het internet als interessante markt ontdekte. Nieuwe aanvallen en misbruiken zijn nu *phishing* en *botnets*. Bij vele toepassingen beschikbaar via het internet, wordt de identiteit van mensen nog steeds geverifieerd aan de hand van een gebruikersnaam en een wachtwoord. Als je op één of andere manier deze gegevens kan kopiëren, kan je iemands identiteit stelen. *Phishing* is een techniek waarbij de gebruikers misleid worden in het verschaffen van persoonlijke informatie aan een vertrouwde bron, terwijl zij het in feite aan een misdadige organisatie verstrekken. Een andere frauduleuze techniek zijn de *botnets*. *Botnets* zijn netwerken van gekraakte computers die gecontroleerd worden door een misdadige organisatie. Dit netwerk zal voor misdadige activiteiten worden gebruikt zoals het verdelen van kinderpornografie, spam en het vertragen van de computers van de organisaties door (10.000 computers of meer) gelijktijdig te verbinden aan de aangevallen organisatie. Het laatstgenoemde scenario is typisch een deel van een chantageaanval.
Dergelijke nieuwe aanvallen zijn gebaseerd op twee mechanismen. Het eerste is gebaseerd op sociale technieken. In deze scenario's worden de gebruikers misleid en gedwongen acties te ondernemen die een aanvaller de mogelijkheid geven om de computer over te nemen en zo belangrijke informatie over de gebruiker te verkrijgen, zoals persoonlijke informatie over het inloggen in belangrijke sites. Een tweede type is gebaseerd op de kwetsbaarheden van de veiligheid in beheerssystemen en hun toepassingen. Het kwetsbaarst zijn diensten of toepassingen die rechtstreeks verbonden zijn met het internet. In dit geval, kunnen de computers binnen enkele minuten besmet raken bij verbinding met het internet. De grootte van de aanval verhoogt met de vooruitgang van breedband en bij continue verbinding. In de loop van de laatste jaren heeft de computerindustrie geprobeerd om de veiligheidsbedreigingen te verminderen en vandaag zien we dat de virussen en de wormaanvallen vertragen. Het is belangrijk om op te merken dat dit slechts op recente technologie van toepassing is. Dit is de technologie die ontwikkeld werd met de bedreigingen van internet in het achterhoofd, dus technologie ontwikkeld in het nieuwe millennium. Veel van de nu nog gebruikte oudere technologie echter werd ontwikkeld vooraleer het internet een succes werd. De ontwikkelaars hadden toen geen idee wat de veiligheidsimplicaties van internet op de technologie

zouden zijn, toen ze die ontwikkelden. In de jaren '80 voorspelden weinigen dat het internet vandaag zo alomtegenwoordig zou geworden zijn.

Hoe kunnen we **burgers** beschermen tegen de risico's van het internet? Een basiselement is bewustzijn. De industrie en de overheid zouden de burgers moeten inlichten over volgende basispunten:

- maak zeker een *back-up* van je gegevens. Dit blijft belangrijk in geval van herstel na een aanval;
- hou je systeem up-to-date met de meest recente virusscanners die door de industrie ter beschikking gesteld worden. Microsoft, bijvoorbeeld, biedt een gratis "Microsoft Update" aan: deze dienst houdt de systemen *up-to-date* met de allerlaatste virusscanners. We moeten de burgers aanraden deze systemen te gebruiken om het installeren van *updates* (*software patches*) te automatiseren;
- installeer of activeer een persoonlijke firewall op je PC. Een aantal persoonlijke *firewalls* zijn gratis beschikbaar. Wanneer deze technologie wordt gebruikt, vermindert het risico op aanvallen door wormen aanzienlijk;
- gebruik *antispyware* en antivirussoftware en hou deze software up-to-date. Deze technologieën verminderen de kans op infectie door besmette software;
- wees een voorzichtige burger. Geef geen persoonlijke informatie in *e-mails* door. Wees voorzichtig met hyperlinks die je vindt in *e-mails* of in *websites*. Wees voorzichtig met bijlagen doorgestuurd in *e-mails*;
- wees een goede internetburger door je computer te beveiligen zoals hierboven beschreven en laad en installeer geen software van een onveilige site. Deze software kan je computer infecteren en deel uitmaken van bijvoorbeeld een botnet.

De industrie zou verder moeten werken aan een veiliger technologie om de omvang van de aanvallen van de georganiseerde misdaad te verminderen op de computers van burgers. Om de impact van aanstaande nieuwe aanvallen van het type *phishing* verder te verminderen zouden de diensten van internet moeten afstappen van de gebruikersnaam en wachtwoord. In België werd massaal de Belgische elektronische identiteitskaart eID geïntroduceerd. Het integreren van deze kaart in de belangrijkste diensten van internet zou het internet tot een veel veiligere plaats maken.

3. JURIDISCHE ASPECTEN

Basisbeginselen

Traditioneel probeert de maatschappij via het invoeren van verschillende regels de veiligheid te verhogen. Bijvoorbeeld, toen de mensen begonnen om wegen te gebruiken om zich van één plaats naar een andere te bewegen, werd het noodzakelijk om enkele elementaire verkeerswetten goed te keuren bijvoorbeeld om te bepalen aan welke kant van een tweerichtingsweg men met zijn paardenspan of zijn auto moest rijden.
Soms ontstaan dergelijke regels spontaan omdat zij in de gewoonten ingeburgerd zijn. In andere gevallen, worden de regels gecreëerd door wetgevers of rechters. Tot slot kunnen de regels ook in een systematischere en preventieve manier, in de vorm van een contract, een statuut of één of ander soort tekst worden neergeschreven.
Een regel wordt een rechtsregel van zodra het mogelijk is de naleving ervan door de interventie van de staat af te dwingen. Dit onderscheidt rechtsregels van ethiek, etiquette of andere niet bindende gedragsnormen. Rechtsregels zijn per definitie bindend en afdwingbaar. Deze kenmerken onderscheiden hen bijvoorbeeld van technische normen. Deze laatste zijn vrijwillig en per definitie **niet** afdwingbaar. In ons Belgisch rechtssysteem spelen de geschreven rechtsregels een zeer prominente rol. In andere rechtssystemen, bijvoorbeeld in de V.S. of Engeland, zijn uitspraken van rechters belangrijker. Oudere of minder ontwikkelde maatschappijen baseren zich zeer op gewoonten als primaire bron van recht.
Het onderscheid tussen rechtsregels en andere gedragsnormen moet niet worden overschat. Diverse categorieën van regels beïnvloeden elkaar. Rechtsregels, bijvoorbeeld, kunnen adequate veiligheidsmaatregelen opleggen die door telecommunicatieoperatoren moeten worden nageleefd maar verwijzen naar het "*the-state-of-the-art*" om de praktische toepassing van de rechtsregel in te vullen. Omgekeerd, kan het overtreden van niet-geschreven gedragsnormen, zoals de algemene plicht van zorg, die op elke volwassene en natuurlijke persoon rust, leiden tot burgerlijke aansprakelijkheid en de gedwongen betaling van schadevergoeding. Desondanks is het onderscheid tussen verschillende categorieën van regels belangrijk om de competitie tussen regelgevers en de processen van regelgeving te begrijpen. Bijvoorbeeld, een regel kan geïntroduceerd worden door één *actor* maar betwist worden en zelfs niet geïmplementeerd worden omdat ze in conflict komt met een regel die door andere actoren gepromoot wordt. Duidelijke voorbeelden zijn de verkeersregels met onrealistische snelheidsbeperkingen. In het gebied van informatiebeveiliging zijn er enkele zeer interessante gevallen van de competitie tussenregelgevers, bijvoorbeeld op het gebied van cryptografie, digitale handtekeningen en privacy.

Een aspect van veiligheid is het beschermen van de staat en de gemeenschap tegen mogelijke vijanden of terroristische aanvallen. Om een voldoende niveau van veiligheid te kunnen garanderen, beweren de staatsveiligheid, leger of politie dat ze aangepaste mogelijkheden nodig hebben voor bewaking, in het bijzonder voor het onderscheppen van elektronische communicatie op publieke netwerken. **Cryptografie** beschikt over middelen om de gebruikers te beschermen tegen het ongewilde binnendringen, maar is tegelijkertijd een obstakel voor de bewaking van publieke netwerken door de officiële instanties. Met als gevolg dat de staat de neiging heeft om regels te promoten die het gebruik van cryptografie beperken. Bijvoorbeeld, in België wordt het gebruik van bepaalde veiligheidstechnieken aan banden gelegd in artikel 127 van de wet over de elektronische communicatie indien het gebruik ervan de interceptie van elektronische communicatie voor gerechtelijke doeleinden zou verhinderen. Gelukkig voorziet hetzelfde artikel ook in enkele belangrijke uitzonderingen wanneer het gebruikt wordt om de confidentialiteit van de communicatie of beveiliging van betalingstransacties te beschermen. Evenwel worden andere beschermingstechnieken, die bijvoorbeeld gericht zijn op het realiseren van anonimiteit, wel beperkt. Operatoren worden gevraagd om gebruikers niet aan te sluiten als ze niet identificeerbaar zijn. Momenteel is deze regel niet van toepassing op voorafbetaalde mobiele telefoniekaarten, totdat artikel 127 verder geïmplementeerd wordt. Het voorbeeld toont aan dat wettelijke regels dikwijls delicate constructies zijn, waarbij moeilijke compromissen moeten worden gemaakt door verschillende partijen (in dit geval: politie en staatsveiligheid, industrie, financiële instanties, mobiele operators, enz.). Dit resulteert niet steeds in een duidelijke en efficiënte wetgeving.

Digitale handtekening

Competitie in het maken van regels kan leiden tot een overregulering. Dit kan worden geïllustreerd door het voorbeeld van de Europese wetgeving over de elektronische handtekening. Om ongecontroleerde nationale regels in sommige lidstaten tegen te gaan werd er in 1999 een richtlijn over dit onderwerp opgesteld. Het hoofddoel van deze richtlijn was de bescherming van de Europese interne markt voor diensten en producten gerelateerd aan de elektronische handtekening en de verzekering van de juridische geldigheid van de elektronische handtekening over heel Europa. Paradoxaal heeft deze richtlijn geleid tot een zeer ingewikkelde en diverse wetgeving in de verschillende lidstaten over heel Europa.

Een belangrijke reden voor deze evolutie is zonder twijfel het gebrek aan communicatie en begrip tussen de juridische en technische partijen in dit gebied. Vanuit juridisch oogpunt is het zeer ongebruikelijk om een nieuwe technologie in een zo vroeg stadium te reguleren, zeker wanneer ze nog vrijwel nergens gebruikt wordt. In het geval van de elektronische handtekeningen werden de basisveiligheidsvereisten onderhandeld op politiek niveau en neergeschreven in een juridische tekst. In een tweede fase werden standaarden opgesteld om de wettelijke vereisten in technische specificaties om te zetten met het gevolg dat de standaarden niet noodzakelijk op dezelfde lijn stonden als de markt. Sommige technische specificaties waren veel te ingewikkeld en hun implementatie was niet toepasbaar voor een groot deel van de ondernemingen in dit gebied. Ervaring heeft geleerd dat juridische regelgeving nooit de rol van standaardisatie mag overnemen. Standaardisatie moet zich richten op functionele vereisten en het beschrijven van een *state-of-the-art* oplossing voor een bepaald probleem. Per definitie zijn standaarden vrijwillig en gebaseerd op een consensus tussen experts en de marktspelers. Om de veiligheidsvereisten van elektronische handtekeningen te bepalen is er geen parlement, overheid of een politiek forum nodig, maar dit proces moet gestuurd worden door technische, functionele en zakelijke overwegingen.

Bescherming van de persoonlijke levenssfeer

Artikel 22 van de Belgische Grondwet erkent het recht van eenieder op eerbiediging van zijn privéleven. Aan dit grondrecht wordt concrete uitvoering gegeven door diverse wetten. De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens concretiseert het grondrecht bij de verwerking van persoonsgegevens en bevat een aantal bepalingen betreffende informatieveiligheid. Deze wet werd in 1998 grondig aangepast om ze in overeenstemming te brengen met de Europese Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Een gecoördineerde versie van deze wet en haar uitvoeringsbesluiten is beschikbaar op http://www.privacycommission.be/normatieve_teksten.htm. Daarnaast bevatten ook een aantal specifieke wetten bepalingen op het gebied van de bescherming van de persoonlijke levenssfeer en de informatieveiligheid bij de omgang met persoonsgegevens, zoals de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen of de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid. Deze wetten blijven in dit korte bestek echter onbesproken.

De Wet Verwerking Persoonsgegevens (WVP) is van toepassing op elke bewerking en elk geheel van bewerkingen (verzamelen, bewaren, bijwerken, wijzigen, verspreiden, met elkaar in verband brengen, …) m.b.t. persoons-

gegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés. Als persoonsgegeven wordt beschouwd elke informatie (tekst, beelden, …) die in verband kan worden gebracht met een natuurlijke persoon (lees: een mens) die is geïdentificeerd of rechtstreeks of onrechtstreeks kan worden geïdentificeerd, rekening houdend met alle middelen die de verantwoordelijke voor de verwerking of enig ander persoon daartoe redelijkerwijs kan inzetten. Het toepassingsgebied van de wet is dus zeer ruim. De verwerking van persoonsgegevens is slechts toegelaten in een beperkt aantal gevallen (artikel 5 WVP), in het bijzonder

- wanneer de betrokkene zijn ondubbelzinnige toestemming heeft verleend;
- wanneer ze noodzakelijk is voor de uitvoering van een overeenkomst of van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;
- wanneer ze noodzakelijk is om een wettelijke verplichting na te komen;
- wanneer ze noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
- wanneer ze noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbare gezag;
- wanneer ze noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of een derde, mits het belang of de fundamentele rechten en vrijheden van de betrokkene niet zwaarder doorwegen.

Voor de verwerking van gevoelige persoonsgegevens (dit zijn persoonsgegevens m.b.t. de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging of het seksuele leven), van persoonsgegevens m.b.t. de gezondheid en van gerechtelijke persoonsgegevens gelden nog striktere voorwaarden. Zij mogen slechts worden verwerkt in nog preciezer in de artikelen 6, 7 en 8 van de Wet Verwerking Persoonsgegevens omschreven omstandigheden. Indien persoonsgegevens worden verwerkt, dient de verantwoordelijke voor de verwerking een aantal verplichtingen na te leven. De verantwoordelijke voor de verwerking is de persoon die (alleen of samen met anderen) het doel en de middelen voor de verwerking van persoonsgegevens bepaalt. Vooreerst moet hij de doeleinden van de verwerking duidelijk en uitdrukkelijk omschrijven, en mag hij de persoonsgegevens enkel verwerken voor die doeleinden of voor doeleinden die daarmee verenigbaar zijn, hierbij rekening houdend met de redelijke verwachtingen van de betrokkene en de wetgeving (het zgn. doelbindingsbeginsel). Hij mag enkel persoonsgegevens verwerken die toereikend, ter zake dienend en niet overmatig zijn t.o.v. de omschreven doeleinden en de persoonsgegevens niet langer bewaren dan nodig voor de verwezenlijking van die doeleinden (het zgn. evenredigheidsbeginsel). Daarenboven moet hij ervoor zorgen dat de persoonsgegevens voldoende nauwkeurig zijn, zo nodig worden bijgewerkt of verbeterd, en worden gewist wanneer ze niet meer dienend zijn. Bij de inzameling van persoonsgegevens bij de betrokkene, of, wanneer de persoonsgegevens bij een derde worden ingezameld, bij de registratie of de mededeling van persoonsgegevens, dient de verantwoordelijke voor de verwerking de betrokkene te informeren over de doeleinden van de verwerking, de identiteit van de verantwoordelijke voor de verwerking en bepaalde van zijn rechten, tenzij de betrokkene hiervan al op de hoogte is. De verantwoordelijke voor de verwerking is echter vrijgesteld van de informatieplicht indien hij, na de persoonsgegevens te hebben ingezameld bij een derde, deze gegevens registreert met het oog op de toepassing van een wet.

Vooraleer hij een geautomatiseerde verwerking van persoonsgegevens start, dient de verantwoordelijke van de verwerking daarvan ook in principe aangifte te doen bij de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. In de aangifte dienen o.a. de doeleinden van de verwerking en de identiteit van de verantwoordelijke van de verwerking te worden vermeld. De aangiften worden door de Commissie opgenomen in een openbaar register. Een nieuwe aangifte dient te geschieden bij een wijziging van de aangegeven informatie of bij de beëindiging van de verwerking. Verwerkingen voor een aantal doeleinden die kennelijk geen gevaar inhouden voor een schending van de persoonlijke levenssfeer, zijn bij een koninklijk besluit van 13 februari 2001 vrijgesteld van een aangifte. Voor die verwerkingen dient de normaal aan te geven informatie dan wel te worden meegedeeld aan iedereen die daarom verzoekt.

De verantwoordelijke van de verwerking moet ervoor zorgen dat zijn medewerkers op de hoogte zijn van de wettelijke bepalingen betreffende bescherming van de persoonlijke levenssfeer en informatieveiligheid, moet erover waken dat zijn medewerkers enkel toegang hebben tot de persoonsgegevens die ze nodig hebben voor de uitvoering van hun opdrachten en de persoonsgegevens enkel gebruiken voor de omschreven doeleinden, en moet gepaste technische en organisatorische veiligheidsmaatregelen nemen om o.a. onrechtmatige wijzigingen, verlies of vernietiging van persoonsgegevens te voorkomen. Deze veiligheidmaatregelen moeten aangepast zijn aan enerzijds de aard van de verwerkte persoonsgegevens en de potentiële risico's, en anderzijds de stand van de techniek en kosten ervan.

Indien de verantwoordelijke voor de verwerking beroep doet op een onderaannemer die te zijnen behoeve persoonsgegevens verwerkt, dient hij een verwerker te kiezen die de nodige waarborgen biedt op het vlak van de bescherming van de persoonlijke levenssfeer en de informatieveiligheid, dient hij met deze verwerker een overeenkomst te sluiten waarin de toegelaten verwerkingen en de informatieveiligheidsmaatregelen worden beschre-

ven, en dient hij controle uit te oefenen op de correcte naleving van de overeenkomst door de onderaannemer. De verantwoordelijke voor de verwerking is aansprakelijkheid voor schade die in hoofde van de betrokken personen ontstaat door een onrechtmatige verwerking van persoonsgegevens. De niet-naleving van bepaalde verplichtingen door de verantwoordelijke voor de verwerking of de onderaannemer kan aanleiding geven tot straffen, waaronder het verbod om gedurende maximaal 2 jaar persoonsgegevens te verwerken.

Naast de verplichtingen die de verantwoordelijke voor de verwerking dient na te leven, kent de Wet Verwerking Persoonsgegevens aan de persoon waarover persoonsgegevens worden verwerkt ook een aantal rechten toe. Bovenop een algemeen recht op bescherming van zijn persoonlijke levenssfeer en het reeds hoger beschreven recht op informatie bij de inzameling, de registratie of de mededeling van persoonsgegevens, heeft de betrokkene recht op kennisname en mededeling van de persoonsgegevens die worden verwerkt, van de oorsprong van deze gegevens en van de logica van de geautomatiseerde besluitvorming; verbetering van onjuiste persoonsgegevens; verwijdering of niet-aanwending van persoonsgegevens die onvolledig of niet ter zake dienend zijn, waarvan de registratie/mededeling/bewaring verboden is of die na verloop van de toegestane duur worden bewaard; een automatische mededeling, door de verantwoordelijke van de verwerking, van verbetering of verwijderingen van persoonsgegevens aan degenen waaraan de verbeterde of verwijderde persoonsgegevens voorheen werden meegedeeld; dit recht bestaat alleen voor zover de verantwoordelijke voor de verwerking nog kennis heeft van de bestemmelingen en de mededeling niet onmogelijk blijkt of onevenredig veel moeite kost; om niet onderworpen te worden aan louter geautomatiseerde beoordelingen van bepaalde aspecten van zijn persoonlijkheid, indien deze besluiten belangrijke rechtsgevolgen inhouden of de betrokkene in aanmerkelijke mate treffen, en deze besluiten niet worden genomen in het kader van een overeenkomst of een wettelijke bepaling; verzet aan te tekenen tegen de verwerking van persoonsgegevens voor doeleinden van direct marketing, of, om zwaarwegende en gerechtvaardigde redenen, tegen de verwerking van persoonsgegevens voor andere verwerkingen dan diegene die noodzakelijk zijn voor het sluiten of uitvoeren van een overeenkomst of voor het nakomen van een wettelijke verplichting; inzage van het openbaar register van de verwerkingen; verhaal bij de voorzitter van de rechtbank van eerste aanleg in geval van schending van zijn rechten op kennisname, mededeling, verbetering, verwijdering, niet-aanwending of verzet; verhaal bij de Commissie voor de Bescherming van de Persoonlijke Levenssfeer bij schending van om het even welke bepaling van de Wet Verwerking Persoonsgegevens; verhaal bij de strafrechter in geval van schending van de strafbepalingen vervat in de Wet Verwerking Persoonsgegevens.
De Wet Verwerking Persoonsgegevens stelt tenslotte bij de Kamer van Volksvertegenwoordigers een Commissie voor de Bescherming van de Persoonlijke Levenssfeer in. De Commissie bestaat uit 8 vaste leden (waaronder een voltijdse voorzittermagistraat en voltijdse ondervoorzitter) en 8 plaatsvervangende leden, die door de Kamer worden benoemd voor een hernieuwbare termijn van 6 jaar. De Commissie ziet toe op de naleving van de Wet Verwerking Persoonsgegevens, behandelt klachten die worden ingediend in geval van schending van de wet, en verstrekt uit eigen beweging of op verzoek van de wetgevende of uitvoerende overheden adviezen en aanbevelingen betreffende iedere aangelegenheid die betrekking heeft op de toepassing van de grondbeginselen van de bescherming van de persoonlijke levenssfeer. De Commissie kan deskundigen inschakelen, onderzoeken ter plaatse uitvoeren, alle nuttige documenten opeisen en alle plaatsen betreden waar vermoedelijk werkzaamheden i.v.m. de toepassing van de wet worden verricht. De Commissie maakt jaarlijks een activiteitenverslag over aan de Kamer van Volksvertegenwoordigers. Ze doet bij de procureur des Konings aangifte van de door haar gekende misdrijven en haar voorzitter kan ieder geschil aangaande de wet en haar uitvoeringsmaatregelen aan de rechtbank van eerste aanleg voorleggen.

Specifieke regels over de bescherming van de persoonlijke levenssfeer vindt men ook in de wetgeving betreffende elektronische communicatie. Daarin staat bijvoorbeeld de verplichting tot beveiliging voor bedrijven die publieke communicatiediensten of publieke communicatienetwerken aanbieden. In dezelfde wet van 13 juni 2005 vindt men ook regels over de verwerking en het gebruik van verkeersgegevens en locatiegegevens. Dat laatste is vooral belangrijk in de context van het mobiele telefoonverkeer. Men vindt er ook bepalingen over het gebruik van "*cookies*", "*spyware*" en andere technieken waarbij dienstenverstrekkers binnendringen in de eindapparatuur van de gebruikers. De richtlijn regelt ook het verzenden van ongevraagde reclameboodschappen ("*spam*") en de opname van gegevens over abonnees en gebruikers in allerlei registers (*directory services*). Tenslotte legt deze wet ook de basis voor de zogenaamde "dataretentie": het verplicht bijhouden van identificatiegegevens, verkeersgegevens en locatiegegevens door operatoren en dienstenverstrekkers met het oog op een mogelijk opvragen door de gerechtelijke autoriteiten. Deze verplichting is verder in detail geregeld in een Koninklijk besluit.

Rol van het recht op het gebied van informatiebeveiliging

Informatiebeveiliging kan niet louter door wetgeving geregeld worden. Wetgeving verloopt traag en kan niet snel inspelen op snel wijzigende omgevingsfactoren. Bovendien moet wetgeving zorgen voor stabiliteit en rechtszeker-

heid. Wetgeving die om de haverklap verandert, leidt tot onzekerheid. Burgers en bedrijven verliezen dan houvast om hun toekomstige gedragingen en strategieën te bepalen. Daarom bevat wetgeving idealiter enkel algemene principes die technologieneutraal zijn en daarom ook toepasselijk blijven wanneer omgevingsfactoren veranderen. De manier waarop de door de wetgever opgelegde algemene gedragslijnen in concrete situaties worden ingevuld, wordt best overgelaten aan de betrokkenen zelf. Zo bepaalde de Europese richtlijn over de verwerking van persoonsgegevens dat de verantwoordelijke voor de verwerking moet zorgen voor "adequate" beveiligingsmaatregelen die aangepast zijn aan de stand van de techniek, de aard van de gegevens en de potentiële risico's. De wetgever bepaalt niet zelf wat onder "adequaat" moet worden verstaan. Indien daarover een betwisting rijst, zal de rechter een beroep doen op een deskundige om te bepalen of in de gegeven omstandigheden de genomen **beveiligingsmaatregelen** adequaat genoeg waren. De expert zal daarvoor vaak teruggrijpen naar standaarden of technische specificaties die door de sector als de "*state-of-the-art*" worden beschouwd. De overheid heeft er dan ook meestal belang bij dat in alle domeinen algemeen *aanvaarde standaarden* tot stand komen. Daarom werken overheden standaardisatie in de hand via de oprichting van standaardisatie-instituten (bijvoorbeeld het Belgisch Instituut voor Normalisatie (BIN), de medewerking aan Europese en internationale standaardisatieorganisaties (CEN, ETSI, ISO, ITU-S, …) of via de officiële "erkenning" van standaarden. Om dezelfde en andere redenen creëren nationale overheden ook een kader waarin bedrijven op voorhand kunnen laten controleren of hun producten en diensten aan bepaalde standaarden voldoen. De controle zelf wordt dan door de overheid aan erkende experts overgelaten maar als het resultaat positief is, wordt dan vervolgens door de overheid een attest uitgereikt. Meestal is een dergelijke accreditatieprocedure niet verplicht. Bedrijven doen er vooral beroep op om zich beter te positioneren op de markt.

4. TOEPASSINGSDOMEINEN

Dit hoofdstuk heeft als doel om de rol en de impact van informatiebeveiliging in een aantal toepassingsdomeinen toe te lichten. De "informatie" of de "gegevens" zijn de voornaamste componenten gedurende de gehele levenscyclus van toepassingen. Naast het feit dat de informatie meerdere vormen kan aannemen, kan deze ook diverse beveiligingsnoden hebben gedurende de diverse stadia van de levenscyclus (creatie, verzending, opslag, enz.). Bijgevolg is de toegangscontrole tot de informatie een cruciale eigenschap naast de integriteit en de vertrouwelijkheid van de gegevens.

4.1 Overheid

Ook de overheid doet steeds meer beroep op de mogelijkheden van de moderne techniek om haar interne werking en haar dienstverlening aan burgers en ondernemingen te verbeteren. Dat wordt e-Overheid of e-Government genoemd. Bedrijfsprocessen in de onderscheiden overheidsdiensten, tussen overheidsdiensten onderling en tussen overheidsdiensten enerzijds en de burgers en ondernemingen anderzijds worden daarbij grondig herdacht en geïnformatiseerd. Voorbeelden hiervan zijn de elektronische aangiften aan de sociale zekerheid en aan de belastingadministratie. Het doel van e-overheid is een effectieve, efficiënte, snelle en juiste dienstverlening aan burgers en ondernemingen, die hen op een geïntegreerde wijze wordt aangeboden volgens hun leefwereld, en met een minimum aan administratieve formaliteiten. Het succes van e-overheid is in belangrijke mate afhankelijk van het vertrouwen dat alle betrokkenen terecht kunnen hebben in de beveiliging van de gebruikte informatiesystemen en in de nodige maatregelen ter bescherming van de persoonlijke levenssfeer. Indien de systemen niet vertrouwd worden, zullen ze door de burgers, de ondernemingen en het overheidspersoneel niet worden gebruikt. Een globaal, overheidsdienstoverkoepelend informatieveiligheidsbeleid, dat de beschikbaarheid, de integriteit en de vertrouwelijkheid van de verwerkte informatie afdoende waarborgt, is dan ook van groot belang. Dat beleid moet gestalte worden gegeven door een geïntegreerd geheel van maatregelen op structureel, organisatorisch, personeels- en technisch vlak. Binnen de onderscheiden overheidsniveaus en –sectoren wordt daar terecht steeds meer aandacht aan besteed. De personeels- en technische maatregelen zijn vrij gelijklopend met deze genomen in andere sectoren en komen elders in dit document aan bod. Specifiek aan de overheidssector zijn een aantal structurele en organisatorische maatregelen.

De *Belgische overheid* heeft er resoluut voor gekozen om geen massieve centrale gegevensbanken op te richten met uitgebreide informatie over alle burgers of ondernemingen. De informatie wordt gedistribueerd opgeslagen volgens een taakverdeling tussen de onderscheiden overheidsdiensten. Tussen de overheidsdiensten is afgesproken wie welke informatie beheert en over de kwaliteit ervan waakt. Meervoudige opslag van dezelfde informatie, die bijkomende veiligheidsrisico's inhoudt, wordt maximaal vermeden. Binnen de overheid zijn aldus "authentieke informatiebronnen" ingesteld, waarin bepaalde informatie op een kwaliteitsvolle wijze beschikbaar is en die op een gecontroleerde wijze toegankelijk zijn voor instanties die daartoe gemachtigd zijn. Voorbeelden van dergelijke authentieke informatiebronnen zijn het Rijksregister (identificatiegegevens m.b.t. natuurlijke personen die in België

verblijven), de Kruispuntbank van de Sociale Zekerheid (identificatiegegevens m.b.t. natuurlijke personen die in het buitenland verblijven, maar in de Belgische overheid gekend zijn, en informatie over het socialezekerheidsstatuut van de burgers), de Kruispuntbank van de Ondernemingen (identificatiegegevens m.b.t. ondernemingen) en de Rijksdienst voor Sociale Zekerheid (loon- en arbeidstijdgegevens van werknemers). De onderlinge elektronische uitwisseling van persoonsgegevens tussen de overheidsdiensten is strikt gereglementeerd. De elektronische mededelingen van persoonsgegevens door federale overheidsdiensten en instellingen van sociale zekerheid zijn in principe onderworpen aan een voorafgaande machtiging van een onafhankelijk sectoraal comité, benoemd door het Parlement, en ingesteld in de schoot van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. De machtiging wordt slechts verleend nadat is vastgesteld dat de mededeling van de persoonsgegevens geschiedt op een veilige wijze en in overeenstemming is met de principes van de reglementering betreffende de bescherming van de persoonlijke levenssfeer, zoals het doelbindings- of evenredigheidsbeginsel. De machtigingen tot mededeling van persoonsgegevens worden gepubliceerd op de website van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer en in het jaarverslag van de sectorale comités. De sectorale comités werken minimale informatieveiligheidsnormen uit, die alle instanties die mededeling verkrijgen van persoonsgegevens dienen na te leven, en ondervragen de betrokken instanties regelmatig over de concrete naleving van deze normen. Om te waarborgen dat de concrete elektronische mededelingen van persoonsgegevens tussen overheidsdiensten in overeenstemming zijn met de verstrekte machtigingen, verlopen deze mededelingen via overheidsdiensten die onafhankelijk zijn van de verzender en de bestemmeling van de persoonsgegevens, en die de overeenstemming met de machtigingen nagaan vooraleer de persoonsgegevens aan de bestemmeling mee te delen. Voorbeelden van dergelijke instellingen zijn de Kruispuntbank van de Sociale Zekerheid in de sociale sector en de Federale Overheidsdienst Informatie- en Communicatietechnologie (FEDICT) in de federale overheid. Elke elektronische uitwisseling van persoonsgegevens wordt door deze instellingen gelogd om ieder eventueel oneigenlijk gebruik achteraf te kunnen traceren. Geleidelijk aan wordt, in navolging van de initiatieven die ter zake al begin van de jaren ’90 werden genomen in de sociale zekerheid, aan alle overheidsdiensten de verplichting opgelegd om over een informatieveiligheidsdienst te beschikken. Deze dienst dient rechtstreeks te rapporteren aan de algemene bestuurder van de betrokken overheidsdienst, en heeft een adviserende, stimulerende, documenterende en intern auditerende taak op het gebied van informatieveiligheid. Hij dient m.b.t. de informatieveiligheid een jaarlijks bijgewerkt meerjarenplan uit te werken en een jaarverslag op te stellen. De informatieveiligheidsdiensten worden geleid door informatieveiligheidsconsulenten, die in daartoe opgerichte organen samenkomen om gemeenschappelijke *policies* en richtlijnen uit te werken. De informatieveiligheidsdiensten van de onderscheiden overheidsdiensten worden ondersteund door één of meer gemeenschappelijke, door de Regering erkende gespecialiseerde informatieveiligheidsdiensten. In overeenstemming met de reglementering betreffende de bescherming van de persoonlijke levenssfeer, mogen de persoonsgegevens die door de overheid worden ingezameld, enkel worden gebruikt voor doeleinden die verenigbaar zijn met de doeleinden waarvoor ze zijn ingezameld, en mogen ze slechts toegankelijk zijn voor daartoe gemachtigde gebruikers in functie van hun wettelijke en reglementaire opdrachten. Telkens de informatie gebruikt wordt voor een beslissing, dient aan de betrokkene de gebruikte informatie meegedeeld te worden tegelijk met de mededeling van de beslissing, zodat hij de juistheid ervan kan nagaan. Daarenboven heeft elke burger of onderneming een recht op toegang en op verbetering van zijn eigen persoonsgegevens. Een meer gedetailleerd overzicht van het informatieveiligheidsbeleid van de overheid en de in uitvoering daarvan genomen maatregelen kan worden gevonden in [2].

Het concept van de informatiebeveiliging is tijdens het laatste decennium geëvolueerd binnen de **defensiegemeenschap**, dankzij 2 hoofdfactoren. De eerste is de introductie van een nieuw concept het “*Network Centric Warfare*” of “*Network-Centric Operations*”. De tweede is het gevolg van het feit dat het leger met traditionele operaties niet langer oog in oog staat met georganiseerde legers, maar meer en meer betrokken wordt in gevechten tegen multinationale terroristische organisaties. Er is geen duidelijke demarcatielijn tussen nationale defensie en nationale veiligheid. Desondanks zijn sommige veiligheidsgebieden typisch voor de militaire gemeenschap. *Network Centric Warfare* is een nieuw concept van militaire operaties, gebaseerd op globale, geïnterconnecteerde, *end-to-end* informatienetwerken. Het omvat technieken, processen en personeel voor het verzamelen, verwerken, bewaren, verspreiden en beheren van informatie, nodig voor oorlogsvoerders, beleidsmakers en ondersteunend personeel. Defensiemachten moeten de mogelijkheden hebben om hun eigen veiligheid uit te bouwen en met beveiligde, betrouwbare informatiesystemen te opereren, die de ruggengraat vormen voor alle huidige militaire operaties. De traditionele benadering van informatiebeveiliging werd daarom toegevoegd in een nieuw concept, “Information Assurance” (IA) genoemd. Dit werd volledig geïntegeerd in de militaire basisoperaties en wordt niet langer beschouwd als een alleenstaand proces.

“Information Assurance” gaat niet alleen over het beheren van betrouwbare, onderhoudbare en kwalitatief hoogstaande informatiesystemen. “*Information Assurance*” behandelt de toepasbaarheid van een informatiesysteem om een brede waaier van verstoringen variërend van natuurlijke rampen en ongevallen tot intentionele verstorin-

gen door vijanden of door insiders te doorstaan. Het is ook noodzakelijk dat "*Information Assurance*" in staat stelt kwaliteitscriteria te definiëren die er voor zorgen dat het informatiesysteem kan functioneren in specifieke militaire situaties. Het belastingsniveau van informatiesystemen is zeer verschillend in vredestijd, tijdens een crisissituatie of bij een oorlogsdreiging, tijdens een beperkte nucleaire oorlog of bij herstel na een aanval. Deze benadering vergt van het personeel het pro-actief detecteren van verstoringen in informatiesystemen en het snel en adequaat reageren in een crisissituatie.

De gebeurtenissen van 11 september 2001 waren een afschuwelijk bewijs dat de globale economische beweging naar meer open gemeenschappen en geliberaliseerde economieën ook bijkomende beveiligingsproblemen meebrengt. Omdat de terroristische organisaties zich niets aantrekken van nationale grenzen, vereist de bescherming tegen internationale terreur een internationaal gecoördineerde aanpak van de veiligheid. Dit vereist een grote verandering in de manier waarop nationale veiligheid beheerd moet worden. Veel meer dan technologie, vereist het een cultuurverandering. Nationale beveiliging steunt nu volledig op een gemeenschappelijke benadering van de veiligheid. Grenscontrole is een belangrijk deel in de collectieve defensie van de EU tegen terrorisme. Het stoppen van terroristische bedreigingen aan de grens is beter dan ze te behandelen binnen de EU. Sommige lidstaten in Europa hebben geen fysieke grenzen meer om te verdedigen, behalve hun luchthavens. Desondanks worden ze beïnvloed door de efficiëntie van deze grenscontroles. Betere controles aan de grens houden ook langere wachttijden voor de mensen en goederen in om de Europese Unie binnen te komen. Om de gevolgen van deze controles te verlichten en hun efficiëntie te verbeteren, moeten de grenscontroles minder steunen op personeel maar meer op informatiesystemen. De introductie van globaal beheerde digitale identificatiesystemen en beveiligde logistieke bevoorradingsketens zal de EU-landen helpen om hun nationale veiligheid te verbeteren. Naast de gecontroleerde toegangspunten naar de Europese Unie (havens, luchthavens, wegen, spoorwegen) moet ze in staat zijn om duizenden kilometers van onbewaakte natuurlijke grenzen (stranden, bossen en bergen) te bewaken omdat een goede beveiliging niet stopt aan de voordeur.

Verkiezingen behoren tot de belangrijke activiteiten, die de overheid in democratieën organiseert. Er kunnen veel argumenten gegeven worden voor het **elektronisch stemmen** (*e-voting*) zowel aan informatietechnologiezijde als voor het kiesproces: het vermindert de verkiezingskosten, en verlaagt de drempel voor democratische deelname op elk niveau. Aan de andere kant, zouden we bewust moeten zijn van de vele "*checks*" en "*balances*" die ontwikkeld werden in het klassieke fysische kiessysteem en de beperkingen van onze huidige IT-infrastructuur. Elektronisch stemmen opent de deur naar fraude op grote schaal. Daarom moet elektronisch stemmen geleidelijk aan geïntroduceerd worden met speciale aandacht voor de specifieke beperkingen. Elk kiessysteem zou volgende elementen in overweging moeten nemen:

- registratie van het stemmen: elke kiezer stemt één keer;
- privacy van de kiezer: niemand weet hoe de kiezer gestemd heeft, zelfs als de kiezer er toe gedwongen wordt of het zelf wil, krijgt hij geen ontvangstbewijs dat hij aan derden kan tonen;
- integriteit: stemmen kunnen niet veranderd, toegevoegd of verwijderd worden. Een nauwkeurige telling, zowel lokaal als centraal die door derden gemakkelijk geverifieerd kan worden;
- beschikbaarheid: het stemsysteem is operationeel voor gebruik telkens wanneer nodig is;
- gebruiksvriendelijkheid – ook voor mindervaliden.

Het is erg belangrijk om het fundamentele verschil tussen twee scenario's voor ogen te houden, namelijk:

- het *elektronisch stemmen in een stemhokje* – deze technologie werd geïntroduceerd in België in het begin van de jaren 1990 en is sindsdien courant gebruikt. De hoofdbekommernis is de integriteit van het stem- en telmechanisme en in het bijzonder het verifiëren van het tellen te garanderen.
- *Kiezen via het internet* – dit vereist veilige eindpunten, is niet triviaal en brengt specifieke problemen met zich mee, nl. de privacy en de integriteit van het proces. Het is ook niet evident om de mogelijkheid uit te sluiten dat er gestemd wordt onder druk.

Over de jaren heen heeft de onderzoekswereld geavanceerde technologische oplossingen ontwikkeld die het "*state-of-the-art*" verbeteren door het verminderen van het aantal, dat beschermd moeten worden (vb. door het verdelen van vertrouwen over verschillende entiteiten en door universele verifieerbaarheid, wat inhoudt dat iedereen kan nagaan dat zijn of haar stem wel degelijk in rekening gebracht is). Over heel de wereld is men aan het terugkeren van de DRE (*Direct Recording Equipment*), waarbij de stem rechtstreeks bewaard wordt op de harde schijf van een computer; er is een brede consensus dat men de integriteit van de stemmachine moet kunnen checken aan de hand van een *audittrail* of papier. Daarnaast brengen deze machines bijkomende privacyrisico's mee. Een belangrijke vraag is hoe de elektronische kiessystemen op elk gebied kunnen gecertificeerd worden: architectuur, software en hardware. Dit vereist specifieke expertise: het publiek en dus verifieerbaar maken van de bronsoftware is één element, maar dit is niet genoeg. Een specifiek probleem is de authenticiteit nl. hoe kan men er zeker

van zijn dat het systeem dat men gebruikt wel degelijk het systeem is dat gecertificeerd werd. Zoals de informatietechnologie evolueert, veranderen de bedreigingen op deze systemen ook. Bijvoorbeeld vormen de introductie en de verspreiding van kleine digitale camera's een inbreuk op de privacy van de kiezer, zelfs in het klassieke stemmen op papier.

4.2 Kritische informatie-infrastructuur

Critical infrastructures (CI) worden gedefinieerd als die materiële *assets* die levensnoodzakelijk zijn voor de normale werking van een gemeenschap als een geheel en voor de economie in het bijzonder. Enkele voorbeelden van dergelijke kritische infrastructuren zijn systemen voor energievoorziening (gas, elektriciteit, brandstof), nutsvoorzieningen (water, afval), telecommunicatie (telefoon, fax, internet), transport (spoorweg, wegen), voedselvoorzieningen (bewaring, verdeling), burgerlijke administratie (overheidsfuncties), [4]. Deze kritische infrastructuren steunen steeds meer op een informatiestructuur van standaard ICT-componenten voor een correcte en efficiënte werking.

Zo wordt bij de *elektriciteitsvoorziening* steeds meer ICT gebruikt voor de planning (selectie van generatoren voor productie, berekening van knelpunten, onderhoud), operationele taken (monitoring, controle, beheer van incidenten), financiële taken (facturatie, marktwerking) en andere aspecten (klantrelaties, public relations). Door deze koppeling wordt de informatie-infrastructuur een essentiële component van de kritische infrastructuur. Ook het fysische niveau van informatie-infrastructuur en elektrische infrastructuur zijn nauw verbonden: naast transmissie- en distributielijnen voor elektrische energie plaatst men een optische kabel voor datacommunicatie, monitoring en controle. Zo worden de ICT-componenten gepromoot tot een *kritische* informatie-infrastructuur (CII) waarvan de functionaliteit bewaard moet blijven ondanks fouten die ICT-componenten treffen: fysische fouten (netwerken of computers die uitvallen), ontwerpfouten (foutief geconfigureerde servers), operationele fouten (operators die per ongeluk bestanden verwijderen) en kwaadaardige fouten (virussen, wormen en cyberaanvallen). Als de CII niet correct werkt, dan faalt de CI in zijn dienstverlening aan de gemeenschap, met als resultaat elektriciteitspannes, spoorwegproblemen en verkeersopstoppingen, problemen met de voedselbevoorrading, onbeschikbaarheid van communicatiediensten, enz. De kritische infrastructuur is dus afhankelijk van de onderliggende ICT-infrastructuur en omgekeerd; ze zijn *interdependent* [7].

Een falende informatie-infrastructuur heeft in het recente verleden al een aantal kritische infrastructuren getroffen. We geven enkele voorbeelden ter illustratie. *Software-upgrades* maakten financiële (bank)diensten onmogelijk; een ontevreden ex-werknemer in Australië belde in op een beheerssysteem van afvalwater en liet miljoenen liter rioolwater vrij in de open natuur; de "*Slammer*" worm infiltreerde een niet *gepatchte databaseserver* in het controlecentrum van een elektriciteitscentrale via een virtueel private netwerkverbinding en blokkeerde hiermee het SCADA-verkeer, wat resulteerde in een suboptimale elektriciteitsproductie; door communicatieproblemen reageerde een operator ondoelmatig op dringende elektriciteitsproblemen in een buurland, met als gevolg een black-out in een groot deel van Europa; hackers die de controle overnamen van een gaspijpleiding nadat ze het regel- en stuursysteem waren binnengedrongen, etc.

Het is duidelijk dat informatiebeveiliging cruciaal is voor dergelijke kritische informatie-infrastructuren, zodat ze goed beschermd zijn en kunnen omgaan met voorspelbare en niet-voorspelde problemen. In deze context hebben verschillende overheden, instellingen en organisaties programma's voor CIP/CIIP (*critical infrastructure protection / critical information infrastructure protection*) opgezet [4,5]. Naast het behandelen van de fysische beveiliging van de kritische infrastructuren, hebben al deze programma's een belangrijke component die de informatiebeveiliging behandelt. Dergelijke elementen omvatten waarschuwingssystemen (*Early Warning Systems* - EWS) voor virussen en wormen, *Computer Emergency Response Teams* (CERTs), gebruik van *back-up* communicatie-infrastructuur voor kritische diensten (zoals satelliettelefoon wanneer de normale communicatie faalt), "*business continuity planning*" na rampen (overstromingen, brand of grote IT-problemen), maar ook uitgebreide niet-technische procedures en richtlijnen (informatie naar het publiek, reactief optreden). Belgische beleidsmakers hebben al de eerste stappen gezet met EWS (viruswaarschuwingen) vanuit het BIPT (Belgisch Instituut voor Post en Telecommunicatie) en de BELNET CERT, maar lopen achter op andere landen die een meer uitgebreid CIP/CIIP programma hebben, meestal geïntegreerd in de nationale beveiligingsprogramma's [4].

Vermits kritische infrastructuren niet stoppen aan de grens van een land (elektriciteitstransmissie, gaspijpleidingen, wegen, telecomsystemen …), moet de beveiliging ervan op een internationaal niveau worden georganiseerd. In deze context heeft de Europese Commissie in 2005 een "*Green Paper on European Programme for Critical Infrastructure Protection*" [6] uitgegeven. Ook de Algemene Vergadering van de Verenigde Naties heeft een reso-

lutie aangenomen (58/99, Jan. 2000) om de "*Creation of a global culture of cyber security and the protection of critical information infrastructures*" [8] te stimuleren. Deze bevat 11 principes ter bescherming van CII.

- Richt waarschuwingsnetwerken op over cyberkwetsbaarheden, bedreigingen en ongelukken gerelateerd aan informatiesystemen.
- Informeer betrokken partijen zodat ze de functie van kritische infrastructuren beter begrijpen en laat ze de rol beseffen die ze moeten spelen in de bescherming ervan.
- Onderzoek infrastructuren en identificeer hun onderlinge afhankelijkheden, om ze hierdoor beter te beschermen.
- Promoot samenwerking tussen de betrokken partijen, zowel privé als openbaar, om informatie over kritische infrastructuren met elkaar te delen en gezamenlijk te analyseren om zo misbruiken te voorkomen, te onderzoeken en te reageren op aanvallen tegen deze infrastructuren.
- Creëer en onderhoud noodcommunicatienetwerken en test ze om zeker te zijn dat ze veilig en stabiel zijn in crisissituaties.
- Zorg ervoor dat het beleid om allerlei gegevens voor derden ter beschikking te stellen niet conflicteert met de noodzaak om kritische informatie-infrastructuren te beschermen.
- Vergemakkelijk het traceren van aanvallen op kritische informatiestructuren en sluit overeenkomsten af met andere landen voor het uitwisselen van dergelijke informatie.
- Organiseer trainingen en oefeningen om de responsiecapaciteiten te verbeteren en om de continuïteit en noodplannen te testen bij een aanval op de informatie-infrastructuur en spoor betrokken partijen aan tot dezelfde acties.
- Beschik over aangepaste wetten, procedures en opgeleid personeel om aanvallen op kritische informatie-infrastructuren te verhinderen en zo nodig opsporingen met andere lidstaten te coördineren.
- Zet internationale samenwerking op voor de beveiliging van de kritische informatie-infrastructuren, met inbegrip van het ontwikkelen en coördineren van waarschuwingssystemen, het delen en analyseren van informatie over kwetsbaarheden, dreigingen en incidenten.
- Promoot nationaal en international onderzoek en ontwikkeling en stimuleer het toepassen van beveiligingstechnologie die de internationale standaarden volgt.

Samenvattend kan men stellen dat, om de kritische infrastructuren van een maatschappij goed te laten functioneren ondanks de bedreigingen tegen de onderliggende informatie-infrastructuren, het ganse scala aan informatiebeveiligingstechnieken noodzakelijk is: van informatieverspreiding en foutpreventie tot foutbestendigheid en trendanalyse; dit alles gebaseerd op een continue risicoanalyse

4.3 Banken en Financiële Instellingen

Reeds een lange tijd geleden hebben banken en financiële instellingen begrepen dat het vertrouwen van de klanten afhangt van hoe goed ze de persoonlijke, zakelijke en rekeninginformatie beveiligen. Omdat informatie en ondersteunende systemen belangrijke zakelijke belangen vertegenwoordigen, zijn hun beschikbaarheid, integriteit en vertrouwelijkheid essentieel in het behouden van het imago van het bedrijf en zijn naleving van de wetten, maar ook voor zijn competitieve kant, nl. zijn cashflow en winst. Daarom is het controleren van informatie en ondersteunende systemen een constante prioriteit van de financiële sector. Hiervoor moet de informatiebeveiliging beheerd worden op een goed geïnformeerde manier en moeten "*best practices*" gevolgd worden op gebied van planning, ontwikkeling, installatie, werking en onderhoud van informatiesystemen. Dit is een ingewikkelde, en veeleisende taak. Het is des te uitdagender omdat er rekening moet gehouden worden met de verschillende facetten van de banken in de huidige dynamische omgeving, zoals:

- stijgend vertrouwen in IT-gebaseerde informatiesystemen;
- de groeiende kwetsbaarheid van computer- en communicatienetwerken;
- grotere samenwerking en gemeenschappelijk beheer van informatie;
- stijgend gebruik van externe netwerken, zoals het internet;
- snelle veranderingen in technologie;
- vraag naar grotere en nieuwere functionaliteit;
- globale competitie.

Om dit te kunnen aanpakken, definiëren banken en financiële instellingen duidelijke veiligheidsprincipes en -controles waaraan ze zich moeten houden, om zichzelf tegen interne en externe bedreigingen te beschermen, met inbegrip van de inherente kwetsbaarheid en risico's van externe verbindingen zoals het internet. Ze gebruiken industrieel aanvaarde veiligheidspraktijken die aangepast zijn aan de manier van zakendoen en communicatie met hun klanten. Onafhankelijk van welk kanaal de klant kiest (bv. bank, internetbankieren, telefoonbankieren), wordt

de identiteit van de klant steeds gevalideerd voor hij toegang krijgt tot zijn rekeningen. Gebaseerd op het risicoprofiel van de aangeboden diensten, werden methoden zoals officiële identiteitspapieren, userid/paswoord, hardware calculator of chipkaarten ontwikkeld voor de klanten door de financiële industrie. De banksystemen zelf gebruiken *state-of-the-art* technologieën zoals *firewalls* en encryptie om de bankgegevens en klantgegevens te beschermen. In geval van elektronisch bankieren, vereisen de banken het gebruik van een *browser*, die beveiligde verbindingen ondersteunt, om tot hun online diensten toegang te krijgen. Beveiligde *browsers* en protocollen stellen de klant in staat te communiceren met hun bank in een beschermde sessie door de encryptie van de informatie-uitwisseling tussen de bank en de klant. Om bijkomende bescherming te bieden wordt er vaak een *time-out* functie gebruikt op geselecteerde delen van de website. Deze functie logt de klant automatisch af van de online sessie na een bepaalde tijd. Dit helpt het verminderen van niet-geautoriseerde toegang tot de rekeningen van de klant.

4.4 Gezondheidszorg

De uitbouw van een gezondheidszorg die de patiënt centraal stelt en hem geïntegreerde, kwalitatief hoogstaande en continue diensten wil verstrekken die zijn veiligheid optimaal garanderen, kan aanzienlijk worden bevorderd door een goed georganiseerd elektronisch informatiebeheer en elektronische informatie-uitwisseling tussen alle betrokkenen. Tevens kan daardoor heel wat onnodig administratief werk voor de gezondheidszorgverstrekkers worden vermeden. De uitbouw van *e-health* is dan ook een belangrijke uitdaging. Meer bepaald wordt daarbij gestreefd naar

- een gestructureerde en gestandaardiseerde elektronische opslag van informatie over de patiënt, de verstrekte zorgen en de resultaten van de verstrekte zorgen;
- de terbeschikkingstelling, aan de behandelende zorgverstrekkers of -instellingen, van een gecontroleerde, goed beveiligde elektronische toegang tot relevante informatie over de patiënt, de verstrekte zorgen en de resultaten van de verstrekte zorgen, die reeds bij andere zorgverstrekkers of –instellingen beschikbaar is;
- een gestructureerde elektronische uitwisseling van zorgvoorschriften tussen zorgverstrekkers, zowel binnen als buiten zorginstellingen;
- de terbeschikkingstelling, aan de behandelende zorgverstrekkers, van informatieve elektronische richtlijnen met goede praktijken en waarschuwingen betreffende de behandeling bij diverse anthologieën;
- de beschikbaarheid van gegevens voor statistisch en epidemiologisch onderzoek.

Uiteraard moet er worden gezorgd voor de nodige waarborgen op het vlak van de informatieveiligheid en de bescherming van de persoonlijke levenssfeer (zie hoofdstuk 3). Artikel 7 van de Wet Verwerking Persoonsgegevens voorziet ter zake in bijzondere waarborgen. Zo mogen persoonsgegevens die de gezondheid betreffen slechts worden verwerkt in een beperkt aantal gevallen: mits toestemming van de betrokkene, voor doeleinden van preventieve geneeskunde of medische diagnose, voor het verstrekken van zorg of behandelingen, voor het beheer van gezondheidsdiensten, voor de toepassing van het arbeidsrecht of de sociale zekerheid, voor de bevordering en de bescherming van de volksgezondheid, … In principe mogen ze enkel worden verwerkt onder de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg (arts, tandarts, apotheker, verpleegkundige, …), die gebonden is door een beroepsgeheim. De toegang tot de gegevens moet strikt beperkt worden tot de zorgverstrekkers en -instellingen die deze persoonsinformatie nodig hebben voor de gezondheidszorgverstrekking. De patiënt en de zorgverstrekkers zijn er echter bij gebaat dat gegevens m.b.t. de verstrekte zorgen en m.b.t. de resultaten ervan in een aantal gevallen efficiënt tussen zorgverstrekkers kunnen worden uitgewisseld. Zo is het evident dat een huisarts best vlot toegang kan krijgen tot de gegevens die over een patiënt beschikbaar zijn in een ziekenhuis waar hij bepaalde onderzoeken ondergaat, of omgekeerd, dat een specialist die een patiënt behandelt, de relevante informatie over de patiënt kan raadplegen bij diens huisarts. Maar de technologie maakt veel meer mogelijk: men denke bijvoorbeeld aan toepassingen van telemonitoring (het volgen van de gezondheidstoestand van een patiënt op afstand doordat regelmatig bepaalde gezondheidsparameters worden meegedeeld) of telegeneeskunde (waarbij een behandeling van een patiënt op afstand wordt ondersteund).

Dergelijke toepassingen zijn veelbelovend, maar vereisen een goede regeling van de toegang tot de gegevens. Zo is het onaanvaardbaar dat bijvoorbeeld artsen werkend voor verzekeringsondernemingen toegang zouden kunnen krijgen tot informatie m.b.t. de gezondheid van een kandidaatlevensverzekeringnemer om het risico te beoordelen en desgevallend een verzekering te weigeren. Daarom is een wetsontwerp in de maak waarbij het sectoraal comité sociale zekerheid, opgericht binnen de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, wordt omgevormd tot een *sectoraal comité sociale zekerheid en gezondheid*. Zoals reeds 15 jaar succesvol geschiedt in de sector van de sociale zekerheid, zal dat comité voortaan ook bepalen welke soorten gezondheidsgegevens in welke omstandigheden kunnen worden overgemaakt door welke instanties aan welke andere instanties met het

oog op de zorgverstrekking, en onder welke voorwaarden op het gebied van veiligheid en bescherming van de persoonlijke levenssfeer. Wanneer het sectorale comité uitspraak doet over de uitwisseling van gezondheidsgegevens zal het zijn samengesteld uit enerzijds een aantal leden van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, en anderzijds een aantal onafhankelijke experts op het gebied van gezondheidszorg aangeduid door het Parlement. Naast het machtigen van de overmaking van persoonsinformatie m.b.t. de gezondheid, zal het sectorale comité ook worden belast met het vaststellen van de richtlijnen op het gebied van informatieveiligheid en de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsinformatie m.b.t. de gezondheid, met het verstrekken van adviezen en aanbevelingen inzake de informatieveiligheid en de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsinformatie m.b.t. de gezondheid, en met het behandelen van klachten inzake onrechtmatige inbreuken op de informatieveiligheid of de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsinformatie m.b.t. de gezondheid. Bij de concrete organisatie van de elektronische uitwisseling van persoonsinformatie m.b.t. de gezondheid dient dan te worden gewaarborgd dat enkel toegangsgerechtigde zorgverstrekkers of –instellingen effectief toegang krijgen tot die persoonsinformatie waartoe zij toegang mogen hebben in overeenstemming met de machtigingen van het sectorale comité en m.b.t. de patiënten waarover zij de betrokken persoonsinformatie nodig hebben voor de zorgverstrekking. Dit veronderstelt vooreerst de instelling van een degelijk systeem voor de verificatie van de identiteit en van de hoedanigheid van de zorgverstrekkers, en een degelijke verificatie van de identiteit van de patiënt. De elektronische identiteitskaart kan worden aangewend voor de verificatie van de identiteit, en authentieke gegevensbanken zullen informatie bevatten over wie zorgverstrekker is. Daarenboven moeten de algemene toegangsmachtigingen verleend door het sectorale comité vertaald worden in concrete toegangsautorisaties. Deze concrete toegangsautorisaties moeten aanduiden welke zorgverstrekker/zorginstelling/-toepassing in welke hoedanigheid in welke situatie toegang mag hebben tot welke soorten persoonsinformatie m.b.t. welke patiënten over welke periode. Een behandelende zorgverstrekker of -instelling weet overigens niet automatisch bij welke andere zorgverstrekkers of -instellingen relevante informatie beschikbaar is over een patiënt aan wie hij zorgen verstrekt. Zonder deze kennis weet hij ook niet waar hij deze relevante informatie elektronisch kan raadplegen. Het is dus nodig dat een *elektronisch verwijzingsrepertorium* wordt uitgebreid en permanent elektronisch ter beschikking wordt gehouden waarin per patiënt, geïdentificeerd aan de hand van zijn patiëntidentificatienummer, wordt aangegeven op welke plaatsen welke soorten elektronische informatie beschikbaar is over de patiënt, de verstrekte zorgen en de resultaten van de verstrekte zorgen, echter zonder dat de inhoudelijke gegevens centraal worden opgeslagen. Daarenboven mag een zorgverstrekker of –instelling in principe slechts toegang hebben tot persoonsinformatie m.b.t. de gezondheid van de patiënten waarmee hij een zorgrelatie heeft. Ook daartoe is een verwijzingsrepertorium met een overzicht van de zorgrelaties nodig.

Het verwijzingsrepertorium bevat enkel informatie over zorgrelaties tussen patiënten en zorgverstrekkers en -instellingen, verwijzingen naar de plaatsen waar persoonsinformatie m.b.t. de patiënten beschikbaar is en welke soorten persoonsinformatie beschikbaar zijn, en impliceert geenszins een centrale opslag van inhoudelijke persoonsinformatie m.b.t. de gezondheid. Eventueel kan het verwijzingsrepertorium via een getrapt systeem worden opgebouwd, waarbij bepaalde zorginstellingen of groepen van zorgverstrekkers de verwijzingen naar de individuele relaties tussen patiënten en zorgverstrekkers opnemen in een lokaal verwijzingsrepertorium, en het centrale verwijzingsrepertorium voor deze zorgrelaties doorverwijst naar het relevante locale verwijzingsrepertorium. Voor de elektronische uitwisseling van persoonsinformatie over de patiënten moet een gemeenschappelijk, goed beveiligd uitwisselingsplatform beschikbaar zijn. Dit uitwisselingsplatform kan gebruik maken van de bestaande netwerkinfrastructuur met *end-to-end* vercijferen van de inhoudelijke persoonsinformatie volgens het concept van een virtueel privaat netwerk. In onderlinge samenwerking tussen de overheid en de groepen van zorgverstrekkers wordt gewerkt aan de uitbouw van dergelijk *uitwisselingsplatform*, dat allicht wettelijk zal worden geregeld. De wet zal daarbij bijzondere aandacht besteden aan de rol van de beheersorganisatie van dat platform op het vlak van de veiligheid en de bescherming van de persoonlijke levenssfeer. Deze beheersorganisatie zal een proactief beleid moeten voeren betreffende het vermijden van onrechtmatige toegang tot persoonsinformatie, o.a. door een preventieve toetsing van de rechtmatigheid van de toegang tot de persoonsinformatie met de machtigingen verleend door het sectorale comité en het bijhouden en de analyse van logbestanden van de uitwisselingen van persoonsinformatie.

4.5 Media en Telecommunicatie

Hier zijn de veiligheidsvereisten en diensten van mobiele en draadloze communicatiesystemen behoorlijk verschillend van deze van vaste netwerken, omwille van de kwetsbaarheid van de draadloze verbinding tussen de gebruiker en het basisstation. Er is immers geen fysische verbinding in de vorm van een vaste telefoondraad tussen de gebruiker en de lokale verdeler, die zou kunnen gebruikt worden om de gebruiker te identificeren voor rou-

teringdoeleinden of voor de facturatie. Authenticatie door middel van cryptografische protocollen is dus noodzakelijk om indringers te verhinderen iemands identiteit te stelen en oproepen en aanrekening om te leiden. Afluisteren van de radioverbinding, opvangen van gegevens of het traceren van een gebruiker door het analyseren van de signaleringsgegevens vormen andere ernstige bedreigingen. Het *Global System for Mobile communications* (GSM) dat startte in 1982 is gesteund op een reeks van standaarden, die rekening houden met deze vereisten en die gebruik maken van een SIM (*Subscriber Identity Module*) kaart, die een veiligheidscomponent is die in een mobiele telefoon moet geplaatst worden. De beveiliging van het GSM-systeem bevat een aantal belangrijke zwakheden; deze zijn deels te wijten aan fouten in het ontwerp (zo kan de gebruiker niet nagaan of hij met een operator dan wel met een vals basisstation communiceert en is de encryptie niet voldoende veilig), maar ook ten dele aan het feit dat het systeem bijna 20 jaar oud is en dat het zeer moeilijk gebleken is om de beveiliging aan te passen. De belangrijkste beveiligingsproblemen van GSM zijn opgelost in de derde-generatiesystemen (3GSM) die nu meer en meer ingang vinden. Experts verwachten dat het zwakste punt daar de interconnectie zal zijn tussen het mobiele netwerk en het vaste internet.

Bij bedrijven en particulieren vindt men een groeiend aantal draadloze internetverbindingen (WLAN). De eerste versies hiervan waren niet of onvoldoende beveiligd (zo werden een groot aantal zwakheden aangetoond in de WEP-standaard). De meeste recente versies (WPA) bieden wel voldoende beveiliging; dit veronderstelt natuurlijk dat de gebruiker de beveiliging activeert en het systeem correct configureert, wat niet altijd even eenvoudig is. Men kan gelijkaardige evoluties verwachten bij nieuwe netwerken: om economische redenen is de beveiliging van de eerste versie meestal ondermaats.

Ook in vaste netwerken speelt beveiliging een groeiende rol, omdat netwerken meer en meer open zijn en verbindingen gedeeld worden. Gesofisticeerde eindgebruikers installeren VPN (Virtueel Private Netwerken), die een veiligheidsniveau kunnen bieden dat zelfs beter is dat van de vroegere private (leased) lijnen. Men mag ook de impact niet onderschatten van de *Peer-to-Peer* toepassingen en *Voice-over-IP*; deze brengen belangrijke nieuwe beveiligingsrisico's mee.

4.6 Automobielsector

Sinds 1960 werd veiligheid steeds belangrijker in de automobielsector. In het laatste decennium groeide het aantal *embedded* processoren van een auto constant. Men verwacht dat ICT-veiligheid en de veiligheid van *embedded* ICT-systemen één van de grootste uitdagingen wordt van deze industrie in het volgende decennium. Momenteel wordt de voornaamste veiligheidstoepassing in de auto gevormd door tekens die de bestuurder identificeren (toegangscontrole en ontstekingssleutel). Vrachtwagens hebben ook gewikkelde digitale tachografen en beheerssystemen op basis van GPS. Gebruikers verwachten niet alleen geavanceerde functies maar ook een hoge betrouwbaarheid (geen *reboots*), maar het is bekend dat veiligheid en complexiteit niet goed samen gaan. Uitdagingen die de industrie tegenkomt zijn veilige communicaties (voor hulpverlening op afstand, onderhoud en software- *upgrades*), "*Digital Rights Management*" (DRM) voor de auto-omgeving, software-integriteit (het beschermen tegen ongeauthoriseerde verandering zoals het *tunen* van de motor) en technologieën voor variabele verzekering en tolrijden. Deze technologieën zouden geen negatief effect mogen hebben op de privacy van de eindgebruiker.

5. TECHNOLOGIE

Het is bekend dat **cryptografie** – combinatie van de Griekse woorden "kryptos" en "grafos", of de wetenschap van geheimschrift – zo oud is als het schrijven zelf. Een breder gebruik van cryptografie werd geïntroduceerd samen met draadloze communicatie in het begin van de 20ste eeuw. In de jaren 1980 werd hardwarecryptografie steeds meer gebruikt op telecommunicatienetwerken voor financiële toepassingen. Vanaf de jaren 1990 groeide het belang van softwarecryptografie met de toenemende populariteit van het internet en de toename in prestaties van processors. De gemiddelde gebruiker heeft nu meerdere cryptografische bibliotheken in zijn PC, gebruikt crypto voor e-commerce en e-bankieren en heeft cryptografische functies in zijn mobieltje, zijn bankkaarten en zijn PDA.

Cryptografie is de studie van wiskundige technieken gerelateerd aan aspecten van informatiebeveiliging zoals vertrouwelijkheid en authenticatie van gegevens en entiteiten [3, p. 4]. Cryptografische technieken maakt het mogelijk de gegevens, gestuurd over open netwerken of opgeslagen in databanken te beschermen en om de gebruikers en machines op afstand te identificeren. Cryptografie lost niet het volledige probleem van de informatiebeveiliging op, maar verschuift de bescherming van gegevens naar dat van de bescherming van de sleutels. In symmetrische

cryptologie gebruiken de zender en de ontvanger dezelfde geheime sleutel die gebruikt wordt om de gegevens te beschermen; dit kan enkel gebeuren in gesloten netwerken en omgevingen. In het midden van de jaren 1970, werd de publieke-sleutelcryptografie ontdekt waarbij de gebruiker twee bij elkaar horende sleutels heeft, een publieke en een private sleutel. Om vertrouwelijke data te versturen naar een derde (*public key encryption*) heeft men enkel een geauthenticeerde kopij van de publieke sleutel van die derde nodig. Dan is de enige persoon die de boodschap kan lezen diegene die beschikt over de private sleutel die hoort bij de publieke sleutel. Omgekeerd, als iemand zijn gegevens met zijn private sleutel, transformeert, kan iedereen die een authentieke kopij heeft van de corresponderende publieke sleutel, nagaan dat deze persoon de gegevens heeft "getekend" (gekend als de *digitale handtekening*). De bescherming van een groot open systeem zoals het internet en onze kredietkaartinfrastructuur zou niet mogelijk zijn zonder publieke-sleutelcryptografie.

De grootste uitdaging in het ontplooien van een cryptografisch systeem is het maken en verdelen van de sleutels. In symmetrische systemen vereist dit een manuele interventie zoals de verdeling van PINcodes of kaarten en toestellen met geheime sleutels. In een zogenoemde PKI ("*Public Key Infrastructure*") is er een centrale partij (de "*Certification Authority*" of CA) die certificaten aanmaakt: een certificaat is een reeks bits, die een publieke sleutel linken aan een identiteit (een unieke naam). Certificaten worden digitaal getekend door CA – dat is vergelijkbaar met de handtekening van een ambtenaar die op een papieren identiteitskaart, de naam van een burger aan zijn of haar foto verbindt. Terwijl men een publieke sleutel algemeen bekend wil maken, is het erg belangrijk om de toegang tot de private sleutel te beschermen door deze veilig te bewaren in een chipkaart beschermd door een PINcode of op een harde schijf beschermd met een paswoord.

Er zijn vele internationale cryptografische standaarden, die de algoritmen en lengte van de sleutel voor een gegeven veiligheidsniveau specificeren. Het is belangrijk om publiek gespecificeerde algoritmen en algoritmen te gebruiken, waarvan de veiligheid grondig bestudeerd werd. Algoritmen die geheim zijn of "*home-grown*" geven een vals gevoel van veiligheid, maar houden heel wat risico's van lekken en onvoldoende evaluatie in en mogen dus nooit vertrouwd worden. Spijtig genoeg is de levensduur van een cryptografische sleutel beperkt: sleutels moeten vervangen worden en soms moet de sleutellengte vergroot worden (de lengte van de sleutels voor RSA zijn geëvolueerd van 512 bits naar 1024 en 2048 bits en zelfs naar 4096 bits). Het gebeurt vaak dat zwakheden in de cryptografische algoritmen ontdekt worden, wat betekent dat zowel sleutels als algoritmen vervangen dienen te worden (voorbeelden zijn DES, dat vervangen werd door *triple-DES* of AES en MD5 en recent SHA-1). Het is daarom belangrijk om efficiënte procedures op te stellen om de cryptografische sleutels te veranderen en de cryptografische algoritmen te upgraden. Bijna alle cryptografische oplossingen ontwikkeld in de laatste 15 jaar hebben technieken om de sleutels te vervangen, maar zeer weinige hebben adequate procedures om de algoritmes te *upgraden* (GSM, *Bluetooth*, SSL en een groot deel van de financiële infrastructuur).

Zoals eerder al vermeld, zijn de belangrijkste toepassingen van cryptografie het opzetten van **veilige netwerkverbindingen** voor *e-commerce* (SSL of TLS in de browser), telewerken (*Virtual Private Networks*), financiële transacties en internetbankieren en draadloze en mobiele communicatie (GSM, 3GSM, WLAN). Daarnaast wordt cryptografie gebruikt voor de **bescherming van gegevens** (authenticatie, autorisatie, privacy) op diverse plaatsen zoals in gegevensbestanden en op de harde schijf van gebruikers.

Een zeer significante evolutie die zich in de loop van de laatste tien jaar heeft voorgedaan is de almaar groter wordende populariteit van **mobiele toestellen**, zoals laptops, "*Personal Digital Assistants*" (PDA's) en "*smart phones*". Doordat werknemers op dit soort toestellen vertrouwelijke informatie begonnen op te slaan en verwerken steeg het risico op misbruik en veranderde zelfs heel de notie van wat vroeger als "*security perimeter*" aanzien werd. Die perimeter zorgde er enerzijds voor dat toestellen die gevoelige informatie opsloegen en verwerkten, indertijd vaak desktop Pc's, zich permanent in een fysiek beveiligde omgeving bevonden. Anderzijds werd het internetverkeer van en naar deze Pc's netjes afgeschermd met *firewalls* en *intrusion detection and prevention* systemen. Geen enkele van deze beide veronderstellingen houdt nog stand als men in plaats van met (immobiele) desktop Pc's, met mobiele toestellen gaat werken. Enerzijds vergroot het risico op diefstal en verlies enorm, anderzijds worden deze toestellen op ongecontroleerde of onvoldoende veilige manier met het internet gekoppeld. Als een bedrijf alsnog het "*security perimeter*" principe wil toepassen dan moet dat tegenwoordig ter hoogte van het mobiele toestel zélf gebeuren. Voorbeelden zijn legio: antivirusbeveiliging, persoonlijke *firewall*, encryptie van de harde schijf en/of bestanden, controle van de PC-poorten en I/O. Al deze toepassingen zijn er gekomen omdat het principe van de perfecte perimeter overboord moest worden gezet, en daarmee ook het al te dominante belang van enkel netwerkbeveiliging.

Een belangrijk beveiligingselement in de digitale wereld is een betrouwbare **identificatie en authenticatie** (I&A) op afstand. Het doel van I&A is na te gaan wie de gebruiker is en om te beletten dat een aanvaller zich voor iemand

anders kan uitgeven en op deze manier ongewettigd toegang kan verkrijgen tot een bepaalde dienst. Met identificatie bedoelt men meestal het verstrekken van een bepaalde identiteit (al dan niet door de gebruiker gekozen), terwijl authenticatie slaat op het bewijzen dat men inderdaad het recht heeft om deze identiteit te gebruiken. Een dergelijk bewijs bestaat meestal uit een combinatie van een of meerdere elementen:

- iets wat de gebruiker kent (paswoord of een PINcode);
- iets wat de gebruiker bezit of een *token* (een hardwaretoestel, een rekenmachine, een chipkaart zoals de Belgische Identiteitskaart of een kredietkaart);
- iets wat een eigenschap is van de gebruiker (een biometrische eigenschap zoals vingerafdruk of irisscan) of van zijn gedrag (manier van typen);
- de locatie van de gebruiker (netwerkadres, cel in mobiele communicatie).

Bij éénfactorauthenticatie wordt meestal een paswoord of identiteitsbewijs verwacht. Bij tweefactorauthenticatie vereist men twee onafhankelijke componenten zoals een chipkaart en een PINcode of een paswoord en een vingerafdruk.

De meeste bekende vorm van I&A is een gebruikersnaam gekoppeld aan een paswoord of paszin (*passphrase*). Dit vergt geen bijkomende infrastructuur wat het zeer goedkoop en efficiënt maakt. Anderzijds hebben paswoorden een belangrijk aantal zwakheden:

- gebruikers kiezen paswoorden die gemakkelijk te raden zijn; dit moet ook afgewogen worden tegen de groeiende rekenkracht van computers, die momenteel paswoorden van minder dan 10 tekens door exhaustieve methoden kunnen kraken;
- gebruikers geven hun paswoorden door aan derden;
- paswoorden zijn kwetsbaar voor fraude door insiders, zoals systeembeheerders;
- gebruikers hebben problemen bij het onthouden van te complexe of teveel paswoorden en zijn geneigd om paswoorden te hergebruiken of ze op te schrijven.

Ondanks al deze problemen blijven paswoorden zeer populair door hun lage kost. Hun gebruik is enkel aanvaardbaar als er een strikte *policy* kan worden afgedwongen en als men kan beletten dat men met een computer paswoorden kan kraken door exhaustief te zoeken (door een limiet te zetten op het aantal pogingen om een paswoord te proberen).

De belangrijkste toepassingen (zoals financiële sector en e-overheid) maken gebruik van twee-factorauthenticatie, waarbij de gebruiker zich authentiseert met de combinatie van een *token* en een PIN of paswoord. Een eerste generatie *tokens* (zoals de bankkaarten met een magnetische strip voor gebruik in bankterminals) kon enkel een geheime sleutel opslaan; zij was vrij kwetsbaar voor het *skimmen* van informatie, d.w.z. het uitlezen van de magnetische strip en de PINcode met een “valse” lezer. Momenteel gebruikt men *tokens* met een microprocessor; in dit geval is het veel moeilijker om de geheime informatie te extraheren.
De meest algemene types van “*smart tokens*” zijn:

- de chipkaarten zoals de bankkaart, de GSM SIM-kaart, de Belgische elektronische identiteitskaart en de kredietkaarten; hierbij maakt men een onderscheid tussen de kaarten met enkel symmetrische cryptografie (zoals de GSM SIM-kaart) en kaarten met een speciale coprocessor voor publieke-sleutelcryptografie;
- de rekenmachines die éénmalige paswoorden genereren zoals de *tokens* van Vasco (*Digipass*) en RSA (*SecurID*), al dan niet met een *challenge-response* functie.

Deze *tokens* zijn verschillend door hun fysische karakteristieken (kredietkaart t.o.v. rekenmachine), *interface* (manueel t.o.v. elektronisch), en de protocollen die zij implementeren (vb. statisch uitwisselen van paswoorden, dynamische paspoortgeneratoren, en “challenge-response”).

Biometrische authenticatietechnologieën gebruiken unieke karakteristieken van een individu en kunnen op die manier gebruikt worden voor twee-factor- of zelfs drie-factorauthenticatie. Er bestaat een zeer brede waaier aan oplossingen, die men kan opdelen in twee types:

- fysiologische: vingerafdruk, handgeometrie, retina of iris, DNA,…
- gedrag: stempatronen, handgeschreven handtekeningen, snelheid van typen,…

De meeste biometrische technologieën zijn meer gebruiksvriendelijk dan een paswoord en kunnen niet doorgegeven worden aan andere gebruikers. Het geboden veiligheidsniveau wordt bestudeerd aan de hand van de kans om een indringer te identificeren en aan de kans dat een rechtmatige gebruiker geweigerd wordt. In commerciële applicaties mag deze laatste kans niet te hoog zijn, wat impliceert dat een indringer een kans van een paar procent heeft om een gebruiker te impersoneren. Dit is op zichzelf niet aanvaardbaar voor de meeste toepassingen,

zodat biometrie in combinatie met andere methoden gebruikt moet worden, wat de kostprijs en complexiteit opdrijft. Biometrie heeft ook belangrijke andere nadelen: vingerafdrukken zijn niet vertrouwelijk (men laat ze overal achter) en er is nog onvoldoende inzicht in wat er zal gebeuren als een groot aantal toepassingen (laptops, reispassen, toegangscontrole van gebouwen) allemaal dezelfde vingerafdrukken zullen gaan gebruiken. Als biometrische eigenschappen gestolen worden, kan men ze niet vervangen, niet alle mensen hebben even goed onderscheidbare eigenschappen en een aantal technieken brengen belangrijke risico's mee voor de privacy van de gebruiker, vooral als er gewerkt wordt met centrale *databases*. Daarom is het aangewezen zeer voorzichtig om te springen met biometrische oplossingen en om deze te gebruiken in combinatie met geavanceerde cryptografische technieken, waarbij cryptografische sleutels op een niet-reversibele en flexibele manier worden afgeleid uit biometrische gegevens. Deze systemen zijn momenteel nog in ontwikkeling.

Naast authenticatie is ook autorisatie van belang: zo moet men kunnen nagaan welke rechten een gebruiker heeft: welke gegevens kan hij of zij raadplegen, overschrijven of verder verwerken. Het vaststellen en beheren hiervan is een vrij complex probleem.

Historisch gezien lag de nadruk in computersystemen op het authenticeren van de gebruikers; in de huidige open netwerkomgeving is het echter even belangrijk om na te gaan dat men als gebruiker wel degelijk met de juiste dienst verbonden is. In de huidige webomgeving gebeurt dit aan de hand van servercertificaten zoals hoger beschreven. Het is echter niet eenvoudig voor de gebruiker om na te gaan of hij wel degelijk met de juiste dienst verbonden is; het probleem schuilt hem niet alleen in de cryptografische certificaten, maar ook in de complexiteit van de infrastructuur en de *interface*. Dit laat de georganiseerde misdaad toe om met behulp van "*phishing*"-aanvallen de authenticatiegegevens van gebruikers te stelen en op deze manier bestaande systemen te omzeilen. Zelfs "smart *tokens*" bieden niet altijd een afdoende oplossing tegen dergelijke aanvallen. Het ontwikkelen van gebruiksvriendelijke oplossingen voor dit probleem vormt een belangrijke onderzoeksuitdaging.

Chipkaarten of "*Smart Cards*" vervullen een steeds toenemende rol in onze maatschappij. Deze draagbare en "actieve" hardware componenten zijn veilige verantwoordingsstukken die een aantal specifieke vereisten vervullen in een waaier van toepassingen en omgevingen zoals bankieren, telecom, gezondheidszorg, overheid, ... Samengevat bestaan deze uit een microcomputer en een programmeerbaar geheugen die zorgen voor een veilig beheer (opslag en bewerking) van gevoelige gegevens zoals de persoonlijke gebruikersgegevens, gebruikersprivileges, cryptografische gegevens en daarnaast ook de beveiligingsmechanismen zoals digitale handtekening en cryptografische algoritmen correct uitvoeren. Deze chipkaarten kunnen gebruikt worden voor de identificatie en authenticatie van een gebruiker als deel van een toegangscontrole tot een computersysteem en een communicatienetwerk en vice versa. Bovendien laten deze de veilige transfer toe van gegevens zoals transactiegegevens tussen de kaart en de kaartlezer.

In de laatste 20 jaar is er een indrukwekkende evolutie geweest van deze kaarten. Deze zijn gewoonlijk gemaakt in plastic en voorzien van een chip. Naargelang de eigenschappen van de chip kan de kaart gebruikt worden als een geheugenkaart met een niet-vluchtig geheugen en vrije toegang tot de informatie, of als een intelligente geheugenkaart met additionele veiligheidshardware of als een chipkaart met een programmeerbaar geheugen of ten slotte als een super chipkaart met een geïntegreerd toetsenbord. Bij intelligente geheugenkaarten en chipkaarten kunnen veiligheidsattributen voor het lezen en schrijven ingebouwd worden. Een deel van het geheugen kan publiek zijn of beschermd, of geheim zijn zodat het enkel beschikbaar is voor intern gebruik. Het beschermde deel van het geheugen is enkel toegankelijk na het aanbieden van een persoonlijk kenmerk van de gebruiker. Tegenwoordig gebruikt men hiervoor dikwijls een PINgetal (*Personal Identification Number*), dat bestaat uit een getal van 4 tot 8 cijfers; het aantal pogingen voor het ingeven van een PIN wordt beperkt. Meer recente authenticatietechnieken zijn gesteund op biometrische gegevens zoals een vingerafdruk. Naargelang de gegevens tussen de kaart en de kaartlezer kan men het onderscheid maken tussen contactkaarten en contactloze kaarten. Omwille van de migratie van oudere naar nieuwere kaarten en de overeenkomstige lezers zijn er op de markt heel wat hybride kaarten met meerdere interfaces zoals magnetische strips, contacten en contactloze.

***Digital Rights Management* (DRM)** omvat de verdeling en handel van digitale werken en informatie op elektronische infrastructuur met inbegrip van de technische, legale en commerciële aspecten. De interesse in DRM is hoofdzakelijk afkomstig van de visie dat het web de nieuwe digitale verdeelinfrastructuur zou worden voor de inhoud van werken. De omvang van de piraterij via het web heeft deze aandacht voor de beveiliging en bescherming van de inhoud sterk doen toenemen met heel wat onderzoek naar nieuwe standaarden, wetgeving, en producten in webgebaseerde DRM-technologieën. Aanvankelijk waren de voornaamste actoren in dit domein, namelijk de eigenaars van de werken, de bedrijven in de consumentenelektronica, en de consumenten zelf in bespreking over de bescherming van de digitale werken. Dit heeft dan geleid tot mediagerelateerde beschermings-

mechanismen tegen kopiëren van optische schijven zowel als conditionele toegangscontrole ter ondersteuning van betaal-TV diensten zoals Prime en Canal Plus. Echter in recente jaren is er een verschuiving van de prioriteit op te merken met bijvoorbeeld de uitwisseling van muziek en video over het web met diensten zoals Napster en Gnutella. Voorname belanghebbenden realiseren zich meer en meer dat hun bedrijfstak in gevaar is en bijgevolg dringen ze aan op een beveiligde distributie van de elektronische inhoud. Het is precies hier dat de wereld van het web en de consumentenelektronica, computers en software elkaar ontmoeten. De grotere beschikbaarheid van internet, de toename van de mobiliteit met de evolutie van alleenstaande huiscomputer naar de draagbare computer en toestellen en de daarmee gepaard gaande beschikbaarheid van massaopslag, maakt de uitwisseling van inhoud meer en meer aantrekkelijk. De snelle verbetering van de audio- en beeldcompressietechnieken MP3 en MPEG-4 vergroten de opportuniteiten voor nieuwe commerciële initiatieven in de distributie van ontspanningsproducten en tegelijk versnellen deze de nood aan bescherming.

Technisch gezien kan DRM opgevat worden als een uitbreiding van het auteursrecht namelijk bescherming tegen ongeoorloofd kopiëren. Beiden vallen echter onder verschillende statuten en regelgevingen. Voor de auteursrechten van massaverdeelde media nl. CD, TV-programma's enz., zijn de rechten van en het fair gebruik door de gebruikers duidelijk geworden in het laatste decennium; bovendien is de vorm van toegelaten praktijken bij de gebruikers redelijk goed afgelijnd. Aan de andere kant zet DRM een regeling op waarbij de consument en de eigenaar van de auteursrechten een individueel contract opzetten dat veel restrictiever gebruik kan omvatten zoals beperkingen in tijdsduur of in aantal keren afspelen. Bovendien refereert DRM vaak naar gesloten systemen. In de huidige consumentenelektronica-omgeving kunnen de vele diverse activiteiten voor de bescherming van de inhoud en DRM leiden tot een situatie, waarbij vele vaak tegenstrijdige standaarden en onnodige beperkingen de vlotte uitwisseling van gegevens tussen meerdere toestellen onmogelijk maken. Het is bijgevolg een grote uitdaging om DRM-oplossingen te ontwikkelen die toch nog de uitwisseling van de inhoud toelaten, die de gebruiker heeft verworven via schijf, media, breedband, en draadloos. Dit kan klaarblijkelijk enkel indien de betrokkenen op een intense manier samenwerken en door het ontwikkelen van open standaarden.

Op zich is het adequaat beschermen van bits tegen kopiëren zeer complex; het vergt eigenlijk een volledige controle van het opslagmedium (bijvoorbeeld de DVD) via de processor tot het scherm of de luidsprekers. Het ontwikkelen van een dergelijk systeem zou ook de controle van de gebruiker over zijn eigen gegevens kunnen bemoeilijken en de aantrekkelijkheid van de PC als een geïntegreerd gegevenssysteem verminderen. Een groot aantal DRM-systemen zijn op dit moment al gekraakt en het ziet er niet naar uit dat men snel een zeer veilig systeem kan ontwikkelen. Men kan verwachten dat de DRM-systemen zullen evolueren naar een oplossing met centrale controle, waarbij een toestel steeds online zal gaan vooraleer informatie getoond wordt; het is duidelijk dat dit belangrijke privacyproblemen kan meebrengen. Een andere mogelijkheid is de ontwikkeling naar meer *open-business* modellen, waarbij de bron van inkomsten verschuift (bijvoorbeeld naar *live events* of *merchandising*).

Om verschillende redenen is het vaak nodig dat informatie voor kortere of langere tijd wordt bijgehouden of **gearchiveerd**. In de openbare sector bestaat een algemene verplichting om alle informatie te bewaren en na tien jaar over te dragen aan het Rijksarchief. De details van deze verplichting worden geregeld in de archiefwet. Maar ook bedrijven en particulieren moeten bepaalde gegevens bewaren. Zo bepaalt de wetgeving bijvoorbeeld dat facturen gedurende zeven jaar bewaard moeten worden voor controle door de administratie van de BTW. Voor boekhoudingstukken geldt een bewaarverplichting van tien jaar. Belangrijke contracten worden gedurende minstens dertig jaar bewaard omdat pas na die tijd de verjaringstermijn verstrijkt voor eventuele betwistingen.

Meer en meer wordt informatie gearchiveerd in elektronische vorm. Dat is veel minder vanzelfsprekend dan het archiveren van papier. Elektronische informatie is per definitie vluchtig en gemakkelijk wijzigbaar zonder enig spoor achter te laten. Bovendien is voor de toegang tot elektronische informatie altijd hardware en software nodig. Die instrumenten zijn onderhevig aan een zeer snelle evolutie zodat het vaak niet zeker is of gegevens die vandaag worden opgeslagen, nog leesbaar zullen zijn met de instrumenten die binnen enkele tientallen jaren zullen worden gebruikt.

Nog moeilijker is het probleem van de onderlinge verwevenheid. In tegenstelling tot papieren documenten bevatten moderne elektronische bestanden talrijke links naar andere bestanden. Documenten bestaan niet meer op zichzelf maar zijn een onderdeel van een informatieweb. Heel vaak worden documenten onbruikbaar omdat ze volstaan met verwijzingen naar andere documenten die echter niet meer te vinden zijn.

Het is ook minder en minder evident om te beslissen wat wel en wat niet moet worden bewaard. Het gebruik van informatietechnologie vergemakkelijkt de creatie van informatie enorm en dat leidt tot een exponentiële toename. Dat is bijvoorbeeld het geval bij e-mail. Vaak wordt daarom verkozen om voor alle zekerheid toch maar alles te bewaren.

Er bestaan nog geen algemeen aanvaarde archiveringsstrategieën voor de elektronische omgeving. Instrumenten zoals de digitale handtekening maken het mogelijk de integriteit van gegevens na te gaan maar bieden natuurlijk geen bescherming tegen al dan niet accidentele wijzigingen of verlies. Bovendien blijft de "*bitstream*" bij vele archiveringsoplossingen niet intact en gaat de handtekening verloren omdat documenten worden geconverteerd en migreren naar nieuwere softwareversies of andere platformen.

Met de ontwikkeling van de informatiegemeenschap groeit de bedreiging voor onze privacy snel en dikwijls zijn de wettelijke oplossingen niet voldoende, vandaar de ontwikkelingen van **privacyverhogende technologieën**, (*privacy enhancing technologies* of PETs). Het verlies van privacy is een natuurlijk gevolg door de ontwikkeling van een online omgeving. Onze moderne communicatiemiddelen (GSM, 3GSM, GPS, internet) laten netwerkoperatoren en ISPs toe de gebruikers te lokaliseren en al hun acties te registreren; voor een groeiend aantal toepassingen worden toestellen, producten en voorwerpen voorzien van RFID (Radio *Frequency Identification*) *tags* die een uniek nummer hebben. Telefoniesystemen bewaren enkel de bestemming en de duur van de oproepen, bepaalde systemen aangesloten op het internet bewaren veel meer informatie van het internetverkeer. Als iemand informatie verkrijgt over al het internetverkeer van een bepaald IP-adres en als iemand zo kan registreren dat een bepaalde gebruiker de website http://www.unitedforpeace.org/ of http://www.digicrime.com bezoekt, brengt dit heel wat informatie over zijn of haar interesses naar boven. Informatie over de locatie is zelfs nog gevoeliger, vooral als de plaats van verschillende gebruikers kan worden gecorreleerd. Al deze informatie kan worden gecentraliseerd over snelle communicatielijnen en bewaard worden in grote databanken. Kryder's wet bepaalt dat de capaciteit van het geheugen elke 18 maanden verdubbelt. In de laatste 15 jaar is de grootte van de harde schijven met een factor 1000 verhoogd. De huidige harde schijven hebben een capaciteit van 500 Gigabyte en in 2014 zullen ze een capaciteit hebben van 64 Terabyte. Dit is voldoende om 10Kbyte voor elke inwoner in de wereld te bewaren of een lageresolutiefilm die 34 jaar duurt. Dan zou men slimme veiligheidsgerelateerde toepassingen kunnen ontwikkelen, zoals het verplicht dragen van een videocamera voor (ex-)gedetineerden om aldus hun doen en laten te registreren. Daarenboven, kunnen er technieken ontwikkeld worden om slim te zoeken en aan gegevensontginningstechnieken (*data mining*) te doen om al deze informatie toegankelijk te maken met een muisklik. Dit onderzoek wordt verder vergemakkelijkt door het succes van XML en metadata. Iedereen kent voorbeelden van onverwachte informatie die naar boven komt bij het zoeken op internet. Als deze technologie ons gebruiksgemak verhoogt of een interessante toepassing aanbiedt, zijn we als individuen geneigd de bijkomende risico's te aanvaarden, zelfs als we niet altijd de implicaties voor de gemeenschap als een geheel begrijpen. Onderzoekers hebben de afgelopen 25 jaar gewerkt aan technologieën die de privacy beschermen (onder de naam PETs of *Privacy Enhancing Technologies*). Dit omvat encryptietechnieken, pseudoniemen en anonieme *credentials*, mixnetwerken, privacyrichtlijnen en talen voor het beschrijven van privacyvereisten. Anonieme credentials leveren het bewijs dat iemand (hij of zij) lid is van een bepaalde dienst of in een bepaalde gemeente woont, zonder zijn naam vrij te geven (behalve wanneer er een vermoeden van fraude is). Mixnetwerken coderen en mengen pakketten zodat het traceren van de bron erg moeilijk wordt. Helaas is het ontwikkelen van deze technologieën in de praktijk ingewikkeld en duur. Daarnaast zijn er ook juridische beperkingen op het gebruik er van. Deze diensten zijn daarom slechts in beperkte mate beschikbaar en de *overhead* (communicatietijd en computerkosten) voor een goede privacybescherming is erg groot. Hier past de overweging dat de publieke-sleutelcryptografie te duur was in de jaren 1980 (behalve voor specifieke hardware), terwijl ze nu algemeen gebruikt wordt in elke PC. We hopen dat verdere vooruitgang in onderzoek en in computerkracht deze technologie beschikbaar zal maken voor elke burger en het geleidelijk mogelijk zal maken om onze privacy terug te winnen. Een belangrijke vereiste is dat deze systemen conditioneel kunnen gemaakt worden, dit betekent dat in een specifieke situatie (het ontdekken van fraude of een gerechtelijke onderzoek) de anonimiteit kan doorbroken worden, zonder de bescherming van de rest van de gemeenschap te schaden.

In het jaar 1999 hebben een aantal grote ICT bedrijven (Compaq, HP, IBM, Intel en Microsoft) de TCPA (***Trusted Computing Platform Alliance***) opgericht. Het doel van TCPA was het ontwikkelen van specifieke hardware voor de beveiliging van de PC van de toekomst. Deze specificaties moesten zorgen voor meer integriteit van de configuratie, isolatie van processen en bescherming van gegevens aan de hand van een kleine uitbreiding van de hardware van de massamarkt-PC. In 2003 werd TCPA omgevormd tot TCG ("*Trusted Computing Group*"). Deze groep bouwt verder op de specificaties en heeft het bereik ervan uitgebreid naar mobiele toestellen, netwerken, opslag, enz. Eén van de belangrijkste specificaties van TCG is TPM ("*Trusted Platform Module*"). TPM is een microchip die vergelijkbaar is met een chipkaart, die op het moederbord van de PC wordt toegevoegd en gebruikt wordt om cryptografische operaties uit te voeren. Betrouwbare *computing* gaat over het inbouwen van integriteit in de PC vanaf het moment van opstarten. Enkele typische scenario's zijn het beschermen van gevoelige data die bewaard worden op de PC, het ondersteunen van cryptografische processen van het beheerssysteem en het beschermen van de integriteit van de PC. De éérste twee scenario's zijn echt voor de hand liggend. Beheerssystemen gebruiken de TPM voor cryptografische bewerkingen of om alle cryptografische sleutels van het beheerssysteem te bescher-

men. Het laatste scenario beschermt de integriteit van het "*boot sequence*" of opstartsequentie van het *operating* systeem en verschaft bijkomende bulk-encryptie.

Om het nut van deze scenario's te verduidelijken beschrijven we wat er kan gebeuren met een laptop van een bedrijf. Deze laptop wordt gebruikt voor belangrijke taken in het bedrijf en moet dus veilig zijn. De gebruiker kan de laptop mee naar huis nemen en er onbetrouwbare software binnenhalen. Dit kan het hele beveiligingssysteem van de laptop in gevaar brengen, met inbegrip van de werkomgeving die via het netwerk kan aangetast worden. Als we denken aan meerdere omgevingen kunnen we beperkingen aanbrengen op één PC, zodat één omgeving volledig geïsoleerd is van de andere omgeving (beschermd door hardware en TPM). In dit geval beïnvloedt een geïnfecteerde omgeving de werkomgeving niet.

Er is veel kritiek op *trusted computing*, hoofdzakelijk omdat het beschouwd werd als een hulpmiddel om meer controle te krijgen over illegale software, over audio en video via het implementeren van DRM technologie of als een "*Big Brother*". Voor vele bedrijfstoepassingen is *trusted computing* echter een hele grote stap voorwaarts naar het bouwen van een veiliger PC-omgeving. De industrie loopt nog altijd achter door het gebrek van veiligheid in de jaren 1980 en 1990. Het succes van het internet en de daarbijhorende veiligheidsrisico's hebben de industrie verrast. Het zou spijtig zijn als deze onveiligheid zou bestendigd of vergroot worden in de volgende golf van computertoepassingen. Klanten en de zakenwereld betrouwen meer en meer op de computer om veilig kritische operaties uit te voeren zoals e-bankieren, *e-government, e-voting, e-business* enz. We moeten meer veiligheid inbouwen in de hardware van de massamarkt-PC en de beheerssystemen om de toekomstige veiligheidsbedreigingen het hoofd te kunnen bieden. Het hoofddoel van *trusted computing* is het ontwikkelen van een veiliger PC-platform. Ook de *open source* gemeenschap (Linux) draagt actief bij tot deze ontwikkeling. In deze context wordt ook een groeiende aandacht vastgesteld voor virtualisatietechnieken, die het mogelijk maken verschillende processen of applicaties op één enkele machine te laten draaien zonder dat ze met elkaar interfereren.

De Gartner Group definieert **Web Services** als volgt *"een software component die een zakelijke functie (of zakelijke dienst) levert en die toegankelijk is voor andere toepassingen (een klant, server of een andere Web dienst) over publieke netwerken, met gebruik van alomtegenwoordige protocollen en transport"*. Web Services beïnvloeden de manier waarop software ontwikkeld wordt. Veiligheid en open standaarden zijn sleutelelementen in het succes van Webdiensten. Om ten volle kunnen genieten van het potentieel van Webdiensten, moet de veiligheid versterkt en gecontroleerd worden en moeten de verschillende technologieën volledig interoperabel zijn. Interoperabiliteit wordt gerealiseerd in nauwe samenwerking met de industrie, met als resultaat "*web services architectures*" (inclusief veiligheidsspecificaties) en open standaarden. De industrie heeft ook een organisatie WS-I opgericht. De organisatie is verantwoordelijk voor het controleren van de interoperabiliteit tussen de verschillende partijen. Webdiensten worden beschreven door open interfaces in XML. Webdiensten zijn een goed voorbeeld om aan te tonen hoe de industrie de veiligheid toepast. Terugkijkend in de tijd naar de grote ontwikkelingen van de technologie, stelt men in de meeste gevallen vast dat de veiligheid pas in een later stadium werd toegevoegd. Het IP (Internet Protocol) kan als voorbeeld genomen worden; hiervoor werd beveiliging slechts in het midden van de jaren 1990 toegevoegd. In het geval van Webdiensten, werd de veiligheid vanaf de eerste dag voorzien onder de vorm van een aantal WS-vereisten. De belangrijkste specificaties zijn:

1. WS-veiligheid – encryptie en integriteitsbescherming van boodschappen;
2. WS-vertrouwen – bouw vertrouwde modellen en interoperabiliteit tussen verschillende beveiligingsmodellen (e.g. Kerberos en PKI);
3. WS-veilige conversatie – uitwisselen van het sleutelmechanisme voor Webdiensten;
4. WS-Privacy – Privacy regels van Webdiensten;
5. WS-Beleid – Beleidsregels voor Webdiensten;
6. WS-Federatie – Gebruik van "*federated identities*", d.w.z. hergebruik en centraal beheer van identiteiten.

Het voorzien van deze diensten betekent echter nog niet dat deze beveiligingen effectief of correct gebruikt worden. Webdiensten introduceren ook nieuwe veiligheidsbedreigingen voor de zakenwereld. Door het aanbieden van essentiële processen uit de handel en diensten via het web [1], wordt de zakenwereld op het internet aan een aantal ernstige gevaren blootgesteld. Er mag dus geen twijfel over bestaan dat er extra veiligheidsmaatregelen moeten genomen worden om de webdiensten veilig te maken. De technologie voor de veiligheid is weliswaar beschikbaar, maar is de nodige expertise aanwezig en worden de ontwerpen van de bedrijfsprocessen in de webdiensten correct en veilig gemaakt? Om te beginnen moeten de ontwikkelaars de correcte technologische componenten incorporeren om Webdiensten veilig te maken. Bovendien moeten ze zich bewust zijn van het belang van de veiligheid. Vaak is dit een groot probleem omdat de meeste ontwikkelaars de veiligheid aan de infrastructuurbeheerders overlaten. De ontwikkelaars moeten opgevoed worden op het gebied van de veiligheid in relatie met webdiensten en de gebruikte *interfaces* moeten geaudit worden. Kan een *hacker* deze *interfaces* gebruiken om

informatie te verkrijgen die niet voor hem bestemd is? De *administrators* moeten zich ook bewust zijn van de veiligheid opgelegd door de webdiensten. Bijvoorbeeld moet er correct omgegaan worden met "*firewalls*". Webdiensten tonen aan dat traditionele *firewalls* niet meer werken. Alle verkeer van webdiensten passeert door de http- poort (*web protocol*). Deze poort is normaal gezien open voor webverkeer. Traditionele *firewalls* stoppen het verkeer van de webdiensten niet en alle zakenverkeer is bijgevolg open op het internet. *Firewalls* moeten het toepassingsgebied en het verkeer controleren. Welk soort webdiensten moeten door de infrastructuur gaan? De firewall moet deze vragen begrijpen en kwaadaardige vragen onmiddellijk stoppen. Webdiensten zijn een grote vooruitgang in de softwarearchitecturen maar we moeten met de veiligheid op een gestructureerde manier omgaan. We moeten processen maken die toelaten om de veiligheidsaspecten van webdiensten te valideren. Pas dan kunnen we optimaal gebruik maken van de mogelijkheden die de webdiensten op onze computerarchitecturen bieden.

6. CONCLUSIES EN AANBEVELINGEN

Tot slot worden de voornaamste besluiten en aanbevelingen geformuleerd die ook gericht worden naar de *diverse doelpublieken*, waarvoor dit rapport werd opgesteld. Uiteraard wordt voor de context en voor de fijnere analyses en aanbevelingen naar de verschillende secties van het rapport verwezen.

Voor het bredere publiek
De aandacht van het bredere publiek is zeer kortstondig en vluchtig, maar de grootte en de impact van de ICT-risico's vereisen een continue zorg bij het bredere publiek voor informatiebeveiliging in tal van diensten en informatiekanalen zoals elektronisch bankieren, internet gebruik, zaken doen via internet, en de bescherming van de levenssfeer.
Bovendien is één van de essentiële elementen van technische beveiliging dat de veiligheid van het systeem bij de rechtmatige gebruikers gelegd wordt door middel van sleutels, *tokens*, paswoorden en software die de gebruiker waarschuwt voor verdachte links of e-mails. Als deze middelen niet veilig gebruikt worden, is de volledige technische beveiliging waardeloos.
Aanbeveling: aangepaste mediacampagne om de aandacht en de waakzaamheid en de zorg bij het bredere publiek blijvend te stimuleren

Voor bedrijfsleiders, diensthoofden, en personeel
In onze hedendaagse maatschappij speelt ICT een steeds maar belangrijker rol en de beveiliging van deze informatie- en communicatiesystemen is dan ook een zeer belangrijk aandachtspunt, dat al bij de conceptie van de systemen grondig uitgedacht en uitgewerkt moet worden. Zoals de sterkte van een ketting bepaald wordt door de sterkte van de zwakste schakel, vereist de beveiliging van ICT-systemen een globale aanpak, die aandacht heeft voor de zeer diverse zwakheden. Door de telecommunicatie en netwerken bevinden de aanvallers zich bovendien vaak op grote afstand en blijven ze onzichtbaar. Veel veiligheidsrisico's zijn vaak niet gekend of worden onderschat. Bovendien maken de globalisering en de computernetwerken de impact van aanvallen veel massaler en onzichtbaarder.
Aanbeveling: Managers, bedrijfsleiders, diensthoofden en personeel verantwoordelijk voor diverse infrastructuren, bedrijven, en diensten dienen terdege rekening te houden met de totale informatiebeveiliging zowel in het ontwerpproces als bij het operationeel gebruik. Door een adequate technische beveiliging, de bijhorende opleiding van het personeel, en de auditing van het systeem kunnen de risico's sterk gereduceerd worden zoals geargumenteerd in het rapport. Voor de eventuele overblijvende risico's kan een verzekeringspolis afgesloten worden. Soms is een uitbesteding van de ICT-beveiliging een goede oplossing om een gewenst niveau van beveiliging te bereiken tegen een redelijke kost.

Voor de onderzoekers en bedrijfsleiders in de ICT-sector
Zoals geargumenteerd in het rapport is er op dit ogenblik al een waardevol en effectief geheel van technische, organisatorische en juridische methodes om de beveiliging van informatie adequaat aan te pakken voor de diverse toepassingsdomeinen. Er blijven echter nog grote opportuniteiten en uitdagingen voor het onderzoek en de ontwikkeling van nieuwe producten in dit domein. De technologische vooruitgang in de rekencapaciteit, geheugenopslag, de zoekmachines, en de cryptografische en computeraanvallen zorgen er echter voor dat de methodieken snel verouderd zijn en niet langer als veilig kunnen beschouwd worden. Bovendien is er in *cyberspace* nood aan nieuwe nieuwe veilige virtuele producten of diensten zoals elektronisch geld of elektronisch stemmen, die niet meer gebonden zijn aan materie. Telkens is het cruciaal om de beveiliging van het systeem van bij de conceptie terdege in rekening te brengen.
Aanbeveling: Managers, bedrijfsleiders, creatieve ingenieurs, informatici en juristen met gedegen kennis van de beveiliging van informatie kunnen deze noden aan beveiligingsproducten en diensten aangrijpen voor relevant onderzoek en ontwikkeling.

Voor de jongeren en de onderwijswereld
De jongeren zijn vaak veel beter bedreven in het gebruik van ICT en internet dan hun ouders, grootouders, of opvoeders. Dat is natuurlijk hoopvol voor de toekomst gezien het toenemende belang en de impact van ICT, maar vaak zijn de jongeren nogal onbezonnen en nieuwsgierig en zich niet voldoende bewust van de vele gevaren van ICT en internet.
Aanbeveling: Eerder dan de jongeren af te houden van deze nieuwe technologieën is een aangepaste aanpak gewenst waarbij de jongeren een verantwoord gedrag, houding en ethisch bewustzijn worden aangeleerd vanaf een jonge leeftijd. Zowel de ouders, grootouders als het onderwijzende personeel moeten hiertoe geïnformeerd en opgeleid worden. Daarnaast moeten alle opleidingen in ICT voldoende aandacht besteden aan informatiebeveiliging.

Voor de politici, en juristen
Misbruiken in ICT veroorzaken vaak een gevoel van onveiligheid, ongrijpbaarheid en straffeloosheid. De technische beveiliging kan hierin wel een adequate barrière opleggen. Maar door financiële beperkingen, menselijk falen, of kwaad opzet kunnen ICT-misdrijven van zeer gevarieerde aard geschieden. De wetgevende overheden op diverse niveaus dienen de nodige regelgeving te creëren om deze misbruiken te beteugelen. Gezien de internationale aard van telecommunicatie en internet zijn lokale aanpak en beteugeling vaak ontoereikend.
Aanbeveling: Meer aandacht in de wetgeving op internationaal niveau voor de cybercriminaliteit.

Voor de overheid
Informatiebeveiliging vergt een complexe interactie met algemene ICT en met beveiliging, waarin naast juridische ook technische, economische en organisatorische aspecten een rol spelen. De overheid neemt een aantal goede initiatieven (elektronische identiteitskaart, BELNET CERT, BIPT *virus warning*, bescherming van de persoonlijke levenssfeer, informatieveiligheidsdiensten), maar in het algemeen ontbreekt een geïntegreerde en gecoördineerde aanpak waarbij maximaal gebruik wordt gemaakt van de expertise die aanwezig is in de onderzoeksinstellingen en bedrijven. Als voorbeelden vermelden we hier initiatieven op het vlak van CIIP (*Critical Information Infrastructure Protection*), accreditatie, certificatie en evaluatie. Als België een competitieve kenniseconomie wil ontwikkelen, moet het net zoals zijn buurlanden voldoende investeren in onderzoek naar alle aspecten van informatiebeveiliging.
Aanbeveling: Betere coördinatie van alle aspecten van informatiebeveiliging op overheidsniveau. Ontwikkelen van een geïntegreerde onderzoeksstrategie op het vlak van informatiebeveiliging met extra aandacht voor de bescherming van kritische ICT-infrastructuur. Uitwerken van een incidentprocedure.

Voor het gebruik van standaarden
Er is heel wat vooruitgang gemaakt in het opstellen van standaarden voor beveiliging en cryptografie, dankzij gedegen onderzoek en samenwerking wereldwijd (cf. internationale encryptiestandaard “AES”). Dergelijke standaarden hebben het grote voordeel grondig en degelijk en op een open en dus volledig publiek verifieerbare manier bestudeerd te zijn. Anderzijds kan men zich juist differentiëren van standaarden door geheime methodieken te gebruiken. Aangezien die methodieken minder grote doelwitten zijn voor aanvallers kan men hopen dat dit hen minder zal aantrekken. Maar de vele gevaren die in geheime methodieken schuilen zoals achterpoortjes, verborgen zwakheden, en vooral de veel geringere studie en analyse van deze methodes, vergen hier een zeer grote voorzichtigheid zeker voor publieke systemen. Bovendien zijn geheime methodieken onmogelijk geheim te houden.
Aanbeveling: in de mate van het mogelijke en redelijke moet beveiliging gebruik maken van standaarden en best practices die hun deugdelijkheid bewezen hebben.

Voor een ethisch bewustzijn
De zorg voor mens, milieu, en maatschappij op korte en langere termijn vraagt een ethische houding t.o.v. informatie en communicatietechnologie zowel van de zijde van de overheid, de dienstenleveranciers, de bestuurders, de verantwoordelijken van ICT-infrastructuur, de ouders, opvoeders, en onderzoekers.
Aanbeveling: Een internationale ethische gedragscode voor de diverse betrokken groepen zou moeten opgesteld worden en ruim bekend gemaakt worden.

7. REFERENTIES

[1] CAWET rapport: *“Elektronisch zakendoen in een netwerkeconomie”,* augustus 2002.

[2] Robben, F. en Deprest, J., “*E-government: the approach of the Belgian federal administration”*, Brussel, FEDICT & Kruispuntbank van de Sociale Zekerheid, 2003, 26 e.v. (aflaadbaar van www.law.kuleuven.ac.be/icri/frobben - Rubriek Publication list).

[3] A. Menezes, P. van Oorschot en S. Vanstone, *"Handbook of Applied Cryptography*", CRC Press, ISBN: 0-8493-8523-7, October 1996, 816 paginas. (aflaadbaar van www.cacr.math.uwaterloo.ca/hac/).

[4] I. Abele-Wigert, M. Dunn, International CIIP Handbook 2006 (Vol. I) - *An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies,* ETH Zurich, Center for security studies, 493 paginas.

[5] Myriam Dunn, Victor Mauer (Eds.), International CIIP Handbook 2006 (Vol. II) - *Analyzing Issues, Challenges, and Prospects,* ETH Zurich, Center for security studies, 235 paginas.

[6] Commission of the European Communities, *"Green Paper on a European Programme for Critical Infrastructure Protection"*, COM (2005) 576, Nov. 2005, 26 paginas.

[7] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, "Identifying, understanding, and analyzing critical infrastructures interdependencies," *IEEE Control Systems Magazine,* Dec. 2001, pp. 11-25.

[8] United Nations resolution 58/199, *"Creation of a global culture of cyber security and the protection of critical information infrastructures",* Jan 2004, 3 pages, online at http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf

Relevante Webpagina's

www.privacycommission.be/publicaties.htm "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens"
www.eid.belgium.be en homes.esat.kuleuven.be/~decockd/ voor meer informatie omtrent de elektronische identiteitskaart
www.cardreaders.be voor meer informatie over de leesapparaten
www.l-sec.be voor informatie over bedrijven actief in informatiebeveiliging:

Auteurs:

Prof. Joos Vandewalle – K.U.Leuven, Coördinator	JV
Prof. Bart Preneel – K.U.Leuven, Coördinator	BP
Prof. Jos Dumortier – K.U.Leuven	JD
Prof. Geert Deconinck K.U.Leuven	GD
Mevr. Annick Loks – ING	AL
Dr. Marijke De Soete – Security4Biz	MD
Dhr. Frank Robben – Kruispuntbank Sociale Zekerheid	FD
Dhr. Hugo Van der Veeken – Banksys	HV
Dhr. Luc Beirens – FCCU	LB
Dhr. Paul Bruyninckx – Fortis, UAntwerpen	PB
Dhr. Frank Jorissen – SafeBoot	FJ
Dhr. Jean-Jacques Cockx – Unisys Consulting	JC
Dhr. Ronny Bjones – Microsoft	RB
Dhr. Jurgen Truyen – L-SEC	JT

CAWET MEMBERS

President:
Dr.ir. Guy HAEMERS
INVENTURES Group Europe

Vice President:
Prof. Ludo GELDERS
Industrial Management, Katholieke Universiteit Leuven

Secretary, External Communications:
Dr. ir. Paul VERSTRAETEN
ArcelorMittal Gent

Members:
Prof. Etienne AERNOUDT
Metals and Materials Engineering, Katholieke Universiteit Leuven
Ir. Guido BEAZAR
V.K.W.
Prof. Ronnie BELMANS
ESAT, ELEN, Katholieke Universiteit Leuven
Prof. Jean BERLAMONT
Hydraulics, Katholieke Universiteit Leuven
Ir. Luc BOSSYNS
Aquafin, Aartselaar
Prof. Bart DE MOOR
Electrical Engineering, Katholieke Universiteit Leuven
Prof. dr. ir. William D'HAESELEER
Energie-instituut, Katholieke Universiteit Leuven
Ir. Marc FRANCKEN
Gevaert, Antwerpen
Burggraaf Dirk FRIMOUT
Ministerie Economie, Brussel
Prof. Derrick GOSSELIN
Suez Energy International, Brussel
Prof. Charles HIRSCH
Fluid Mechanics, Vrije Universiteit Brussel
Dr. ir. Jan KRETZSCHMAR
VITO, Mol
Ir. Robert LENAERS
NV Vanhout, Geel
Dr. ir. Jan LEURIDAN
LMS International, Leuven
Dr. ir. Egbert S.J. LOX
Umicore N.V.
Ir. Leo MICHIELS
Proviron, Oostende
Prof. dr. ir. André OOSTERLINCK
Coördinatie Associatie, Katholieke Universiteit Leuven
Ir. Norbert VAN BELLE
Janssen Pharmaceutica, Beerse
Prof. Hendrik VAN BRUSSEL
PMA, Katholieke Universiteit Leuven
Prof. Erick VANDAMME
Industrial Microbiology, Universiteit Gent
Prof. Georges VAN DER PERRE
Biomechanics and Graphic Design, Katholieke Universiteit Leuven
Prof. Joos VANDEWALLE
ESAT, Katholieke Universiteit Leuven
Ir. Willy VAN OVERSCHEE
IBM, Brussel
Dr. ir. J. VAN REMORTEL
Alcatel Bell, Antwerpen

Honorary Presidents:
Prof. Achiel VAN CAUWENBERGHE
Control Engineering, Universiteit Gent

Ir. Valentin VAN den BALCK
Berenschot, Brussel

Prof. Daniël VANDEPITTE
Civil Engineering, Universiteit Gent

Ir. Joost VAN ROOST
ExxonMobil, Breda
Dr. ir. Erik TAMBUYZER
Genzyme Flanders N.V.
Ir. Ivo VAN VAERENBERGH
REM-B, Zoersel
Prof. Pierre VERBAETEN
Computer Science, Katholieke Universiteit Leuven
Prof. Ronny VERHOEVEN
Hydraulics, Universiteit Gent
Prof. Ignaas VERPOEST
MTM, Katholieke Universiteit Leuven
Prof. Willy VERSTRAETE
Microbial Ecology, Universiteit Gent
Prof. Jacques Baron WILLEMS
Electrical Systems, Universiteit Gent

Associate Members:
Ir. Herman DEROO
KVIV, Antwerpen
Prof. Robert GOBIN
Graphic Design, Katholieke Universiteit Leuven
Mr. Erik JACQUEMIJN
Stichting Flanders Technology International, Mechelen
Dr. Henri MALCORPS
Royal Meteorological Institute, Brussel
Ir. Michel NAZE
Capsugel, Bornem
Ir. Alfons PEETERS
Eternit, Brussel
Ir. Paul VAN DER SPIEGEL
Keerbergen
Dr. Jan VAN KEYMEULEN
Kasteelbrakel
Prof. Hendrik VAN LANDEGHEM
Technische Bedrijfsvoering, Universiteit Gent
Prof. Pascal VERDONCK
Hydraulics, Universiteit Gent

Honorary Members:
Ir. Jean BEECKMAN, Dr. ir. Stan BEERNAERT, Prof. Hugo DE MAN, ir. Jozef DEMAN, ir. Jean-Pierre DE PAEMELAERE, ing. Lucien DE SCHAMPHELAERE, Prof. Walter Baron FIERS, Prof. Gilbert FROMENT, Prof. René JACQUES, ir. Jan JONGBLOET, Roland MAES, Dr. ir Lars MALMROS, Dr. ir. Urbain MEERS, Prof. Jacques PETERS, Prof. Niceas SCHAMP, Ir. Marcel SOENS, Ir. Stan ULENS, Prof. Jean VAN BLADEL, Prof. Marc Baron VAN MONTAGU, Prof. Marc VANWORMHOUDT, Ir. Roland WISSAERT

BACAS *Steering Committee*

Dr. ir. G. HAEMERS, president CAWET and BACAS
Prof. L. GELDERS, vice-president CAWET
Dr. ir. P. VERSTRAETEN, secretary CAWET
Prof. A. VAN CAUWENBERGHE, past president

Prof. Ph. BOURDEAU, president CAPAS
Prof. N. DEHOUSSE, past president
Ir. P. KLEES, past president CAPAS
Ir. J.J. VAN DE BERG, vice-president CAPAS

Prijs : € 12,50