Beveiliging moet anticiperen op veranderingen

IFIP-congres biedt 'onderlinge hulp' voor beveiliging

Het jaarlijkse congres van de International Federation for Information Processing (IFIP) over beveiliging en bescherming van informatiesystemen had dit jaar als thema: 'Computer Security and Information Protection in our Changing World'. Dit verslag is de visie van de auteur op het congres dat plaatsvond in het Finse Espoo. De auteur was hier mede aanwezig namens het Nederlands Genootschap voor Informatica (NGI) op uitnodiging van Data Security Digest. Dit artikel is geschreven in het kader van het project 'Securable Distributed Information Systems' (SEDIS). Dit project beoogt inzicht te verwerven in en bij te dragen aan beveiliging in gedistribueerde informatiesystemen.

Ir. Paul Overbeek is werkzaam bij TNO/FEL te Den Haag

De International Federation for Information Processing (IFIP) heeft als doel de leidende internationale organisatie te zijn voor de stimulering van onderzoek, ontwikkeling en gebruik van informatie-technologie ten dienste van de mensheid. Al sinds de oprichting in 1960 betekent dit vooral de stimulering van internationale contacten tussen mensen die actief zijn in de informatietechnologie. Er is veel verwantschap met de rol van het NGI binnen Nederland. IFIP kent verschillende werkgroepen (Technical Committees) die zich met specifieke onderwerpen bezighouden. Technical Committee 11 (TC11) is zo'n zeven jaar geleden opgericht met als doel zich te richten op de problemen rond beveiliging en bescherming van informatieverwerkende systemen. TC11 organiseert ieder jaar een congres met een thema dat gerelateerd is aan informatiebeveiliging. Het congres fungeert tevens als ontmoetingsplaats voor mensen met dezelfde beroepsmatige achtergrond en problemen, een soort 'onderlinge hulpdienst'. Dit jaar waren er 280 deelnemers uit 30 landen, waarvan 13 uit Nederland. Nederland kwam daarmee na de Scandinavische landen op een vierde plaats. Het thema van dit jaar was 'Computer Security and Information Protection in our Changing World'. Het aspect 'verandering' kwam op verschillende manieren in de lezingen terug. De belangrijkste invalshoeken waren: verandering in de organisatie, vooruitgang in de techniek, zich wijzigende externe factoren en de invloed van veranderingen op audit.

Organisatie

Er is een tendens naar gedistribueerde gegevensverwerking in netwerken op workstations en PC's. In de lezingen van Charles Cresson Wood (Information Integrity Investments, USA) en Robert Moeller (Sears, Roebuck & Co, USA) kwam naar voren dat in veel organisaties de verantwoordelijkheid en betrokkenheid van de afdeling Electronic Data Processing (EDP, het rekencentrum) daarbij minimaal

is. Dit is een van de factoren die kan leiden tot verminderende budgetten en krimp voor de EDP-afdeling. Voor beveiliging kan dit negatieve gevolgen hebben, om de volgende drie redenen:

1 Bij gedistribueerde gegevensverwerking zal een deel van de verantwoordelijkheid voor de technische beveiliging, die vroeger uitbesteed was aan de EDP-afdeling, ingevuld moeten worden door de gebruikers (denk aan de beveiliging van gegevens op de PC in het netwerk). Als dit al efficiënt gebeurt, dan nog ontstaat een onaantrekkelijke situatie van verdeling van verantwoordelijkheden tussen de EDP-afdeling en de gebruikers. Er kunnen delen van de infrastructuur en gegevensverzamelingen ontstaan waar niemand zich verantwoordelijk voor voelt.

2 Werken in een situatie met workstations 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 Het is niet waarschijnlijk dat de EDP-afdeling bij druk op de budgetten de beveiligingsactiviteiten gaat intensiveren. Een vraag die EDP-afdelingen zich voortdurend moeten stellen is: worden wel de diensten geboden die de gebruikers nodig hebben. 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 moeilijk af te dwingen. Er zijn zoveel potentiële lekken dat de beheerders deze onmogelijk allemaal in de gaten kunnen houden. Dit levert ook problemen op voor de EDP-auditor.

Personeel

Veel sprekers halen onderzoeken aan waaruit zou blijken dat beveiligingsincidenten in de meeste gevallen veroorzaakt worden door de eigen medewerkers. Don Parker (SRI International, USA) zegt echter schertsend over deze statistieken: '85.9% of all statistics are invalid'. Terecht merken veel sprekers op dat in de praktijk veel afhangt 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 essentieel. 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.

Uitwijk

Sommige bedrijven zijn dermate afhankelijk geworden van hun computers dat het voor het bedrijf een ramp is als computerfaciliteiten gedurende langere tijd niet beschikbaar zijn. In het geval van een calamiteit in het computercentrum, zoals brand of waterschade, is het dan noodzakelijk op korte termijn de gegevensverwerking weer op gang te brengen. Kan dit niet binnen het bedrijf, dan moet er worden uitgeweken. Richard Hackworth (Midland Bank) en Karl Kreuger (The World Bank) beschreven hoe in een calamiteiten- of rampenplan verschillende scenario's met de bijbehorende acties in detail worden uitgewerkt. Computeruitwijk is natuurlijk maar één onderdeel van het rampenplan. Even belangrijk is het bijvoorbeeld om voor vervangende kantoorruimte en middelen voor het personeel te zorgen.

Techniek

Databases

Er is de laatste jaren veel vooruitgang geboekt op het gebied van beveiliging in databases. De eerste commerciële database-producten zijn nu beschikbaar die aan delen van de database labels voor de rubricering en specifieke toegangseisen kunnen verbinden. De toegangsmogelijkheden voor gebruikers kunnen zo beter beheerst worden. Dat echte multi-level secure databases nog ver weg zijn bleek uit de lezing van Rea Burns (Kanne Associates, USA) waarin een aantal fundamentele problemen werden uiteengezet waarvoor de theorie nog geen antwoorden biedt.

Netwerken

Internationale onderzoeksprogramma's als het CEC COST-11 project 'Security Mechanisms for Computer Networks' en het EURECA project OASIS (Open and Secure Information Systems) hebben de richting aangegeven voor het huidige onderzoek naar veiligheid in netwerken. Het eerste project gaat uit van de techniek en doet onderzoek naar uitbreiding van de OSI Security Architecture en de te gebruiken mechanismen. In het tweede project wordt onderzoek gedaan naar het overdragen van vertrouwen (trust) in netwerken. In presentaties van Sead Muftic (Universiteit van Sarajevo, Joegoslavië) en van Hans Peter Riess (Siemens, BRD) kwam naar voren dat in beide projecten de conclusie wordt getrokken dat de concepten voor beveiliging zoals die nu in besturingssystemen gangbaar zijn (zoals de referentie monitor), in een netwerk niet toegepast kunnen worden.

Virussen

De discussie rond computervirussen begint te luwen. Er zijn steeds minder paniekverhalen en de voorgestelde oplossingen worden steeds realistischer. De meningsverschillen tussen 'experts' liegen er echter niet om. Don Parker voorspelt: '..sinds mei '89 is de belangstelling voor het maken van virussen verdwenen en verkopers van virusprotectie en -detectiesoftware zullen verdwijnen bij gebrek aan markt'. Prof. Highland (USA) daarentegen zegt dat de volgende generatie virussen onderweg is die ook schade toe brengt aan de hardware. Merkwaardig is dat niemand zich af lijkt te vragen waarom het virusprobleem bestaat. Zou het probleem nog steeds bestaan als besturingssystemen onderscheid kunnen maken in betrouwbare en 'nog-niet'-betrouwbare software waarbij rechten in het systeem tevens verbonden zijn aan de gebruikte software?

Externe factoren

Privacywetten en computercriminaliteit

Eerder dit jaar werd op de Parijse Securicom reeds geconcludeerd dat de harmonisatie van de privacywetten en wetten tegen computercriminaliteit binnen Europa traag gaat. Dat deze verschillen voor de wereld buiten Europa nog veel groter zijn werd duidelijk uit de presentaties van Matti Tenhunen (Centraal Bureau Criminaliteit, Finland) en van Mark Tantam (Serious Fraud Office, UK). Het gevaar dreigt dat landen met een gebrekkige privacy-wetgeving gebruikt gaan worden als data-paradijs en dat landen aantrekkelijk zijn voor bepaalde computercriminaliteit (hacker-hemels). Dataverwerking wordt steeds meer internationaal. Dat vraagt om uniforme internationale rechtspraak.

Evaluatiecriteria voor beveiliging

Zowel aanbieders als kopers van IT-producten hebben belang bij een 'meetlat' voor de beveiliging van producten. In het verleden heeft hiervoor het Amerikaanse Orange Book (Trusted Computer Systems Evaluation Criteria) de belangrijkste rol gespeeld. In de loop van de tijd zijn echter nieuwe beveiligingsbehoeften ontstaan, zoals integriteit en continuïteit. Daarnaast was toetsing tegen de criteria van het Orange Book voor fabrikanten buiten Amerika aanzienlijk moeilijker dan voor Amerikaanse fabrikanten. Vanuit deze achtergrond hebben Nederland, Frankrijk, Engeland en Duitsland, met steun van de Europese Commissie, intussen een voorstel gedaan voor Europese Criteria. In dit voorstel, genaamd Information Technology Security Evaluation Criteria (ITSEC), wordt onderscheid gemaakt tussen beveilingingsfunctionaliteit en de zekerheid dat deze functionaliteit correct wordt aangeboden. Daarnaast wordt apart aandacht besteed aan de effectiviteit van de implementatie. Om het voor de gebruikers eenvoudig te houden zijn er tevens Functionality Classes gedefinieerd die voor een bepaald toepassingsgebied de gewenste functionaliteit beschrijven. Het is nog te vroeg om te zeggen of de ITSEC levensvatbaar is. Ook is nog niet duidelijk of van daaruit de gewenste internationaal aanvaarde standaard tot stand kan komen, bij voorkeur via de Internationale Organisatie voor Standaardisatie (ISO). Wel is duidelijk dat dit een serieus initiatief is dat steun verdient.

Audit

De rol van de EDP-auditor ligt ten dele in het verlengde van die van de accountant. Eén van taken van de EDP-auditor is het controleren of de gerealiseerde beveiliging in de informatiesystemen wel in overeenstemming is met de door het management geformuleerde uitgangspunten. Uit lezingen van Knud Kristiansen (Sparekasse, Denemarken) en Ib Bentzien (Bikuben, Denemarken) werd duidelijk dat de EDP-auditor het door de toenemende complexiteit steeds moeilijker krijgt om zich een beeld te vormen van de beveiliging in een systeem. Veelal ontbreken goede auditpunten en de nu beschikbare hulpmiddelen voor audit van systemen bieden een te beperkte functionaliteit.

Tot slot

Uit Nederland waren er dit jaar twee bijdragen. Prof. Hans de Lange (Vrije Universiteit van Amsterdam) ging in op audit in netwerken. Door de grote flexibiliteit in netwerken is nauwelijks te beoordelen wie wel en wie geen toegang heeft tot voorzieningen. Hoewel zijn boodschap positief was (wat kan er wel geaudit worden) was de onderliggende toon dat effectieve audit eigenlijk nauwelijks mogelijk is. Peter Capiteijns (Philips) ging in op de consequenties voor de organisatie van beveiliging in een omgeving waarin organisatorische veranderingen regelmatig voor komen en de rol die een goed beveiligingsbeleid daarin kan spelen. De Belg Hedwig Cnudde (Cryptech) gaf een beschrijving van een veilig electronic mail systeem voor de Belgische overheid waar ook het kabinet gebruik van maakt. Dit systeem stelt de gebruikers in staat van huis uit berichten te versturen en te ontvangen. Naar aanleiding van een kraak in 1985 werd besloten dit systeem te beveiligen.

Mijns inziens voorziet dit congres in een duidelijke behoefte. Er is voldoende gelegenheid om met beroepsgenoten in contact te komen en de sprekers snijden problemen uit de praktijk aan zonder oppervlakkig te worden. De organisatie en de deelnemers kunnen terugzien op een geslaagd congres. Volgend jaar is het congres in Brighton in Engeland van 15-17 mei. Het thema is dan 'Creating Confidence in Information Processing'.

IR. PAUL L. OVERBEEK