

De bijdrage van IT-leveranciers aan informatiebeveiliging

Prof. Dr. Ir. R. Paans

THEMA

1 Inleiding

Het beveiligen van persoonlijke en zakelijke eigendommen is een zeer oud probleem, waarmee onze verre voorouders reeds worstelden. De oudste koningsgraven en piramiden in Egypte, sommige bijna 3.000 jaar voor onze jaartelling gebouwd, zijn de nog steeds zichtbare symbolen van de reeds lang geleden onderkende beveiligingsproblematiek. Van oudsher trachtte men zaken te beschermen die tastbaar en zichtbaar waren. In de vijftiger jaren van onze eeuw, met de introductie van de eerste computers, is hieraan een nieuwe dimensie toegevoegd. Namelijk, hoe beschermt men een eigendom in de vorm van met het oog niet waarneembare gegevens en programmatuur opgeslagen op een magnetisch of optisch medium of tijdens transport via een kabel of door de lucht? Deze kunnen worden gemodificeerd of gekopieerd zonder sporen na te laten. Met de huidige snelle proliferatie van grote, middelgrote en kleine computersystemen binnen alle sectoren van onze maatschappij, inclusief de huiselijke omgeving, neemt de ernst van deze problematiek in een hoog tempo toe. Velen die gebruik maken van de computer of van netwerken ontdekken hoe kwetsbaar zij worden voor opzettelijke of onopzettelijke verstoringen, en hoe zoiets hun eigen functioneren kan beïnvloeden. Dit kan lopen van een Raad van Bestuur, die wordt geconfronteerd met een ernstige fraudezaak door manipulatie van

digitale gegevens, tot een particulier die wordt getroffen door een virusinfectie in een persoonlijk systeem.

Informatiebeveiliging krijgt in toenemende mate aandacht binnen de overheid en het bedrijfsleven. Hierbij blijkt dat voor de grotere omgevingen met de traditionele mainframe-computers veel beveiligingsmiddelen en kennis is te verkrijgen. Maar voor de decentrale omgevingen, met name voor de persoonlijke werkstations en de daar gebruikte netwerken, wordt men geconfronteerd met een gemis aan adequate ondersteuning door de leveranciers van de apparatuur en programmatuur. De leveranciers zien de beveiligingsproblematiek daar primair als een verantwoordelijkheid van hun klanten. Natuurlijk, tegen additionele prijzen wordt er wel iets geleverd, maar veelal heeft de gebruiker de perceptie dat men zelf het wiel dient uit te vinden.

De toenemende aandacht leidt tot het ontwikkelen van standaarden, eventueel binnen de eigen organisatie, maar bij voorkeur op een meer overkoepelend niveau. Deze activiteiten bevinden zich veelal nog in een prematuur stadium, maar de eerste resultaten beginnen zichtbaar te worden en een draagvlak te krijgen. In dit artikel worden enkele voorbeelden besproken, zonder daarbij uitputtendheid na te streven.

2 De klassieke visie van leveranciers

Bij een kritische beschouwing van de rol van de leveranciers mag men hun primaire doelstelling niet uit het oog verliezen. Dat is het leveren van de mogelijkheid om effectief en efficiënt gegevens te verwerken en te transporteren. Het zwaartepunt

Prof. Dr. Ir. R. Paans RE was gedurende 10 jaar werkzaam voor IBM, onder andere als Corporate Programs manager bij IBM Europa. Sinds 1990 is hij hoogleeraar EDP-auditing aan de Vrije Universiteit en sinds 1994 directeur bij KPMG EDP Auditors te Amstelveen.

van hun ontwikkelingsactiviteiten is hier van oudsher op gericht geweest. Zo ging het om de ontwikkeling van steeds snellere processoren en grotere geheugens tegen de door de markt gewenste lage prijzen, relatief goedkope programmatuur waarmee men op gebruikersvriendelijke wijze effectief kan werken, en een betaalbare koppeling van iedereen aan wereldomspannende netwerken. Dat was waar de klant om vroeg en waar de klant voor betaalde. Dat daarnaast de vertrouwelijkheid, integriteit en beschikbaarheid moesten worden gewaarborgd, had bij de klant niet altijd de hoogste prioriteit. Dit gebrek aan een groot marktpotentieel en een hoge omzet heeft logischerwijs gevolgen voor de prioriteitsstelling van de leveranciers. De massaverkopen liggen in het vlak van functionaliteit, terwijl de met beveiligingsapparatuur en -programmatuur te behalen omzetten veelal marginaal zijn.

2.1 Grote omgevingen

De aandacht van de leveranciers voor informatiebeveiliging is verschillend per omgeving. Zo ziet men in de markt van de grote omgevingen, de traditionele mainframes, reeds aan het einde van de zeventiger jaren een beperkte omslag. Op dat moment vroegen overheidsinstanties en grote bedrijven om integriteit als een van de kwaliteitskenmerken van hun grote informatiesystemen. Zo een integriteit vraagt een basis binnen de harde kern, namelijk de apparatuur en besturingsprogrammatuur. Op 21 oktober 1981 kwam IBM, daarbij gedreven door de markt, met een verklaring op dit gebied. Dit was het 'Statement of MVS system integrity', gericht op de computers met het Multiple Virtual Storage (MVS) besturingssysteem. Het luidt:

'At the time the MVS system control program became available, it was stated that all known system-integrity exposures had been removed from MVS. That statement was based on IBM's knowledge of system-integrity exposures at that time. Because it is not possible to certify that any system has total integrity, it was expected that additional exposures should come to light. Therefore, it was also stated that customers' complaints describing additional exposures would be accepted.'

Deze nog steeds geldige verklaring bevat een aantal interessante aspecten. Zo bevestigt men dat er lekken waren in de beveiliging, die men heeft

opgeheven voor zover deze bekend waren bij de ontwerpers. De formulering impliceert dat men een - achteraf terecht gebleken - vermoeden had dat er nog meer lekken bestonden. Daarnaast stelt men dat geen enkel systeem waterdicht is, hetgeen gezien de omvang van de besturingssystemen niemand zal verrassen. Een besturingssysteem van rond de 20 miljoen machine-instructies, over een periode van ruim dertig jaar gegroeid dankzij de inspanning van generaties aan programmeurs, kan nooit geheel vrij van fouten zijn. Daarnaast is het luisteren naar klachten van de klanten de enige echte garantie die wordt gegeven. Zodra een klant een beveiligingslek tegenkomt en dat gedocumenteerd onder de aandacht van de leverancier brengt, wordt actie ondernomen.

Bij zo een actie ontstaat een moeilijk dilemma. Stel dat van het betreffende besturingssysteem er wereldwijd enige tienduizenden licenties zijn verstrekt. Daarbij blijkt dat veel van de klanten wat achter lopen met onderhoud, oftewel te laat tot veel te laat zijn met het aanbrengen van de door de leverancier voorgestelde updates van de programmatuur. Hoe licht men nu deze klanten in dat er een serieus beveiligingslek is dat reparatie behoeft. Een groot deel van de klanten zit namelijk nog niet op het onderhoudsniveau dat voor de reparatie is vereist, en zodra men iets bekend maakt kunnen minder eerlijke gebruikers misbruik maken van het gesignaleerde lek. IBM loste dit op door periodiek de reparaties voor besturingssystemen aan de klanten toe te zenden, inclusief de reparaties voor beveiligingslekken, zonder in detail bekend te maken voor welk probleem deze laatste waren bedoeld. Op zich is dit een risico, aangezien de klant dan de urgentie van het aanbrengen van de update niet zal onderkennen. Binnen IBM loste men dit dilemma op via een apart communicatiekanaal, opgezet door de eigen beveiligingsdeskundigen, waarbij men de reparaties voor lekken classificeerde in een aantal categorieën, en voor de meest dringende updates bindende implementatieperioden voorschreef. Periodiek werd deze lijst met updates en hun urgentie doorgegeven aan de interne rekencentra, om zo zorg te dragen voor tijdige implementatie.

Zo een benadering werkt alleen bij een strak geleid bedrijf, waar de integriteit en vertrouwelijkheid een duidelijke prioriteit hebben bij het verantwoordelijke management. Als men dit

vergelijkt met vele andere organisaties, ziet men dat het in de lucht houden van bestaande informatiesystemen en het starten van nieuwe systemen vaak hogere prioriteit heeft dan het nastreven van het meest recente onderhoudsniveau. Hierbij past de kanttekening dat sommige organisaties jaren achter lopen met hun onderhoudsniveau, vooral doordat hun aandacht op functionaliteit en kosten-beheersing is gericht. Daardoor komt het aanbrengen van reparaties voor lekken in het gedrang, zo men deze al als urgent onderkent.

Leveranciers zijn niet scheutig met het verstrekken van informatie over beveiligingsproblemen, mede omdat men niet te veel onrust wil veroorzaken binnen de organisaties van hun klanten. Daarnaast speelt het dilemma dat verstrekte informatie kan worden misbruikt door kwaadwilligen, met name bij die systemen waar de systeembeheerders de bekendgemaakte lekken nog niet hebben kunnen sluiten.

2.2 Decentrale omgevingen

De laatste jaren hebben de decentrale omgevingen een gigantische groei doorgemaakt. Bijna iedere organisatie kent intern een spinnenweb van Local Area Networks (LANs), gekoppeld via Wide Area Networks (WANs) en met vele verbindingen naar van alles en nog wat. Overal ziet men lokale gegevensopslag- en verwerkingseenheden, de servers, en grote aantallen lokale werkstations. Dit wordt aangevuld met vele draagbare laptops, uitgerust met steeds grotere schijfeenheden, en imposante aantallen modems om via telefoonlijnen verbindingen op te bouwen. Voor de hiermee ontstane olievlek aan beveiligingsproblemen weet nog niemand een goede oplossing.

Een van de meest urgente problemen wordt veroorzaakt door het draagbare karakter van de moderne systemen. Een bureau-model workstation kan zo worden opgepakt, inclusief alle daarin opgeslagen gegevens. Hetzelfde geldt voor de laptops, die men vaak onbeheerd op bureaus, in auto's of thuis ziet rondslingeren. Soms zitten deze systemen boordevol met gevoelige gegevens in de vorm van vertrouwelijke documenten en persoonsgebonden informatie. Men zou verwachten dat de leveranciers deze problematiek onderkennen, en al deze systemen uitrusten met gedegen versleutelmechanismen en authenticatietechnie-

ken, maar niets is minder waar. Binnen de overgrote meerderheid der organisaties worden deze systemen gebruikt zonder enige vorm van beveiliging of met ten hoogste een eenvoudig te breken wachtwoord bij het inschakelen. De gevolgen waren voorspelbaar. Momenteel worden veel van deze systemen of de bijbehorende opslagmedia (CD's, diskettes, enz.) gestolen en niemand weet wat er daarna met de gevoelige gegevens gebeurt. Hooguit als het diskettes van een officier van justitie betreft, komt deze informatie na onduidelijke omwegen prominent in het nieuws. Maar veel meer informatie verdwijnt in een grijs circuit, waarbij men naar de wijze van gebruik (of misbruik) slechts kan gissen.

Door gebrek aan een basisbeveiliging binnen deze draagbare systemen, op een voldoende hoog niveau van effectiviteit, moeten de klanten nu zelf op zoek naar aanvullende beveiligingsapparatuur en/of -programmatuur. Dit vereist een selectieproces, extra kosten en training, en een proces van het bewustmaken van de gebruikers. Deze moeten worden aangemoedigd de overhead voor het beveiligen te accepteren, en inderdaad alle gevoelige informatie te beschermen via bijvoorbeeld versleuteling. Zolang deze vorm van beveiliging optioneel is en door de gebruiker als een vermijdbare last wordt ervaren, mag men geen te hoge verwachtingen hebben. Voor de leveranciers ligt hier nog een terrein braak, om deze decentrale systemen standaard met een afdwingbaar beveiligingsmechanisme uit te rusten om zo de risico's van ongewenste onthulling van gevoelige informatie bij diefstal van draagbare systemen te minimaliseren. De techniek bestaat en is relatief goedkoop in te passen, maar commerciële overwegingen vormen momenteel blijkbaar nog een te hoge drempel.

Een ander minder ernstig, maar wel irritant, probleem vormen de virus-programma's. Dit zijn zichzelf reproducerende programma's die zichzelf nestelen in programma's of zelfs in elektronische documenten, en via diskettes en netwerken met uit te wisselen programma's en gegevens mee reizen. Indien de persoonlijke werkstations en laptops in een bedrijf eenmaal zijn besmet, is het een kostbare en tijdrovende operatie alle kopieën van zo een virus-programma op te sporen en te elimineren. Bij het lezen van vakbladen zoals *Computer Fraud & Security* van Elsevier Science Ltd wordt men

steeds weer verrast door de inventiviteit die de ontwerpers van virussen tonen, en het feit dat het steeds moeilijker wordt om niet met deze ongewenste producten te worden geconfronteerd.

3 Standaarden

Informatiebeveiliging is een combinatie van technische maatregelen in de vorm van apparatuur en programmatuur, en organisatorische maatregelen. Het een kan niet zonder het ander. Men zal via het verstrekken van richtlijnen, bewustwording en training de gebruikers moeten bewegen om de technische maatregelen op de juiste wijze te gebruiken. Inmiddels wordt binnen een aantal organisaties gewerkt aan standaarden voor informatiebeveiliging, zoals op wereldwijd niveau binnen I-4, op Europees niveau binnen European Security Forum (ESF) en in Nederland binnen het Overlegorgaan Technische Beveiligingsstandaarden. Daarnaast worden 'best practices' vastgelegd, bij voorkeur gedragen door een aantal toonaangevende organisaties als een breed geaccepteerde standaard.

3.1 Code voor informatiebeveiliging

Een voorbeeld van een document bedoeld als leidraad voor beleid en implementatie is de Engelse 'Code of practice for information security management', uitgebracht als British Standard BS 7799 (1995). Deze is op basis van praktijkervaringen met informatiebeveiliging opgesteld door de Engelse overheid (Department of Trade and Industry) en het bedrijfsleven, zoals onder andere Shell, Unilever en Sema Groep. Via het ministerie van Economische Zaken is een Nederlandse vertaling gerealiseerd. Deze wordt door het NNI (1994) uitgebracht onder de naam 'Code voor informatiebeveiliging'. Ondanks kritieken op de soms beperkte en soms te vergaande diepgang, is dit boekwerk een praktisch hulpmiddel met een groot aantal aandachtspunten, op een bruikbare wijze gerangschikt (zie ook Roos Lindgreen, 1996, pp. 110-120). Het bespreekt de opzet van een beveiligingsbeleid, de beveiligingsorganisatie en het toezicht. Daarnaast geeft het richtlijnen voor het classificeren en beheren van bedrijfsmiddelen, inclusief gegevens, fysieke en logische toegangsbeveiliging, en ontwikkeling en onderhoud van systemen. Het belangrijkste nadeel is dat de toonzetting toch enigszins is gericht op de

grootschalige omgevingen en er geen duidelijk onderscheid wordt gemaakt naar wat men op realistische wijze binnen de kleinschalige omgevingen dient te realiseren.

Deze leidraad is vooral bedoeld voor de beveiligingsfunctionarissen, die namens de organisatie de risico-analyse uitvoeren en een balans zoeken voor de voor te schrijven maatregelen. Zij dienen lijnmanagement te adviseren over een consistent beleid voor informatiebeveiliging, zonder dat iedere manager zelf naar een lokale oplossing moet zoeken. Bij zo een beleid dient men een voor de organisatie passende balans te vinden tussen enerzijds het belang van de systemen en gegevens (de waarde) en de werkelijke risico's, en anderzijds de verzameling te treffen maatregelen (de kosten). Hierbij dient men te grote risico's door onvoldoende maatregelen en te hoge kosten door een overmaat aan maatregelen te vermijden.

3.2 Technische beveiligingsstandaarden

In 1992 is IBM Corporation een interne werkgroep gestart om de 'best practices' met betrekking tot informatiebeveiliging op papier te zetten. Dit vond plaats onder verantwoordelijkheid van de vice-president voor Information & Telecommunication Services (I&TCS). In deze werkgroep hadden beveiligingsdeskundigen zitting vanuit alle regio's. Vanuit hun ervaring hebben zij twee documenten samengesteld die vergelijkbaar zijn met de bovengenoemde 'Code of practice for information security management', namelijk de IBM-standaarden I&TCS 200 voor mainframes en middelgrote systemen, en I&TCS 201 voor decentrale omgevingen. Naast de algemene richtlijnen voor informatiebeveiliging, stelden de automatiseringsdeskundigen een reeks van appendices samen met een vertaling van de regels naar instellingen binnen de specifieke besturingssystemen. Dat zijn onder andere voor de mainframes Multiple Virtual Storage (MVS), Virtual Machine (VM) en Customer Information Control System (CICS). Voor de middelgrote omgevingen is dat Operating System/400 (OS/400), en voor decentraal onder andere AIX/6000 (IBM-variant op Unix) en OS/2 LAN Server. De appendices vormden een soort kookboek voor de systeembeheerders met eenduidige richtlijnen over hoe alle opties van de besturingssystemen en de logische

toegangsbeveiliging moesten worden ingesteld om veilige omgevingen te verkrijgen. Daarnaast dienden deze documenten als basis voor de controleprogramma's van de EDP-auditors. Dit had als voordeel dat de systeembeheerders vooraf de normen van de EDP-auditors kenden, en hun systemen en organisaties zo konden inrichten dat zij een redelijke kans hadden op een goedkeurende verklaring. Na accordering door de vice-president werden deze regels wereldwijd verplicht gesteld voor de interne rekencentra en voor de overige automatiseringsactiviteiten binnen IBM.

Binnen Nederland is naar voorbeeld van deze IBM-aanpak een overeenkomstige werkgroep opgericht. Dit is het Overlegorgaan Technische Beveiligingsstandaarden (OTB), waarin een aantal interne accountantsdiensten en beveiligingsdeskundigen van overheidsinstanties en uit het bedrijfsleven participeren. Gezamenlijk bundelen zij hun kennis om implementeerbare standaarden te ontwikkelen, die enerzijds zijn bedoeld als een richtlijn voor de systeembeheerder, en anderzijds een basis vormen voor de controle-aanpak van de interne en externe EDP-auditors. Inmiddels zijn de 'exposure drafts' verschenen van de OTB-standaard (1996) 'UNIX' en de OTB-studie (1996) 'Internet', die na ontvangst van alle review-commentaren in het najaar in een definitieve versie worden uitgebracht. Deze documenten zijn een aanvulling op datgene wat de leveranciers van apparatuur en programmatuur leveren. Dat betreft de producten, die ieder op zich een groot aantal vrijheidsgraden kennen voor de instelling van de beveiligingsopties. De leveranciers documenteren de opties, maar geven nauwelijks aan welke combinaties men hoe moet instellen om het gewenste niveau van beveiliging te bereiken. In dit kader vormen deze boekwerken een goede aanvulling, omdat zij voorkomen dat ieder bedrijf zelf het wiel moet uitvinden. Daarnaast geeft het de systeembeheerders een warm gevoel, omdat zij gebruik kunnen maken van kennis van andere instanties en niet meer zelf hoeven te investeren in het opbouwen van die ervaring.

3.3 Industriestandaarden

Een van de bekendste en breed geaccepteerde industriestandaarden voor informatiebeveiliging is het 'orange book' van het Amerikaanse Depart-

ment of Defense (1983). Ondanks de inmiddels hoge leeftijd van dit boek, is de visie van de auteurs vandaag nog steeds relevant en toepasbaar. De richtlijnen hebben betrekking op de 'trusted computing base' (TCB), de kern van ieder informatiesysteem. Deze bestaat uit de apparatuur, het besturingssysteem en de logische toegangsbeveiliging. In feite wordt hiermee een keurmerk gegeven, na toetsing aan de in het boek genoemde normen. Er zijn een aantal klassen gedefinieerd op verschillende niveaus van vertrouwelijkheid en integriteit, waarvan de belangrijkste de klassen C2 en B1 zijn. Bij C2 (discretionary access control) is er sprake van vrijwillige beveiliging, waarbij het systeem de opties biedt en de houders van de gegevens deze opties kunnen gebruiken om hun gegevens en programmatuur te beveiligen. Bij B1 (mandatory access control) is sprake van afgedwongen beveiliging, waarbij de beveiligingsfunctionaris alle gebruikers en gegevens classificeert, en zo de mogelijkheden van de houders beperkt. Hierbij kunnen de houders alleen die personen toegang verstrekken tot hun gegevens die daartoe door de beveiligingsfunctionaris zijn geautoriseerd.

In de loop der tijden is er ook een Europese variant op het orange book samengesteld onder verantwoordelijkheid van de EEG. Dit is Information Technology Security (ITSEC), die echter nooit de status van het orange book heeft gekregen. Momenteel is er sprake van een Amerikaanse en Europese samenwerking om gezamenlijk de opvolger van deze industriestandaard samen te stellen (zie Computer Fraud & Security, mei 1996).

Een beperking van deze standaarden is dat zij alleen betrekking hebben op het product zoals dat door een leverancier wordt geleverd. Men kan dit vergelijken met KEMA-keur voor elektra: indien een contrasteker is goedgekeurd door KEMA weet men dat deze aan bepaalde normen voldoet. Laat men deze echter dagen in de regen buiten liggen, zal er toch kortsluiting optreden. Hetzelfde geldt voor een TCB-keurmerk. Het product is goed, maar het is een open vraag hoe de systeembeheerders en de gebruikers hiermee omgaan. Via de toepassingprogrammatuur, de netwerken, de instellingen, het gebruik van opties en de organisatie kan het basisproduct op een totaal andere manier worden gebruikt dan de bedoeling was van

de ontwerpers, waardoor de effectiviteit van de beveiliging geweldig kan worden aangedaan. In dit kader vormen de Code of practice en de technische beveiligingsstandaarden een goede aanvulling op zo een industrie-keurmerk. Met een combinatie wordt zowel het basisproduct als het gebruik geadresseerd.

4 Ter afsluiting

Informatiebeveiliging is en blijft een uitdagend vakgebied. Enerzijds door de snelle ontwikkelingen in informatietechnologie en de daaruit voortvloeiende bredere integratie van automatisering en datacommunicatie in onze maatschappij. Anderzijds door de uitbreiding van de mogelijkheden tot beveiliging en de toenemende aandacht en ondersteuning voor het opstellen van standaarden en richtlijnen. Daaraan is gekoppeld de ruime belangstelling voor het vak EDP-auditing, hetgeen onder andere blijkt uit de grote belangstelling voor de postdoctorale EDP-auditopleidingen aan de VU, Erasmus en KUB, en de sterke groei in EDP-auditafdelingen binnen de accountantskantoren en de interne accountantsdiensten. Uiteindelijk zijn

de EDP-auditors de experts bij uitstek die op de werkvloer dagelijks aandacht besteden aan informatiebeveiliging en veelal het voortouw nemen bij het initiëren van standaardisatie- en certificatie-activiteiten.

L I T E R A T U U R

- British Standard BS 7799, (1995), *Code of practice for information security management*, British Standards Institution, Londen.
- Department of Defense, (1983), *Trusted computer system evaluation criteria*, document CSC-STD-001-83, USA.
- NNI, (1994), *Code voor informatiebeveiliging, een leidraad voor beleid en implementatie*, Nederlands Normalisatie-instituut.
- OTB-standaard, (1996), *Unix (concept)*, Overlegorgaan Technische Beveiligingsstandaarden (verkrijgbaar via KPMG EDP Auditors, Amstelveen).
- OTB-studie, (1996), *Internet (concept)*, idem.
- Roos Lindgreen, E.E.O., (1996), *A sense of secureness, approaches to information security*, proefschrift Technische Universiteit Delft.