VERLEDEN, HEDEN EN TOEKOMST VAN INFORMATIEBEVEILIGING

Invloed van veranderingen in de informatie technologie

Auteur

ir. Paul L. Overbeek
Fysisch en Elektronisch Laboratorium - TNO
Postbus 96864, 2509 JG Den Haag

Samenvatting

In dit artikel wordt ingegaan op ontwikkelingen in de informatie technologie (IT) en de consequenties die dit heeft voor informatiebeveiliging.
Getoond wordt hoe het gebruik van IT is gegroeid van de klassieke computer met kaartlezer tot de huidige situatie van samenwerkende computers in netwerken. In de toekomst zal gegevensverwerking vaker en eenvoudiger gedistribueerd in netwerken plaats kunnen vinden.
Deze veranderingen hebben consequenties voor de noodzakelijke beveiliging:

1 Verantwoordelijkheden voor beveiliging verschuiven;
2 Procedures moeten worden afgestemd op de gedistribueerde verwerking;
3 Het effect van fysieke beveiliging wordt kleiner;
4 Er zal een zwaarder beroep gedaan worden op systeem-technische beveiliging. De huidige mogelijkheden voor technische beveiliging lopen echter achter bij de snel toenemende mogelijkheden voor gedistribueerde gegevensverwerking.

1. INTRODUCTIE

In dit artikel wordt ingegaan op ontwikkelingen in de informatie technologie (IT) en de consequenties die dit heeft voor informatiebeveiliging. De invoering van computernetwerken maakt het mogelijk effectief informatie te delen en beter (gemeenschappelijk) gebruik te maken van kostbare computerapparatuur via een computernetwerk. Netwerken maken het mogelijk dat informatie gedistribueerd wordt verwerkt. Het toenemende gebruik van netwerken brengt naast veel goede kanten ook een aantal beveiligingsproblemen met zich mee. Het lijkt erop dat de noodzakelijke veranderingen die dit met zich mee moet brengen, momenteel onvoldoende worden onderkend.

Allereerst wordt het belangrijkste beveiligingsjargon uitgelegd. Daarna wordt in een overzicht de 'evolutie' van de IT beschreven en een blik geworpen op toekomstige ontwikkelingen. Vervolgens wordt gekeken naar de beveiligingsmogelijkheden en -behoeften in de verschillende evolutiestadia van de IT.

2. TERMEN EN BEGRIPPEN

In dit hoofdstuk worden in het kort de belangrijkste termen en begrippen op beveiligingsgebied geïntroduceerd.

2.1 De waarde van informatie

Informatiebeveiliging heeft als doel de veiligheid van informatie. *Veiligheid* (safety[1]) is het gevrijwaard zijn van onbewuste risico's. *Beveiliging* (security) is daartoe het middel. Hetgeen beveiligd moet worden is de waarde van de informatie. De waarde van de informatie wordt bepaald door de aspecten vertrouwelijkheid, integriteit en beschikbaarheid.
Vertrouwelijkheid (confidentiality) is het exclusief voorbehouden zijn (aan een persoon of groep) van informatie en het exclusieve gebruik van informatie.
Integriteit (integrity) is de juistheid, volledigheid en ook het correct in de tijd zijn van informatie.
Beschikbaarheid (availability) is het op een gewenst moment binnen een zekere tijd kunnen beschikken over de informatie, en dus ook over de informatieverwerkende middelen.

Afgeleide aspecten zijn privacy en controleerbaarheid. *Privacy* heeft betrekking op tot een natuurlijke persoon herleidbare informatie. Merk op dat privacy zowel vertrouwelijkheid als integriteit van persoonlijke informatie betreft. En bijzonder onderdeel van privacy is het 'recht' op anonimiteit. Controleerbaarheid geeft de mogelijkheid de effectiviteit van de beveiliging te kunnen toetsen.

Informatiebeveiliging staat ten dienste van de belangen van het bedrijf of de organisatie. Niet alle informatie en informatiediensten zijn even waardevol. Informatiebeveiliging moet afgestemd zijn op de waarde van de informatie. Een vorm van rubricering (classificatie) van de informatie is daarvoor noodzakelijk.

---

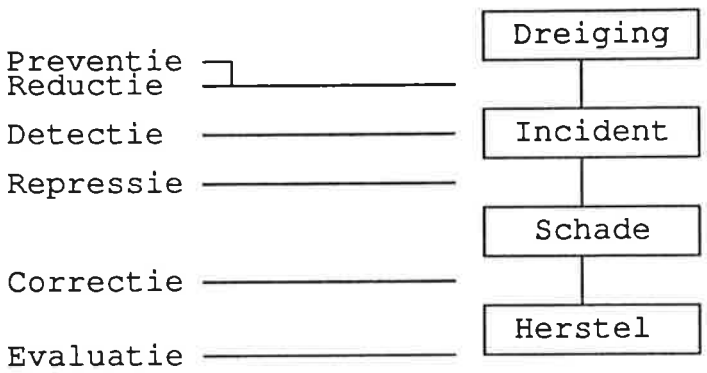
1 Aangezien vrijwel alle literatuur op dit gebied Engelstalig is, zijn de gangbare Engelse termen tussen haakjes toegevoegd.

2.2 Beveiligingsmaatregelen

Met beveiligingsmaatregelen kunnen de risico's voor de informatie beperkt (verkleind of weggenomen) worden. Uitgangspunt en verreweg het belangrijkste is een goede *organisatie* van beveiliging, met duidelijke verantwoordelijkheden en taken, richtlijnen, rapportagelijnen en afstemming van maatregelen. *Fysieke* beveiligingsmaatregelen, zoals de fysieke afscherming van de computerruimte, zijn vaak doeltreffend en eenvoudig. De reikwijdte is natuurlijk beperkt. *Systeemtechnische* beveiligingsmaatregelen (ook logische beveiliging genoemd) bieden beveiliging in een computersysteem of netwerk. Dit is bijvoorbeeld de beveiliging die het besturingssysteem biedt voor de scheiding tussen gebruikers of de 'login' voor toegang tot een systeem. *Procedures* beschrijven hoe er in bepaalde gevallen door het personeel gehandeld moet worden. Zo horen er bijvoorbeeld procedures te zijn die beschrijven wie er wanneer toegang heeft tot de computerruimte, en procedures die beschrijven wanneer een 'account' vervalt en wat er dan met de nog aanwezige informatie gebeurt.
Beveiligingsmaatregelen hebben alleen nut in onderlinge samenhang. De beveiligingsorganisatie moet daar zorg voor dragen.

2.3 Soorten beveiligingsmaatregelen

Beveiligingsmaatregelen zijn gericht op een bepaald moment van de *incidentcyclus* (event cycle), zie figuur 1.



Figuur 1: Incidentcyclus

In de incidentcyclus worden de volgende stappen onderscheiden. Allereerst is er de dreiging dat er iets zou kunnen gebeuren. Als er daadwerkelijk iets gebeurt spreken we van een (beveiligings)-incident. Hierdoor ontstaat schade (aan informatie of aan middelen) die hersteld moet worden.

Aan al deze stappen moet aandacht besteed worden met passende beveiligingsmaatregelen, wederom afhankelijk van de waarde die aan de informatie wordt gehecht. Allereerst wordt met *preventieve* beveiligingsmaatregelen getracht om te voorkomen dat een incident optreedt. Tevens worden op voorhand maatregelen genomen die de eventuele schade die mogelijk zou kunnen ontstaan zo beperkt mogelijk moeten houden. Dit zijn *reducerende* beveiligingsmaatregelen. Mocht een incident optreden, dan is het van belang dit zo snel mogelijk te ontdekken: *detectie*. Vervolgens wordt met *repressieve* maatregelen voortduring of herhaling van het incident tegengegaan. Met *correctieve* maatregelen wordt de schade zo goed mogelijk hersteld. Bij ernstige incidenten is na verloop van tijd een *evaluatie* nodig: wat ging er fout, hoe is het veroorzaakt, en hoe kan dit in de toekomst voorkomen worden. Evaluatie is niet alleen per incident nodig, maar ook op basis van inzicht in alle incidenten en de ontwikkeling hiervan. Deze 'hogere orde' evaluatie moet ondersteund worden door een meldingsprocedure voor beveiligingsincidenten.

3. ONTWIKKELING VAN DE INFORMATIETECHNOLOGIE

In dit hoofdstuk wordt getoond hoe het gebruik van IT is gegroeid van de klassieke computer met kaartlezer tot de huidige situatie van samenwerkende computers in netwerken. Tevens zal een blik op toekomstige ontwikkelingen worden geworpen.
Dit overzicht heeft als doel om de veranderingen te tonen in het gebruik van IT; er is geen pretentie van volledigheid.

3.1 Verleden

De geschiedenis van de IT is geschreven in de afgelopen drie decennia. Daarin zijn twee belangrijke stappen te onderscheiden: de batch-periode en de interactieve periode.

3.1.1 Batch periode

In het eerste begin stond de hardware centraal in het computergebruik. Programma's werden geschreven in een taal die 'dicht bij de machine' stond, zoals assembler. De machine werd door zijn gebruikers gevoed met ponskaarten en het resultaat van een 'job' kwam via de printer beschikbaar.
Al het werk werd batchgewijs uitgevoerd. Dat wil zeggen dat er een wachtrij (queue) is voor het uit te voeren werk op de computer. Het besturingssysteem bedient die wachtrij door daar een nieuwe job van af te halen zodra een vorige klaar is. Op één moment is er maar één job actief in het systeem. Het besturingssysteem kon daardoor, naar de maatstaven van vandaag, eenvoudig zijn.

3.1.2 Interactieve verwerking

Voor bepaalde taken was batch-verwerking niet handig, met name voor beheerstaken. Daar werd het volgende voor gevonden: voor bepaalde jobs kon een één-regelige 'job' aangeboden worden en in een aparte queue worden geplaatst waarin de job vrijwel zonder wachttijd werd uitgevoerd. Eén stap verder is het queue-mechanisme vervangen door een interrupt-mechanisme (een electronische 'bel' in de computer) en is de interactieve verwerking (U vraagt, de computer antwoord bijna direct) definitief een feit.

De ponskaart had hiermee zijn langste leven gehad. Het was nu mogelijk om in plaats van met ponskaarten te werken met kaart-beelden: het equivalent van de ponskaart op een beeldscherm.

De kaartbeelden konden vanaf het scherm worden aangemaakt, gewijzigd en opgeslagen. De electronische stapel kaarten werd vervolgens weer voor batchgewijze uitvoering aangeboden. De gebruiker hoefde nu niet meer met ponskaarten naar het systeem te komen maar voerde het werk uit achter een terminal, die met een vaste lijn verbonden was met het computersysteem.

Overigens maakten niet alle leveranciers deze stap op dezelfde manier. Er zijn leveranciers die vanuit een achtergrond in de procesbesturing (typisch een real-time toepassing) interactieve systemen zijn gaan ontwikkelen.

Door het toenemend aantal taken nam de complexiteit van de besturingssystemen toe. Karakteristiek voor deze periode is dat er wel meer jobs in het systeem aanwezig zijn, maar dat er daarvan maar één actief kan zijn. Het besturingssysteem verdeelt de beschikbare capaciteit zo eerlijk mogelijk over de jobs in de tijd.
Nota Bene: het interactieve werk is niet in plaats van het batch-werk gekomen. Het batchwerk blijft gewoon bestaan en de techniek hiervoor ontwikkelt zich verder; het interactieve werk kan echter voorzien in andere soorten informatiebehoeften.

3.2 Heden: netwerken met zelfstandige systemen van verschillende leveranciers, PC's en werkstations

Het aantal computers binnen een organisatie neemt snel toe. Om informatie uit te kunnen wisselen tussen computers worden netwerken aangelegd, in eerste instantie voor gebruik tussen computers onderling maar al snel worden deze netwerken ook voor terminal-toegang tot andere systemen gebruikt.
De gebruiker zit niet meer achter een terminal maar achter een PC of werkstation die is opgenomen in het netwerk.
Een 'normale' verwerkingsomgeving voor informatie bevat systemen van verschillende leveranciers en met verschillende besturingssystemen. Er zijn mainframe's, mini's, PC's en servers. Een deel van de infrastructuur staat veelal centraal opgesteld en wordt ook centraal beheerd. Een ander deel wordt door de gebruikers zelf beheerd, vrijwel zonder controle vanuit de organisatie. De connectiviteit tussen de systemen wordt bereikt met diverse netwerkproducten, soms over gescheiden, soms over dezelfde bekabeling. Tevens kan gebruik gemaakt worden van de openbare PTT-infrastructuur. Een opkomend fenomeen is dat het onderscheid tussen lokale verwerking en gedistribueerde verwerking via het netwerk aan het vervagen is. De plaats van

verwerking of opslag wordt in toenemende mate dynamisch bepaald. Complexe informatiesystemen, waarvan de juiste werking vóóraf niet eens volledig getoetst kan worden, moeten in deze omgeving functioneren.
In deze omgeving vol onzekerheden wordt informatie die van vitaal belang is voor een organisatie verwerkt, getransporteerd en opgeslagen.

De opkomst van de PC's en werkstations versterkt het belang van netwerken. Langzamerhand ontstaat een scheiding van opslag (op fileservers) en verwerking (op de lokale PC of op een centraal systeem dat beter geschikt is voor een bepaalde toepassing). Netwerken verzorgen de hiervoor noodzakelijke verbindingsmogelijkheden (connectiviteit).

3.3 Toekomst: netwerken met gedistribueerde gegevensverwerking

Er zijn een aantal trends te onderkennen. Netwerken zullen in de toekomst belangrijker worden. De huidige groei in het gebruik van lokale netwerken (netwerken binnen een lokatie en in eigendom van het bedrijf), zal zich ook gaan manifesteren in de 'wide area'-netwerken (netwerken tussen lokaties en in eigendom van een PTT). De nu nog gescheiden (lokale) netwerken zullen steeds meer met elkaar verbonden worden. Netwerken zullen gedeeld worden voor gebruik door verschillende organisaties.
De gebruiker zal niet meer gebonden zijn aan zijn werkplek. Vanaf iedere PC of werkstation zal hij zijn werk kunnen uitvoeren. Overigens zal de apparatuur die daarvoor nodig is makkelijk meegenomen kunnen worden. Voor de gebruiker zal het verschil tussen 'lokaal' en 'netwerk' vervagen. Taken worden uitgevoerd daar waar het op dat moment het beste uitkomt. De gegevensopslag en -verwerking zal vaker en eenvoudiger gedistribueerd plaats kunnen vinden.

Verdere standaardisatie van netwerkprotocollen is daarvoor noodzakelijk. Tevens moeten besturingssystemen aangepast worden voor de gedistribueerde verwerkingsmogelijkheden. Het zal bijvoorbeeld mogelijk moeten zijn om informatie uit te wisselen tussen computersystemen over de beschikbare middelen en diensten.

4. ONTWIKKELING VAN BEVEILIGING

Uitgaande van deze korte beschouwing over de ontwikkeling van de IT wordt nu beschreven hoe de beveiliging zich daarbij heeft ontwikkeld. Hierbij wordt gekeken naar de drie beveiligingsaspecten vertrouwelijkheid, integriteit en beschikbaarheid; naar de soorten beveiligingsmaatregelen en naar hun werking.

4.1 Verleden

4.1.1 Batch periode

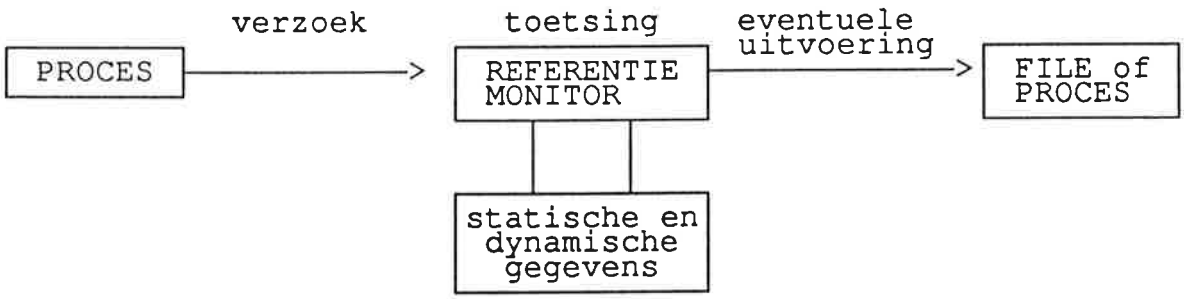
De 'machine' moest beschermd worden, want deze was kwetsbaar en kostbaar. Daarom werd de computer in een aparte ruimte geplaatst met beperkte toegangsmogelijkheden: de centrale computerruimte. Invoer (ponskaarten) en uitvoer (printwerk) vond plaats via een soort loket bij de centrale computerruimte. Een bijkomende functie van dit loket was (sociale) controle van het computergebruik.
Aan de hand van de job-control-kaarten werden voor het starten van de job de juiste schijven en bestanden bereikbaar gemaakt. Als er al werd gecontroleerd of toegang tot bepaalde gegevens toegestaan was, dan gebeurde dat vooraf aan de hand van deze job-control-kaarten. Deze controle richte zich op ongeoorloofde toegang tot de gegevens, vooral om de vertrouwelijkheid te bewaren. Er was nog geen aandacht voor integriteit en beschikbaarheid.

De verantwoordelijkheid voor de beveiliging van de computer en de gegevens was uitbesteed aan het hoofd van de computerafdeling. Beveiliging was voornamelijk fysiek. Eventuele systeemtechnische beveiliging werd vooraf uitgevoerd, was voornamelijk gericht op vertrouwelijkheid en had een preventieve werking. Procedures waren simpel en vanuit beveiligingsoogpunt was het leven eenvoudig.

4.1.2 Interactieve verwerking

De opkomst van de interactieve verwerking bracht een aantal nieuwe beveiligingsproblemen: de gebruikers achter de terminals waren anoniem en moesten gecontroleerd worden; het terminalverkeer was onbeschermd; gebruikers moesten in het systeem uit elkaar gehouden worden, en van elkaars gegevens afblijven.

De computer, de printer en de disks met de informatie bleven centraal opgesteld en konden nog steeds effectief met fysieke beveiligingsmaatregelen beschermd worden. De systeemtechnische beveiliging moest aanzienlijk worden uitgebreid, immers, in de batch-periode was hier nauwelijks behoefte aan. In het verleden was beveiliging in informatiesystemen (applicaties, besturingssystemen en netwerken) nooit een ontwerpcriterium. Beveiliging moest altijd in een later stadium toegevoegd worden. Dit 'achteraf beveiligen' is een moeilijke exercitie omdat alle beveiligingslekken gevonden moeten worden, die dan vervolgens weer verholpen moeten worden. Als dit al succesvol verloopt dan is er tenminste sprake van verlies aan performance of functionaliteit en een negatieve beeldvorming bij de gebruiker.
In het gunstigste geval werd de systeemtechnische beveiliging gebaseerd op het concept van de referentie-monitor, in figuur 2 vereenvoudigd weergegeven. In dit concept wordt ieder verzoek voor een bepaalde actie voor uitvoering getoetst. Deze toetsing vindt plaats vóór uitvoering, aan de hand van statische gegevens over de betrokkenen maar ook aan de hand van dynamische gegevens over de toestand in het gehele systeem.



Figuur 2: toetsing door referentiemonitor

De referentiemonitor moet zorgdragen voor gecontroleerde toestandsovergangen van de ene veilige toestand naar de volgende. Of een toestandsovergang is toegestaan, wordt beoordeeld op basis van informatie uit security-databases waarin b.v. informatie over rechten en plichten die bij de betrokken files of processen (gebruikers) horen. Op basis van deze informatie beoordeelt de referentiemonitor of het verzoek, en daarmee de overgang naar een nieuwe toestand toegestaan is. Tijdens de beoordeling door de referentiemonitor mogen er geen voor beveiliging relevante wijzigingen optreden. De toestand in het systeem wordt als het ware 'bevroren'.

Dit concept is alleen bruikbaar in systemen waarin één beheersbare toestand is. Dit is bijvoorbeeld het geval op computers met één processor. In netwerken en in gedistribueerde systemen is geen sprake van één vaste, beheersbare toestand. De referentiemonitor is voor deze systemen dan ook minder geschikt.

De verantwoordelijkheid voor beveiliging kon nog steeds bij de centrale computerafdeling blijven liggen. Deze had immers toch al het technische beheer van de systemen en kon daarom goed de uitgebreidere systeemtechnische beveiliging er bij nemen. Zoals gezegd werd de systeemtechnische beveiliging belangrijker, maar kon de fysieke beveiliging niet worden verwaarloosd. Procedures namen toe in aantal en complexiteit. Beveiliging was nog steeds voornamelijk gericht op preventie, echter reductie (backup) en detectie (audit) werden belangrijker.
De noodzaak tot beveiliging werd echter vaak niet voldoende onderkend: de gebruikersgroep was min of meer bekend en de problemen bleven aanwijsbaar en lokaal.

4.2 Heden: netwerken met zelfstandige systemen van verschillende leveranciers, PC's en werkstations

Informatiebeveiliging moet in een omgeving met netwerken en computersystemen van verschillende leveranciers functioneren. Uitgangspunt moet zijn dat de infrastructuur gedeeld wordt met mogelijk onbetrouwbare of onvoorspelbare deelnemers (computers, gebruikers en software) en dat de communicatie plaatsvindt over onveilige kanalen.
Connectiviteit is belangrijk. Informatiestromen zijn niet beperkt tot één specifieke computer, besturingssysteem of netwerk, zelfs niet tot een bepaalde applicatie. Informatiebeveiliging moet de informatie zelf, de informatiestromen en dus de connectiviteit kunnen beheersen. Dit is alleen bereikbaar met behulp van standaardisatie.

4.2.1 Systeemtechnische beveiliging

De realiteit is dat vandaag de dag beveiliging 'host'-georiënteerd is, dat wil zeggen dat de beveiliging *per computer* geregeld is. De systeemtechnische beveiliging is gebaseerd op het concept van de referentiemonitor, waarvan bekend is dat het in een netwerk minder geschikt is.

De verantwoordelijken voor informatiebeveiliging hebben een zware taak. Het ontbreekt aan essentiële hulpmiddelen voor informatiebeveiliging. Bijna alle beveiligingshulpmiddelen zijn gericht op preventie. Voor de andere stappen van de incidentcyclus bestaan te weinig

geautomatiseerde hulpmiddelen. De beheersing van de integriteit van informatie en software is voorlopig nog onderwerp van onderzoek. Hetzelfde geldt voor de beschikbaarheid van informatie en diensten.

4.2.2 Verantwoordelijkheden

Hoe zit dat inmiddels met de verantwoordelijkheden voor beveiliging? Liggen die nog precies hetzelfde als in het 'batch'-tijdperk?
Er is een tendens naar gedistribueerde gegevensverwerking in netwerken op werkstations en PC's. De betrokkenheid en verantwoordelijkheid van de computerafdeling voor deze decentrale systemen is in veel organisaties minimaal.
Voor beveiliging kan dit negatieve gevolgen hebben, om de volgende drie redenen:

1 Bij gedistribueerde gegevensverwerking zal een deel van de verantwoordelijkheid voor de beveiliging, die vroeger uitbesteed was aan de computerafdeling, ingevuld moeten worden door de gebruikers (denk aan de beveiliging van gegevens op een PC in het netwerk). Als dit al efficiënt gebeurt, dan nog ontstaat een onaantrekkelijke situatie van verdeling van verantwoordelijkheden tussen de computerafdeling en de gebruikers. Er kunnen delen van de infrastructuur en gegevensverzamelingen ontstaan waar niemand zich verantwoordelijk voor voelt. Dit is ongewenst.
2 Werken in een situatie met werkstations en PC's in netwerken vergroot de behoefte aan beveiliging. Immers, netwerken brengen naast veel goede zaken (zelfs op beveiligingsgebied) ook een aantal beveiligingsproblemen met zich mee; daarnaast wordt het aantal systemen dat veilig moet zijn steeds groter.
3 De prioriteiten van de computerafdeling liggen in veel gevallen nog bij de centrale systemen.

Een vraag die de computerafdeling zich voortdurend zou moeten stellen is of de diensten die de gebruikers nodig hebben wel geboden worden. Op een hoger nivo moet de vraag gesteld worden: waar komen, gezien de veranderingen, de verantwoordelijkheden voor informatiebeveiliging te liggen, en welke middelen en organisatie zijn daarvoor noodzakelijk.

Beheer

Door de toenemende complexiteit en connectiviteit tussen systemen wordt ook steeds duidelijker dat de beschikbare middelen voor goed beheer, inclusief beveiligingsbeheer, ontoereikend zijn. De noodzakelijke samenhang tussen applicatie-, systeem- en netwerkbeheer is nauwelijks af te dwingen. Er zijn zoveel potentiële lekken dat de beheerders deze onmogelijk zelf allemaal in de gaten kunnen houden.

4.2.3 *Procedures*

Het effect van procedures neemt af naarmate er meer mensen zijn die zich er aan moeten houden. Het maakt een groot verschil of er één persoon is die overal een backup van moet maken, of dat er honderd een deel moeten doen.
In onderzoeken wordt gemeld dat beveiligingsincidenten in de meeste gevallen veroorzaakt worden door de eigen medewerkers. Veel hangt af van de motivatie en het beveiligingsbewustzijn (awareness) van het personeel. Daarnaast moet controle van de werkzaamheden van het eigen personeel niet geschuwd worden (wie controleert de beheerder) en is een goede afbakening van verantwoordelijkheden van belang.
Tevens moet de vraag gesteld worden of die afhankelijkheid van de goede wil van het eigen personeel wel zo wenselijk is. Is het niet zo dat de kwetsbaarheid van informatiesystemen voor menselijk falen te groot is? Techniek zou daar een oplossing voor moeten bieden.

4.2.4 *Fysieke beveiliging*

Vroeger was er één centrale ruimte die fysiek beveiligd moest worden om informatie veilig te stellen. Nu is informatie op veel meer plaatsen aanwezig. Beveiliging van de informatie op de werkplek is belangrijk, maar er moet een evenwicht zijn tussen de beveiliging van de werkplek en andere delen van de infrastructuur. Het heeft weinig nut Uw PC om te bouwen tot een kasteel als het netwerk dat U gebruikt zo goed als open is.

De vroegere eenzijdige nadruk op het aspect vertrouwelijkheid is aan het vervagen. Vanwege het toenemende belang van de informatieverwerking wordt de beschikbaarheid van gegevens steeds belangrijker. Er is dan ook een toenemend gebruik van zogenaamde 'fault tolerant systems', een wat misleidende naam voor systemen waarbij een deel van de hardware dubbel is uitgevoerd. Technische storingen in die hardware kunnen hiermee gedeeltelijk worden opgevangen. Dit helpt echter niet bij software fouten, menselijke fouten of andere storingen, bijvoorbeeld in het netwerk.
Daarnaast wordt ook de integriteit van de gegevens steeds belangrijker. Gegevens vertegenwoordigen geld, bestellingen en strategische informatie. Fouten in die gegevens kunnen grote gevolgen hebben.

4.3 Toekomst: netwerken met gedistribueerde gegevensverwerking

Om het hoofd te bieden aan de beveiligingsproblemen in een situatie waar niet langer 'de computer' maar 'het netwerk' centraal staat zijn er oplossingen nodig voor volgende gebieden:

1 Gegevens zullen steeds vaker getransporteerd worden via mogelijk vijandige netwerken en opgeslagen zijn in mogelijk onveilige computersystemen. Deze gegevens kunnen beschermd worden door gebruik te maken van cryptografie (codering). Er zijn snelle cryptografische technieken nodig die flexibel genoeg zijn om gebruikt te worden in netwerken. Deze technieken moeten gegevens beschermen afhankelijk van het belang van de gegevens en deze bescherming binden aan de eigenaar van de gegevens.

2 Systeemtechnische beveiliging in computersystemen en netwerken moet geïntegreerd en verbeterd worden. (Momenteel heeft een computersysteem bijvoorbeeld geen kennis van de beveiliging in het netwerk en de beveiliging op een ander computersysteem.)
Nieuwe systemen zullen beter om moeten gaan met integriteit van gegevens. Onderdeel hiervan is het bewaken van de integriteit van software.
Beschikbaarheid wordt ook belangrijker. Niet langer zal het hier in de eerste plaats gaan om bescherming tegen storingen, maar om het beschikbaar houden van bepaalde gegevens en diensten. Immers, in een gedistribueerde omgeving kunnen gegevens via meer wegen bereikbaar zijn, en taken op meerdere plaatsen worden uitgevoerd.

3 Om veiligheid tussen verschillende besturingssystemen en netwerkprotocollen tot stand te brengen is standaardisatie noodzakelijk.

4 Preventieve beveiligingsmaatregelen blijven van belang. Daarnaast zal het belang van maatregelen voor detectie, repressie en correctie toenemen. Hiervoor zijn technische hulpmiddelen noodzakelijk.

5 Hoe kunnen deze complexe systemen beheersbaar gehouden worden?

5. TOT SLOT

In dit artikel is duidelijk gemaakt dat de ontwikkeling in de informatie technologie consequenties *moet* hebben voor beveiliging. Dit betreft vooral veranderingen op organisatorisch en systeemtechnisch gebied. Verantwoordelijkheden voor beveiliging zullen verschuiven. De rol van de fysieke en procedurele beveiliging zal ook veranderen. Procedures moeten worden afgestemd op de gedistribueerde verwerking en de effectiviteit van fysieke beveiliging wordt kleiner.
Er zal een zwaarder beroep gedaan worden op systeem-technische beveiliging. De huidige mogelijkheden voor technische beveiliging lopen echter achter bij de snel toenemende mogelijkheden voor gedistribueerde gegevensverwerking. Deze achterstand moet ingehaald worden. Daarvoor is noodzakelijk:

- Aandacht voor integriteit en beschikbaarheid in besturingssystemen en netwerken;
- Meer aandacht voor hulpmiddelen ter detectie, repressie en correctie van beveiligingsincidenten;
- Standaardisatie op beveiligingsgebied.

Daarnaast zijn betere hulpmiddelen voor het beheer van IT-voorzieningen en ontwikkeling van complexe informatiesystemen noodzakelijk.

Aan deze problemen moet nu aandacht besteed worden. Zo niet, dan zal beveiliging steeds verder achter lopen bij de andere ontwikkelingen in de informatie technologie. Nieuw toepassingsmogelijkheden van informatie technologie kunnen hierdoor ernstig bemoeilijkt worden, zo niet onmogelijk gemaakt.

THEMADAG 1991
PHILIPS SECURITY OFFICE

COLLOQUIUM
COMPUTER- EN COMMUNICATIE-BEVEILIGING

EVOLUON EINDHOVEN

1 Oktober 1991