Waardevol maakt kwetsbaar

Het belang van informatiebeveiliging

Geachte aanwezigen,

Inleiding

Informatiebeveiliging is actueel. Hoe vaak lezen we in de krant niet dat er weer een bedrijf of instelling getroffen is? En dan valt het nog mee als de schade zich beperkt tot één organisatie, want voor hetzelfde geld wordt een hele regio 'platgelegd', zoals heel Rome door een grootschalige stroomstoring op 28 september jl. Dat kan hier ook gebeuren. En de berichten in de media zijn nog maar het topje van de ijsberg; dat zijn de echte calamiteiten, waarbij doden en gewonden zijn gevallen. Kleinere incidenten komen veel vaker voor. Vaker dan u denkt. Elk moment kan uw computer crashen, een hacker uw website binnendringen, het netwerk verstopt raken, of een nieuw computervirus uw bestanden aantasten.

We hebben de neiging om de kans van al die bedreigingen te bagatelliseren. Hoe vaak hoor je niet uitspraken zoals bijvoorbeeld "er is bij ons toch niets te halen", of "de kans op brand is zó klein"? We hebben er zelfs een spreekwoord voor, eentje over een kalf en een put. Blijkbaar is het heel gewoon om niets te doen tot het te laat is; tot we zelf getroffen zijn. En als er dan wel maatregelen getroffen worden, dan is het vooral om huis en haard te beschermen. Maar hoe zit het dan met de informatiesystemen en de peperdure informatie daarin? De informatie waar het voortbestaan van de organisatie van afhangt? Daaraan moet nog heel wat verbeterd worden.

In deze rede neem ik u mee naar de wereld van de *informatiebeveiliging*. Velen van u vinden dit waarschijnlijk een technisch onderwerp, of tenminste een zeer specialistisch onderwerp. En dat klopt ook! Aan de andere kant is informatiebeveiliging ook een zeer alledaags verschijnsel, maar daar kom ik nog op terug. Eerst wil ik inzoomen op het eerste deel van het woord informatiebeveiliging, namelijk de term *informatie*. Informatie is – kort door de bocht – met subjectieve betekenis verrijkte gegevens. De begrippen *gegevens* en *informatie*, betekenen dus niet hetzelfde, maar vandaag gebruik ik de term informatie ook als er 'gegevens' bedoeld worden.

Informatie en informatiesystemen

Informatie is niet uit onze maatschappij weg te denken. Onze hele maatschappij en elke organisatie daarin draait op informatie. Informatie speelt binnen *iedere* organisatie een cruciale rol. *Zonder informatie geen organisatie!* En dat geldt heel letterlijk. Informatie kan verschillende verschijningsvormen hebben: mondeling, schriftelijk en digitaal. De grenzen tussen deze verschijningsvormen zijn niet altijd even scherp. Zo wordt tijdens mobiel bellen mondelinge informatie door de GSM-telefoon omgezet in digitale informatie en vice versa.

Informatie, al dan niet op een bepaalde drager, kan meer of minder waarde hebben. Soms is de waarde niet zo goed te bepalen, zoals bijvoorbeeld de waarde van een onderzoeksrapport. In andere gevallen is de waarde direct duidelijk, zoals bijvoorbeeld bij een bankbiljet. Een ander document dat om zijn waarde bekend staat, is het paspoort. De maatschappelijke schade van één vermist Nederlands paspoort is ongeveer € 40.000. Dat komt met name doordat een *on*eerlijke vinder van een paspoort met behulp daarvan onterecht uitkeringen, subsidies en leningen kan aanvragen. Ook digitale informatie kan duidelijke waarde hebben. Voorbeelden hiervan zijn de bankpas en de creditcard. Met de bijbehorende pincode kan direct geld uit de geldautomaat gehaald worden.

Binnen een organisatie is allerlei informatie aanwezig, zoals informatie over personeel, cliënten, producten, financiën, onderzoeksresultaten, enzovoorts. Al die informatie wordt verwerkt, opgeslagen en getransporteerd in *informatiesystemen*. Zij vormen het zenuwstelsel van de organisatie. Als kritische informatiesystemen uitvallen, dan stagneren de bedrijfsprocessen; en als dat te lang duurt dan gaat de organisatie daaraan ten onder. Ernstige gevolgen kunnen ook ontstaan door financiële malversaties, of doordat de salarisadministratie per abuis op de website gezet wordt. De gevolgen kunnen van financiële aard zijn, maar ook betrekking hebben op klantenverlies, imagoschade, of erger. Stelt u zich maar eens voor wat er gebeurt als de medische informatie van patiënten in een ziekenhuis niet meer klopt. Dat kan leiden tot verkeerde medische handelingen, die het nieuws halen; en dat schaadt het vertrouwen in het betreffende ziekenhuis, maar misschien ook wel de hele medische sector.

De omvang van de schade die op kan treden is een goede maat voor de waarde van een informatiesysteem en de informatie daarin. Sommige informatiesystemen zijn zo onmisbaar voor onze maatschappij dat het wegvallen van zo'n informatiesysteem tot slachtoffers of ontwrichting van het maatschappelijk leven kan leiden. Voorbeelden

hiervan zijn de systemen voor stormvloedwaarschuwing en het besturen van de stormvloedkering, de systemen van de luchtverkeersleiding, de communicatiesystemen van de hulpdiensten en de systemen van de Nederlandse betaalinfrastructuur. We moeten er toch niet aan denken dat zo'n systeem uitvalt.

Waardevolle informatiesystemen hebben een grote aantrekkingskracht op allerlei mensen binnen en buiten de organisatie. Deze mensen zijn niet noodzakelijkerwijs allemaal te goeder trouw. Integendeel, echt waardevolle informatiesystemen trekken onbetrouwbare types aan en dat maakt deze systemen extra kwetsbaar. Dit betekent niet perse dat waardevolle informatiesystemen ook weerloos zijn, om de woorden van Lucebert te gebruiken; dat is een kwestie van beveiliging. Goede informatiebeveiliging zorgt ervoor dat waardevolle informatiesystemen en informatie juist *niet* weerloos zijn. Overigens zit daar nog wel een probleem, want het realiseren van goede informatiebeveiliging is verre van eenvoudig, maar daar kom ik nog op terug.

Bedreigingen

Moderne informatiesystemen zijn in hoge mate geautomatiseerd, oftewel gebaseerd op informatie- en communicatietechnologie (ICT). Deze technologie is echter vatbaar voor vele verschillende bedreigingen. Een kleine greep uit de mogelijkheden: brand, bliksem, overstroming, apparatuur- en programmatuurstoringen, elektriciteitsstoringen, menselijke vergissingen, virussen, hacking, diefstal, fraude, sabotage, enzovoorts. Dat deze bedreigingen niet hypothetisch zijn, blijkt uit een niet aflatende stroom incidenten. Alleen de ergste incidenten halen het nieuws. Recente voorbeelden zijn de verwoesting van het computercentrum van Rijkswaterstaat in Lelystad door brand, de verstoring van bedrijfsnetwerken door internetvirussen en wormen zoals Slammer en Sobig, de fraude met Nederlandse paspoorten, het boekhoudschandaal bij Albert Heijn en de gemanipuleerde onderzoeksresultaten over geluidsoverlast van Schiphol. En zo zou ik met nog meer voorbeelden deze hele rede wel vol kunnen krijgen.

Risico's

Vanwege de grote verschillen in de aard van de bedreigingen moet er ook een heel palet aan zeer verschillende *beveiligingsmaatregelen* getroffen worden.

Om te bepalen tegen welke bedreigingen maatregelen getroffen moeten worden, moet men niet zozeer naar de *bedreigingen* kijken, maar naar de *risico's*. De risico's geven aan welke schade men kan verwachten door toedoen van de bedreigingen. Op basis daarvan

is gerichter te beveiligen, en kan je voorkomen dat je een euro uittrekt om een dubbeltje te beschermen. Het begrip schade doelt niet alleen op de directe financiële schade, maar ook de andere vormen van schade voor de organisatie zelf en de maatschappij.

Er bestaat een verband tussen de risico-omvang, ofwel de te verwachten schade door bedreigingen, en de kosten van de getroffen maatregelen. In de figuur is dat aangegeven door de dalende curve, die in de praktijk wat minder gelijkmatig verloopt dan de getoonde curve. Globaal laat de figuur zien dat de risico's steeds verder dalen bij het treffen van steeds meer maatregelen. Daarbij gaan we er wel van uit dat de getroffen maatregelen zinnig zijn en een samenhangend geheel vormen.

De figuur laat ook zien dat er in de curve drie zones onderscheiden kunnen worden. De bovenste zone is die waarin weinig of geen maatregelen getroffen zijn. Organisaties die in deze zone blijven hangen kunnen niet voorkomen dat ernstige bedreigingen tot onacceptabele schade leiden. Hierbij valt te denken aan het verlies van het bedrijfspand door brand, dodelijke slachtoffers door een ongeval, faillissement door fraude, enzovoorts. De term onacceptabel geeft al aan dat dergelijke risico's te allen tijde voorkomen moeten worden. Van de hiervoor noodzakelijke maatregelen mag er niet één ontbreken. In de privé-sfeer is dit te vergelijken met bijvoorbeeld een ziekteverzekering. Het is zeer onverstandig om, als besparing, de medische kosten ten gevolge van ongevallen uit te sluiten omdat de kans op een ongeluk zo klein is. Afgezien van het feit dat de kans op een ongeluk helemaal niet zo klein is (alleen in het Nederlandse verkeer vallen jaarlijks al meer dan 1000 doden en nog veel meer gewonden), is het ook nog eens zo dat het optreden van een ongeluk niet alleen bepaald wordt door je eigen gedrag, maar ook door het gedrag van anderen. Je zal maar net de pech hebben om 's avonds op straat een dronken brokkenpiloot te treffen; de kans daarop is klein, maar niet nul. Ook in het bedrijfsleven geldt dat er altijd omstandigheden zijn die weinig tot niet te beïnvloeden zijn, zodat je er vanuit moet gaan dat er ongewenste gebeurtenissen op kunnen treden. Maatregelen hiertegen zijn dus noodzakelijk.

Naast het nemen van *te weinig* maatregelen is het ook mogelijk om *te veel* maatregelen te treffen. Dit is de onderste zone in de figuur. Hier bevinden zich de overbodige maatregelen; hier worden euro's uitgegeven om dubbeltjes te beveiligen. Hier vinden we ook de maatregelen die vallen onder de noemer beveiligingshypes. Een hype is een modieuze trend die niet voor iedere organisatie even nuttig is. Als een organisatie klakkeloos een beveiligingshype volgt, dan levert dat al gauw onnodige maatregelen op. Een beveiligingshype van dit moment is bijvoorbeeld biometrie. Voor sommige organisaties een uitkomst, voor andere organisaties een onnodige kostenpost. In

Schiphol wordt een vorm van biometrie, namelijk irisherkenning, gebruikt om passagiers met een daarvoor bestemd abonnement te identificeren zodat deze sneller de grens kunnen passeren. In dit geval is biometrie een zinnige maatregel, maar in de meeste andere organisaties moeten eerst nog een heleboel basale zaken geregeld worden voordat men toe is dit soort geavanceerde maatregelen.

Het treffen van te veel maatregelen is niet alleen overbodig, maar zelfs ongewenst. In een organisatie mogen dergelijke maatregelen eigenlijk niet getroffen worden. Buiten het feit dat ze onnodig geld kosten, tasten ze namelijk het cruciale vertrouwen in de andere maatregelen aan; andere maatregelen die wel noodzakelijk zijn. In beveiligingsland geldt daarom *niet* het adagium "baadt het niet, schaadt het niet", maar in plaats daarvan "overdaad schaadt". En dat mag u letterlijk opvatten. Toch wordt dit principe vaak overtreden, ook door deskundigen op het gebied van informatiebeveiliging. In hun drang om informatiebeveiliging toch vooral serieus te nemen, lopen ze te hard van stapel en introduceren overbodige maatregelen. Een veel voorkomend voorbeeld hiervan is dat gebruikers hun wachtwoord regelmatig moeten wijzigen. U herkent deze maatregel misschien wel uit uw eigen werksituatie. Het nieuwe wachtwoord moet bestaan uit weer een nieuwe onraadbare tekencombinatie, die dus ook nauwelijks te onthouden is. Zo'n maatregel, die in bepaalde situaties zeer nuttig of zelfs noodzakelijk is, wordt dan klakkeloos en ongedifferentieerd voor iedereen binnen de organisatie in dezelfde vorm verplicht gesteld. De gebruikers hebben in zo'n geval echter haarfijn door, dat als de regel voor bijvoorbeeld de systeembeheerder en de directeur geldt, dat andere medewerkers, waaronder bijvoorbeeld de magazijnbediende, dan zwaarder beveiligen dan nodig is. Deze en vele andere overbodige of ongedifferentieerde maatregelen hebben in het algemeen zeer negatieve gevolgen voor de attitude ten aanzien van informatiebeveiliging. Dit punt is één van de grootste problemen binnen de informatiebeveiliging en ik zal daar dan ook nog op terugkomen.

De middelste zone in de figuur is het gebied waar het bij informatiebeveiliging om gaat. Hier bevinden zich de maatregelen waarover keuzes gemaakt moeten worden. Het betreft maatregelen tegen bedreigingen die weliswaar vervelende consequenties hebben, maar die ook niet onoverkomelijk zijn. Op basis van genuanceerde overwegingen moeten hieruit de juiste maatregelen gekozen worden. Dit vergt niet alleen kennis van bedreigingen, maar ook kennis van de organisatie. Goede keuzes stoelen op goede informatie. Informatie over eerdere incidenten kan daarbij erg nuttig zijn; van het verleden kunnen we namelijk een hoop leren. Deze informatie ontbreekt echter vaak. De noodzakelijke registratie van beveiligingsincidenten is in het algemeen slecht op orde. En mede daardoor ontbreekt het ook aan algemene statistieken over het manifesteren van

bedreigingen en de daarbij opgetreden schade. Het lectoraat Informatiebeveiliging kan hierin een functie vervullen, onder andere door het doen van statistisch onderzoek naar bedreigingen, met name in de Haagse regio.

Risicoanalyse

Met behulp van kennis over bedreigingen en risico's is het mogelijk om geschikte beveiligingsmaatregelen te vinden. De analyses die daarvoor nodig zijn, de zogenaamde *risicoanalyses*, maken deel uit van de informatiebeveiliging. Eén bepaalde variant van risicoanalyse, namelijk de Afhankelijkheids- & Kwetsbaarheidsanalyse (A&K-analyse), wordt veel bij de Nederlandse overheid toegepast. Voor de Rijksoverheid is de A&K-analyse zelfs verplicht voor het uitvoeren van risicoanalyses. Sterker nog, volgens het Voorschrift Informatiebeveiliging Rijksdienst (VIR) uit 1994 dient elke instelling van de Rijksoverheid voor *elk* geautomatiseerd informatiesysteem een A&K-analyse uit te voeren, om te bepalen welke beveiligingsmaatregelen voor het betreffende systeem nodig zijn.

Het uitvoeren van een risicoanalyse, en dus ook een A&K-analyse, is echter een lastige en tijdrovende klus. Als we er van uitgaan dat het niet uitzonderlijk is als een departement honderden tot duizenden informatiesystemen heeft, dan is het niet verrassend dat het uitvoeren van A&K-analyses voor *alle* informatiesystemen een departement nogal wat problemen bezorgt. En dat het uitvoeren van A&K-analyses de departementen problemen bezorgt, is wel zeker. Bijna tien jaar na het verschijnen van het VIR zijn er nog steeds departementen die het niet gelukt is om voor alle informatiesystemen A&K-analyses uit te voeren. Dit betekent dat er informatiesystemen zijn waarvoor nog nooit één A&K-analyse uitgevoerd is, laat staan dat er geactualiseerde analyses beschikbaar zijn. Voor dergelijke informatiesystemen is het dus niet vast te stellen of de beveiliging op orde is.

Een extra complicatie voor het uitvoeren van A&K-analyses is dat het daarvoor eigenlijk noodzakelijk is om een goed geautomatiseerd hulpmiddel te hebben. Het vele schrijf-, puzzel- en opzoekwerk kost anders gewoon te veel tijd. Het probleem is echter dat er nog geen geschikt geautomatiseerd hulpmiddel beschikbaar is. Onze Rijksoverheid heeft weliswaar een poging gedaan om zo'n hulpmiddel te laten maken, maar het resultaat daarvan is helaas onbruikbaar. Het enige beschikbare hulpmiddel is dus een onbruikbaar hulpmiddel. Er worden nu wel noodoplossingen ingezet zoals het toepassen van minder geschikte hulpmiddelen uit het buitenland, maar het toepassen daarvan kost weer veel extra inspanning.

Al met al is het laatste woord over het VIR en methoden voor risicoanalyse nog niet gezegd. Het lectoraat Informatiebeveiliging kan partij zijn bij het evalueren van regels en richtlijnen voor risicoanalyses, zoals bijvoorbeeld het VIR, maar ook bij het evalueren en verbeteren van methoden en technieken voor risicoanalyse.

Informatiebeveiliging

Voor iedere organisatie is het van belang dat verantwoord wordt omgaan met risico's. Er zijn personele, materiële, en financiële risico's, maar ook risico's met betrekking tot de informatievoorziening. Het reduceren van de risico's met betrekking tot de informatievoorziening is het domein van de informatiebeveiliging. Informatiebeveiliging wordt gedefinieerd als het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid van de informatie en de informatiesystemen te waarborgen. Informatiebeveiliging is een verzamelnaam voor de processen en maatregelen die door de organisatie ingericht worden om de vertrouwelijkheid, de beschikbaarheid en de integriteit van de informatie en de informatiesystemen te beschermen tegen allerlei onheil.

Informatiebeveiliging heeft een lange en rijke historie. Voor de opkomst van de automatisering speelde informatiebeveiliging zich grotendeels af in militaire kringen. Al in de tijden van de Grieken en de Romeinen werden oorlogen uitgevochten. Toen al werden cryptografische en steganografische technieken gebruikt om onderling tactische militaire informatie uit te wisselen, zonder dat deze in handen van de tegenpartij zou vallen. In die tijd was er ook sprake van een 'wapenwedloop' tussen enerzijds de ontwikkelaars van steeds weer nieuwe beveiligingstechnieken en anderzijds de krakers ervan. Aangezien vrijwel elke staat of groepering met enige regelmaat een oorlog uitvocht met deze of gene, werd op veel plaatsen, naast al het onderzoek naar wapentechnologie, ook onderzoek gedaan naar het beveiligen van de eigen informatie en het kraken van andermans informatie. Dat beeld is door de eeuwen heen eigenlijk niet meer veranderd.

Met de komst van de automatisering na de Tweede Wereldoorlog is een tweedeling in de informatiebeveiliging ontstaan: het beveiligen van digitale informatie versus het beveiligen van de overige informatie. De eerste, het beveiligen van digitale informatie, kreeg en krijgt binnen het vakgebied informatiebeveiliging de grootste aandacht. Binnen het lectoraat Informatiebeveiliging zullen we deze tendens wel volgen, maar ons niet uitsluitend op het beveiligen van digitale informatie richten.

Tijdens de opkomst van de automatisering is het beveiligen van digitale informatie meegegroeid met de ontwikkelingen in automatiseringsland. In het mainframe-tijdperk – de jaren ’60 en ’70 van de vorig eeuw – was alle digitale informatie geconcentreerd op enkele locaties, namelijk in en rond de mainframes. Informatiebeveiliging was toen heel overzichtelijk. Daarna heeft de automatisering een tijd van spreiding gekend, de opkomst van de personal computers (de pc’s). De digitale informatie spreidde mee en ook de beveiliging ervan speelde ineens op vele locaties. Ondanks de grote spreiding van digitale informatie was er eerst nog niet zoveel digitale communicatie; communicatie met behulp van floppies was heel gewoon. Informatiebeveiliging speelde zich toen voornamelijk af op de vele locaties waar de computers stonden. Gaandeweg kwamen er echter steeds meer netwerken met daarover steeds omvangrijkere informatiestromen. Netwerken werden onderling gekoppeld tot steeds grotere netwerken. Internet ontstond en werd binnen een paar jaar razend populair. Vrijwel iedere organisatie sloot aan op Internet en zelfs de pc’s en de spelcomputers in de huiskamer werden aangesloten op Internet. Dat is de situatie die we nu kennen: vrijwel iedereen heeft op zijn werk of thuis een computer en communiceert digitaal door middel van e-mail, chatten, browsen, enzovoorts. Zelfs draadloos wordt er steeds drukker gecommuniceerd. Draadloze communicatie via WiFi-technologie is de kinderschoenen ontgroeid. Via andere draadloze technieken zoals GSM, GPRS en binnenkort UMTS gaat niet alleen digitale spraak door de lucht, maar ook foto’s en zelfs video.

Dat iedereen met iedereen via al dan niet draadloze netwerken kan communiceren heeft wel een keerzijde. Ook het aantal en de omvang van bedreigingen is sterk toegenomen. Denk aan hacking, virussen, spyware, spam, enzovoorts. Hacking is verworden van een obscure hobby van gespecialiseerde nerds tot een activiteit voor ‘script-kiddies’, oftewel iedereen die de moeite neemt om de handleidingen voor hacking op Internet op te zoeken. Daarnaast is hacking ook een zaak van nationale veiligheid en dus van inlichtingendiensten geworden. Oorlogvoering vormt zich geleidelijk om van fysiek geweld tot digitaal geweld. Het bijbehorende onderzoeksdomein staat bekend onder de naam ‘information operations’, maar is informeel ook wel bekend als ‘cyber warfare’. Professionele hackers spelen hierin een belangrijke rol. Er gaan miljarden om in digitale spionage en ontregeling van vijandelijke netwerken. Eén van de bekendste spionagesystemen is het Echelon-netwerk, dat na alle publicaties erover ineens niet meer zo geheim was. Oorspronkelijk is dit wereldomvattende netwerk opgezet door de Verenigde Staten en enkele bevriende landen om wereldwijd digitale communicatie, waaronder telefoon en e-mail, af te tappen en te onderzoeken op zaken die de nationale veiligheid van de initiatiefnemers aan kunnen tasten. Eenmaal opgezet konden de beherende partijen de verleiding echter niet weerstaan om de afgetapte informatie ook

voor andere doelen te gebruiken. Het is weliswaar nooit goed bewezen, maar er zijn sterke vermoedens dat onder meer strategische informatie van de Europese vliegtuigbouwer Airbus doorgesluisd is naar de Amerikaanse vliegtuigbouwer Boeing.

Digitale informatie is niet meer uit onze maatschappij weg te denken. Voor elke organisaties is al dan niet digitale informatie, naast personeel, het belangrijkste bedrijfsmiddel. Ernstige verstoring van de informatiestromen kan een organisatie slechts zeer korte tijd doorstaan. Het beveiligen van informatiesystemen en informatie is daarmee een onontkoombare zaak geworden. Maar aangezien de verschillende bedrijfsmiddelen, te weten personeel, materieel, financiën en informatie, een samenhangend geheel vormen, is het beveiligen van informatiesystemen en informatie niet los te zien van het beveiligen van de andere bedrijfsmiddelen. Bovendien is er ook een interactie tussen beveiliging en productie – sterkere beveiliging gaat namelijk ten koste van productie en vice versa. Hierdoor zijn beveiliging en productie ook niet los van elkaar te zien. De beveiliging van de bedrijfsmiddelen, waaronder informatiebeveiliging, staat dan ook niet op zichzelf, maar is een integraal onderdeel van de bedrijfsvoering. Dit klinkt logisch, maar in veel organisaties is men zo gericht op het behalen van productiedoelen en het ontwikkelen van persoonlijke carrières, dat de onmisbare ondersteunende processen, zoals informatiebeveiliging, in het gedrang komen. De prioriteit, van met name het management, ligt dan niet bij deze ondersteunende processen. In zulke situaties zijn informatiebeveiligers goed te vergelijken met Don Quichot, vechtend voor een verloren zaak. Als de organisatie, te beginnen bij het management, nog niet toe is aan informatiebeveiliging, dan is de functie van informatiebeveiliger een zeer ondankbare en kan informatiebeveiliging nooit goed van de grond komen.

Het feit dat informatiebeveiliging geïntegreerd is – of zou moeten zijn – in de bedrijfsvoering, terwijl voor informatiebeveiliging ook nog veel specifieke specialistische kennis nodig is, maakt het tot een complexe en veelzijdige discipline. Informatiebeveiliging vraagt een gedegen kennis van technische onderwerpen, zoals bijvoorbeeld wiskunde, natuurkunde, informatica, telematica en elektrotechniek, maar ook van niet-technische onderwerpen, zoals bijvoorbeeld bedrijfskunde, communicatiekunde, rechten, economie en psychologie.

Het domein van informatiebeveiliging is zo breed, dat we binnen het lectoraat twee thema's gekozen hebben waarop we de nadruk zullen gaan leggen, namelijk:

- *Netwerkbeveiliging*, oftewel het beveiligen van computernetwerken, waaronder zowel Internet als netwerken voor draadloze communicatie.

- *Het organiseren van informatiebeveiliging*, oftewel het inrichten van de informatiebeveiliging en het inbedden hiervan in de bedrijfsvoering.

Netwerkbeveiliging

Het eerste thema van het lectoraat, netwerkbeveiliging, is het meest technische thema. Binnen dit thema draait het om informatie- en communicatietechnologie, oftewel ICT. Steeds meer ICT-componenten, zoals bijvoorbeeld computers, worden met elkaar verbonden via netwerken. Waar eerst nog sprake was van netwerken binnen organisaties, worden in toenemende mate netwerken van verschillende locaties, of zelfs van verschillende organisaties, aan elkaar gekoppeld, al dan niet via publieke netwerken zoals Internet. Internet is te beschouwen als de 'openbare weg' van netwerkland. Organisaties die hun eigen netwerk aan Internet koppelen, kunnen op die manier relatief eenvoudig en goedkoop wereldwijd communiceren met andere vestigingen, leveranciers, klanten en overheden. Bovendien kunnen thuiswerkers via Internet toegang krijgen tot de eigen bedrijfsinformatie die anders alleen vanuit het interne netwerk te benaderen zouden zijn. Maar, zoals Johan Cruijf pleegt te zeggen: "elk voordeel hep z'n nadeel". Internet gedraagt zich namelijk echt als een openbare weg; dat wil zeggen, dat iedereen zich daar vrijelijk over kan verplaatsen. Dus ook de vandalen van netwerkland, de hackers. Alle hackers op de wereld kunnen zomaar aankloppen bij elk op Internet aangesloten bedrijfsnetwerk. Elke zichzelf respecterende organisatie die aan Internet gekoppeld is, heeft dan ook een firewall geïnstalleerd om als een portier bij de voordeur al het netwerkverkeer tussen het interne netwerk en Internet te controleren en hackers buiten te houden. Vanwege die grootschalige toepassing wordt een firewall steeds meer beschouwd als een standaardproduct dat kant en klaar gekocht of gehuurd wordt. Hoewel het instellen en onderhouden van een firewall nog niet altijd zo eenvoudig is als men voor een standaardproduct mag verwachten, hebben we daarin de afgelopen jaren wel duidelijke verbeteringen zien ontstaan.

Echter, hoe nuttig een firewall ook is, de beveiligingende werking ervan is beperkt. De belangrijkste beperking is dat de firewall het langskomende verkeer slechts beperkt kan controleren. Een firewall functioneert als een sluis tussen het interne netwerk en Internet, waar al het ingaande en uitgaande verkeer langs komt. Als een waterdichte controle hiervan al mogelijk zou zijn, dan zou het veel te veel tijd vergen. Om de verkeerscapaciteit niet al te ongunstig te beïnvloeden, controleert een firewall daarom

slechts een beperkt aantal aspecten van het langskomende verkeer. Hierdoor ontstaat echter wel een zwakke plek in de beveiliging die door hackers misbruikt kan worden om op het interne netwerk in te breken.

Een andere beperking van de firewall wordt niet zozeer bepaald door de firewall zelf, maar door de plaats ervan. Een firewall kan namelijk alleen beschermen tegen ongewenst verkeer van buiten (het Internet). De eigen medewerkers, die direct toegang hebben tot het interne netwerk, hoeven voor hun activiteiten helemaal niet door de firewall. Uit verschillende onderzoeken blijkt echter dat juist de eigen medewerkers in het algemeen voor de grootste problemen zorgen. Weliswaar is het leeuwendeel van de intern veroorzaakte problemen gestoeld op fouten en vergissingen te goeder trouw, maar ze leiden toch tot verstoringen.

Een organisatie met een eigen netwerk heeft naast de firewall andere maatregelen nodig die de werking van de firewall aanvullen. Het intrusion detection systeem (IDS) is zo'n maatregel. Als we de firewall beschouwen als de portier die iedereen controleert die naar binnen of naar buiten wil, en zonodig ongewenste individuen tegenhoudt, dan kunnen we het IDS beschouwen als het inbraakalarm dat afgaat op het moment dat er een indringer gesignaleerd wordt. Bovendien kan het IDS ook ongewenste activiteiten van eigen medewerkers op het interne netwerk detecteren.

De ontwikkeling van intrusion detection systemen staat nog in de kinderschoenen. De probleemstelling is dan ook complexer dan deze op het eerste gezicht lijkt. Ten eerste moet een IDS een aanzienlijke verwerkingscapaciteit hebben. Vooral als het gebruikt wordt voor het netwerk van een grote organisatie die haar netwerk intensief gebruikt. Het systeem moet dan al het langskomende netwerkverkeer aftappen en analyseren om direct na een verdachte activiteit alarm te kunnen slaan. Dit vergt nogal wat van het IDS. Ten tweede is het niet eenvoudig om ongewenst netwerkverkeer te onderscheiden tussen een gigantische hoeveelheid gewoon netwerkverkeer. Eenvoudige aanvallen die uitgevoerd worden door onervaren hackers, de script-kiddies, zijn weliswaar relatief eenvoudig te detecteren. Maar het detecteren van professionele hackers is een ander verhaal. Deze doen er juist alle moeite voor om hun aanvalsactiviteiten te verbergen in de ruis van het gewone netwerkverkeer.

Aanvallen van script-kiddies zijn te detecteren met behulp van zogenaamde 'handtekeningen'. Dit mechanisme vertoont een sterke analogie met de detectie van computervirussen. Virussen worden door antivirus-software herkend door verdachte bestanden te vergelijken met karakteristieke patronen van bekende virussen. Analoog

worden aanvallen van hackers door een intrusion detection systeem herkend door verdacht netwerkverkeer te vergelijken met karakteristieke patronen van bekende aanvallen. Deze aanpak werkt echter alleen bij bekende aanvallen; nieuwe aanvallen worden niet herkend en kunnen dus ongestoord uitgevoerd worden. En daar zit nou het probleem voor het detecteren van professionele hackers, die juist zo min mogelijk gebruik maken van bestaande technieken.

Het alternatief voor het gebruik van 'handtekeningen', is statistische analyse van het netwerkverkeer om zo aanvallen te detecteren. Het uitgangspunt daarbij is dat een IDS kan bepalen welk netwerkverkeer normaal is. Als er dan afwijkingen gedetecteerd worden ten opzichte van het normale verkeer, dan wijst dat op verdachte activiteiten. Het ontwerpen en implementeren van dergelijke technieken is echter veel complexer dan het gebruik van handtekeningen. Er is nog relatief weinig publiek toegankelijk onderzoek gedaan naar dit onderwerp en dat is terug te zien in het beperkte aantal publicaties hierover. Toch wordt ook het inzetten een IDS binnenkort een standaardmaatregel, net als het inzetten van een firewall. Het is dan nodig dat er meer kennis beschikbaar is over intrusion detection. Met name kennis over geavanceerde technieken voor statistische analyse van netwerkverkeer. Het lectoraat kan daaraan bijdragen zonder direct in vraagstellingen voor fundamenteel onderzoek te duiken.

Netwerkbeveiliging richt zich op meer zaken dan alleen firewalls en intrusion detection systemen. Het richt zich op het opsporen van allerlei bedreigingen met betrekking tot netwerken en het ontwerpen van oplossingen hiervoor. Andere onderwerpen zijn bijvoorbeeld het verbeteren van de beschikbaarheid van netwerken, het implementeren van technieken ten behoeve van opsporingsinstanties, enzovoorts. Het lectoraat heeft echter binnen netwerkbeveiliging als primaire aandachtsgebied het beveiligen van netwerken tegen personen die ongeoorloofde activiteiten willen ontplooien op het netwerk. Dit aandachtsgebied gaat overigens ook verder dan firewalls en intrusion detection systemen. Hieronder vallen bijvoorbeeld ook het toepassen van veiliger netwerkprotocollen, zoals IPsec en IP versie 6, en ook het analyseren en beveiligen van draadloze netwerken.

Overigens levert het beveiligen van netwerken met allerlei goede beveiligingsmaatregelen nog niet zondermeer veilige netwerken op. Ook al zijn de maatregelen op zich nog zo sterk, de totale sterkte wordt bepaald door de samenhang en de compleetheid van de maatregelen. Bovendien worden alle maatregelen geselecteerd, ingericht en onderhouden door mensen. De wijze waarop de mensen omgaan met

netwerkbeveiliging is daarom minstens zo belangrijk als de toegepaste technieken voor beveiliging. Daarmee komen we op het terrein van het volgende thema.

Het organiseren van informatiebeveiliging

Het tweede thema van het lectoraat is het *organiseren* van informatiebeveiliging. In tegenstelling tot het thema netwerkbeveiliging is dit thema nauwelijks technisch te noemen. In dit thema gaat het over mensen en organisaties. Informatiebeveiliging komen we dan ook overal tegen; het is eigenlijk een zeer alledaags fenomeen. Wat doet u als u in gezelschap iets vertrouwelijks tegen iemand anders wil zeggen? Waarschijnlijk fluistert u de boodschap. Of u neemt de ander even mee naar een rustig plekje. In zo'n geval doet u aan informatiebeveiliging. En dit is nog maar één soort informatie, namelijk mondelinge informatie, die beschermd werd tegen één soort bedreiging, namelijk afluisteren. Andere plaatsen waar u informatiebeveiliging zoal tegenkomt zijn de handtekening onder een document, het inloggen met een wachtwoord op een computer, de bankpas met pincode voor geldautomaten, enzovoorts. Hoe alledaags informatiebeveiliging ook is, het is bepaald niet eenvoudig. Sterker nog, in een organisatie van enige omvang is het goed inrichten van informatiebeveiliging een uitdaging van formaat. Voor een groot deel wordt dit juist veroorzaakt doordat er mensen bij betrokken zijn. Mensen zijn niet weg te denken uit de bedrijfsprocessen. Zij zijn een cruciaal element in elk bedrijfsproces. Maar aan de andere kant vormen de mensen ook een belangrijke bedreiging voor die processen. Mensen blijken vaak de zwakste schakel van de spreekwoordelijke ketting te zijn. Hoe onbetrouwbaar apparatuur en programmatuur ook mogen zijn, gemiddeld genomen zijn mensen nog onbetrouwbaarder. En dat komt in het algemeen *niet* door het ontbreken van goede wil. Nee, ondanks alle goede wil maken mensen fouten, veel fouten. Het grote aantal spreuken en gezegdes dat als onderwerp menselijk falen heeft, spreekt boekdelen.

Hoewel in deze lijst zowel opzettelijk als onopzettelijk falen voorkomen, worden in de praktijk de meeste problemen veroorzaakt door onopzettelijk falen, door zaken als onoplettendheid, onvoorzichtigheid en onwetendheid. Het aantal opzettelijk veroorzaakte incidenten, door bijvoorbeeld diefstal, oplichting, fraude en hacking is relatief klein, maar daar staat tegenover dat de schade per incident veel groter kan zijn. Beide oorzaken, onopzettelijk en opzettelijk falen, zadelen de organisatie met een aanzienlijke schadepost op. Mensen zijn dan ook de grootste bedreiging voor een organisatie. En van alle incidenten die door mensen veroorzaakt worden, komt het leeuwendeel voor rekening van de eigen medewerkers. Dus eigenlijk kunnen we stellen dat de medewerkers van een organisatie de grootste bedreiging zijn.

Er treedt nu echter een flinke complicatie op. De medewerkers van een organisatie zijn de grootste bedreiging. Maar daar staat tegenover dat informatiebeveiliging vooral mensenwerk is, werk waarin de medewerkers van de organisatie de hoofdrol spelen. De medewerkers zijn dus niet alleen de belangrijkste bedreiging, maar ook de remedie. Oftewel: *informatiebeveiliging is dat medewerkers maatregelen treffen tegen hun collega's!* Dit levert natuurlijk wel een spanningsveld op. Collega's hebben elkaar nodig en willen elkaar graag vertrouwen en het treffen van beveiligingsmaatregelen tegen elkaar past daar niet zo goed bij. Het is dan ook van uitermate groot belang om binnen een organisatie alleen de noodzakelijke maatregelen te treffen en de noodzaak daarvan bovendien erg goed uit te leggen. De voortrekkersrol hiervan ligt in eerste instantie bij het management en *niet* bij de informatiebeveiligingsfunctionaris, de security manager, of iemand met een soortgelijke functie.

Het management trekt de kar. Zij formuleert de regels voor informatiebeveiliging (het beleid), brengt die voldoende onder de aandacht en bewaakt de naleving ervan. Het beleid voor informatiebeveiliging staat overigens niet op zichzelf, maar moet aansluiten op het overige bedrijfsbeleid. Hierdoor kan informatiebeveiliging een geïntegreerd onderdeel van de bedrijfsvoering worden. Het beleid voor informatiebeveiliging is de basis voor de selectie van beveiligingsmaatregelen en de implementatie ervan, maar ook voor het toewijzing van verantwoordelijkheden op het gebied van informatiebeveiliging.

Het toewijzen van verantwoordelijkheden op het gebied van informatiebeveiliging klinkt eenvoudig en is dat in feite ook. Maar desondanks gaat dat daarbij nog wel eens mis. Het toewijzen van verantwoordelijkheden is zinloos als de betreffende verantwoordelijkheden niet opgepakt worden, of niet uitgevoerd kunnen worden. En daar wringt het in veel organisaties. Het management, medewerkers en beveiligingsfunctionarissen beschuldigen elkaar van onkunde, laksheid en verkeerde prioriteiten. En als er dan een incident gebeurt, dan spelen ze elkaar de zwartepiet toe. Als buitenstaander kun je je afvragen wie er eigenlijk gelijk heeft. Zonder in te gaan op specifieke situaties, zijn er wel trends te onderkennen. In tegenstelling tot de gangbare opvatting, valt het merendeel van de medewerkers in het algemeen weinig te verwijten. Er zijn altijd dwarsliggers, maar dat zijn uitzonderingen. De meeste fouten en vergissingen worden veroorzaakt door slechte procedures, of door het toewijzen van beveiligingstaken aan de verkeerde mensen. We kunnen dan ook stellen dat de meeste beveiligingsproblemen te herleiden zijn tot organisatorische fouten, waar we het management op aan kunnen spreken. Datzelfde management dat wel meer steken laat vallen. Veel managers hebben nog niet helemaal door wat het fenomeen integraal management voor hun betekent. Een manager is

daarbij niet alleen verantwoordelijk voor de productie of de dienstverlening, maar ook voor de daarvoor benodigde ondersteunende zaken. Dit betekent dat ook informatiebeveiliging op het bordje van die manager ligt. Als dat besef in alle organisaties doordringt, dan zou informatiebeveiliging een stuk beter af zijn. Aan de andere kant komt de manager die wel integraal management op informatiebeveiliging toepast voor een lastig dilemma te staan: hoe meer je aan informatiebeveiliging doet, hoe minder incidenten er optreden. Maar hoe weet je dan dat het wegblijven van de incidenten niet op toeval berust, dus gewoon een kwestie van statistiek is? Is alle beveiliging dan geen pure verspilling geweest? Deze vragen zijn door veel managers niet zonder meer te beantwoorden en dat heeft in het algemeen een ongunstig effect op hun motivatie om veel tijd en moeite in informatiebeveiliging te steken.

Hoe slecht informatiebeveiliging bij het management ook tussen de oren kan zitten, zij zijn niet de enigen waarbij het mis gaat. Op andere plaatsen in de organisatie gaat het ook vaak mis, ook op een plaats waar je het niet direct verwacht, namelijk bij de beveiligingsfunctionarissen. Zij zijn vaak zo gericht op de maatregelen, dat ze de mens in de organisatie nogal eens uit het oog verliezen. In al hun enthousiasme voor beveiliging nemen ze gauw te veel of te zware maatregelen en besteden te weinig tijd aan het uitleggen en organiseren ervan. Dit kan leiden tot een overdaad aan maatregelen (en we weten dat "overdaad schaadt") en tot maatregelen waarvan het nut niet duidelijk is voor degenen die er mee moeten werken. Voor een deel wordt dit veroorzaakt doordat beveiligingsfunctionarissen veel weten over bedreigingen en maatregelen. Kennis hierover zouden ze meer moeten delen met de rest van de organisatie.

Wat kunnen we hieruit leren? Ten eerste dat de problemen op het gebied van informatiebeveiliging ontstaan op verschillende plaatsen in de organisatie en zelfs voorkomen in de hoek waar de meeste kennis over informatiebeveiliging zit. Blijkbaar gaat het niet om de hoeveelheid kennis, maar om soort kennis. Een bepaalde kenniscomponent, namelijk kennis over de menselijke factor, is te veel onderbelicht. Het hoger onderwijs kan hierop inspelen door informatiebeveiliging aan te bieden als een multidisciplinair vak, waarin menselijke aspecten in belangrijke mate vertegenwoordigd zijn. Dit kan ingevuld worden door studenten in technische opleidingen uitgebreider kennis te laten maken met de zogenaamde 'zachte aspecten' van informatiebeveiliging, terwijl studenten in niet-technische opleidingen meer de 'harde aspecten' van informatiebeveiliging krijgen. Daarnaast moet in beide ook voldoende aandacht geschonken worden aan andere organisatorische zaken, zoals het inrichten van de organisatie voor informatiebeveiliging, taken en functies, het afstemmen van activiteiten

voor informatiebeveiliging onderling en met andere activiteiten, het opsporen van onacceptabele risico's, standaardisatie in methoden en technieken, enzovoorts.

Tevens kan het hoger onderwijs een rol spelen in verder onderzoek naar de menselijke aspecten in relatie tot informatiebeveiliging. Hoewel er binnen de sociale disciplines veel kennis op het gebied van menselijk gedrag is, is er binnen de informatiebeveiliging nog steeds een dringende behoefte om die kennis daar toepasbaar te maken. Zo is het bijvoorbeeld nog steeds niet helemaal duidelijk onder welke voorwaarden beveiligingsopleidingen, -trainingen en -bewustzijnscampagnes effectief zijn. Nader onderzoek naar de menselijke factor in de informatiebeveiliging is dus nodig. Het lectoraat kan hierin een rol spelen, in samenwerking met het beroepsveld.

Kenniskring

Aan het lectoraat is een Kenniskring Informatiebeveiliging verbonden. De leden van deze kenniskring zijn docenten van de Hogeschool die deskundig zijn op het gebied van informatiebeveiliging. Hoewel het lectoraat pas in september jl. van start is gegaan, kan ik u de heugelijke mededeling doen dat zich nu al enkele docenten aan de kenniskring hebben kunnen en willen verbinden. Ik kan u zelfs hun namen geven. Het gaat om Cobie van der Hoek, Leo van Koppen en Pieter Burghouwt. Op de fotogallerij kunt u zien over wie ik het heb. Ze zijn vandaag alledrie aanwezig, dus ik nodig u uit om na deze rede met hen van gedachten te wisselen over de ins en outs van informatiebeveiliging.

Naast de kenniskring is extra deskundigheid beschikbaar vanuit de Klankbordgroep Informatiebeveiliging. Ook voor deze groep hebben zich al verscheidene docenten bereid verklaard om daarin zitting te nemen. Er zit nog te veel beweging in de samenstelling van de klankbordgroep om u vandaag al de namen van de bemanning te geven, maar op de nog door ons in te richten website zullen we zo spoedig mogelijk ook de leden van deze groep aan u voorstellen.

Doelstellingen lectoraat

Informatiebeveiliging is heden ten dage een serieus vakgebied met eigen onderzoek, eigen literatuur en eigen opleidingen. Het vakgebied kent inbreng vanuit vele andere vakgebieden, en speelt zelf weer een rol van betekenis binnen die andere vakgebieden. Dit betekent dat het vak informatiebeveiliging multidisciplinair ingevuld moet worden en bovendien dat het vak een plaats moet krijgen binnen de opleidingen waar het relevant is. En dat zijn niet alleen de informaticaopleidingen, maar ook bijvoorbeeld bedrijfskunde,

wiskunde, elektrotechniek, economie en rechten. Samenwerking tussen het lectoraat en deze opleidingen is noodzakelijk.

De leden van de kenniskring en ik hebben ons ten doel gesteld om in samenwerking met verschillende opleidingen binnen en buiten de Hogeschool het onderwerp informatiebeveiliging binnen het onderwijs te versterken. Dit betekent dat er nieuw onderwijs ontwikkeld zal worden en dat meer studenten kunnen afstuderen in informatiebeveiligingsonderwerpen.

Daarnaast zullen wij onderzoek opstarten, met name op het gebied van toepassingsgerichte informatiebeveiligingsvraagstukken. Hierbij zullen we samenwerking zoeken met andere partijen die geïnteresseerd zijn in dat onderzoek. We streven er naar om een kenniscentrum voor de Haagse regio te worden op het gebied van informatiebeveiliging.

U merkt het al, wij hebben grote plannen. Toch kunnen wij geen ijzer met handen breken, dus we zullen onze ambities realistisch moeten houden. Maar ik kan u verzekeren: u hoort nog van ons!

Dankwoord

En daarmee ben ik aan het einde van deze rede gekomen. Ik wil via deze weg al degenen bedanken die het mogelijk hebben gemaakt dat ik hier nu sta. Vrienden, familie en collega's, dank voor alle inspiratie, ondersteuning en advies binnen het werk, maar zeker uit daarbuiten. In het bijzonder wil ik mijn ouders bedanken, die letterlijk aan de wieg van mijn loopbaan hebben gestaan. En natuurlijk mijn vrouw Marian en mijn zoons Daniël en Laurens, die daarbinnen hoofdrollen spelen.

Dank u voor uw aandacht.

Marcel Spruit
3 december 2003.