



INFORMATIEBEVEILIGING

De ontwikkeling van een IT Compliance Mode

3

Petra Bos Om grip te krijgen en te houden op de mate van compliance binnen een bedrijf heeft Petra Bos een IT compliance model ontwikkeld. In dit artikel meer over de achtergronden van compliance, het onderzoek en het door de auteur ontwikkelde model.

Identiteitsfraude: methoden, omvang en maatregelen

7

Nicole van der Meulen In dit artikel worden de verschillende soorten van identiteitsfraude en de uiteenlopende werkmethode van fraudeurs beschreven. Ook wordt inzicht gegeven in de omvang van het probleem in de Verenigde Staten en het Verenigd Koninkrijk.

Daarom SAPM Tools!

16

Rob Greuter Gebruikers met volledige superuser-, root- of administrator rechten brengen voor een organisatie grote risico's met zich mee als het gaat om bewust en/of onbewust misbruik. Dit artikel gaat dieper in op zowel deze problemen als op de beschikbare oplossingen.

Federated Identity Management: Het einde van de digitale sleutelbos?

22

Martijn Verbree en Emanuël van der Hulst Een belangrijke maatregel in het palet van informatiebeveiliging is het implementeren van logische toegangsbeveiliging. Juist om deze digitale sleutelbos terug te dringen, is er de laatste jaren een nieuwe trend ontstaan: 'Federated identity management'. In dit artikel de ins en outs.

Derde IB-OPLEIDINGENMARKT

26

Fred van Noord Op donderdag 24 mei 2007 wordt alweer de derde informatiemarkt van opleidingen voor informatiebeveiliging gehouden. Dit op de Erasmus Universiteit in Rotterdam. Het evenement biedt de laatste stand van zaken op het gebied van opleidingen en richt zich op beveiligingsprofessionals, ict-ers en studenten van mbo- en hbo-instellingen en universiteiten.

Economische beoordeling van informatiebeveiliging

28

Said El Aoufi Er wordt in dit artikel antwoord gegeven op de vraag waarom het moeilijk is om investeringen op het gebied van informatiebeveiliging te beoordelen en hiermee de waarde van informatiebeveiliging te bepalen.

Security in Nederland bij Sentinels in 2006

Auteur: Dr. Rik D.T. Janssen, Technologiestichting STW, secretaris Sentinels. Telefoon: (030) 600 12 83, e-mail: info@sentinels.nl.



Het doel van het Sentinels onderzoeksprogramma is om alle soorten informatiesystemen en netwerken veiliger te maken. Er bestaat al behoorlijk wat security-onderzoek in Nederland, zowel bij universiteiten als binnen het bedrijfsleven. Allerlei stichtingen, instellingen en ministeries zijn hierbij betrokken. Een belangrijk doel is dan ook het coördineren hiervan en het verbeteren en stimuleren van de samenhang. Daarnaast wordt, door een verplichte bedrijfsbijdrage bij elk Sentinels project, een actieve rol verwacht van bedrijven die deelnemen aan onderzoek. Hiermee hopen we te bereiken dat de resultaten uit het onderzoek ook uiteindelijk door bedrijven en instellingen in Nederland gebruikt gaan worden.

Sentinels projecten 2005

In 2005 zijn de volgende onderzoeksprojecten gestart:

- JASON, Generic and Secure Remote Management Infrastructure;
- IPID, Integrated Policy-based Intrusion Detection;
- Practical Approaches to Secure Computation;
- ProBiTe, Protection of Biometric Templates;
- DeWorm, Worm monitoring on Internet backbones;
- PINPAS JC, Program INferred Power-Analysis in Software for Java Card.

Uitgebreide informatie over deze projecten is te vinden op www.sentinels.nl/projects. Ook in 2006 is de Sentinels ambassadeur actief geweest. Hieronder zal eerst van elk project een korte samenvatting gegeven worden, gevolgd door de voortgang in het afgelopen jaar. Daarna zal het werk van de Sentinels ambassadeur besproken worden.

- JASON, *Generic and Secure Remote Management Infrastructure*
dr. Erik Poll en dr. Jaap-Henk Hoepman, Radboud Universiteit Nijmegen
De onderzoekers willen een secure

Sentinels (www.sentinels.nl) is het Nederlandse onderzoeksprogramma op het gebied van informatiebeveiliging, beveiliging van informatiesystemen en van computernetwerken. Het wordt gefinancierd door Technologiestichting STW, NWO en het ministerie van Economische Zaken. In het vorige nummer van Informatiebeveiliging zijn de vijf projecten beschreven die in 2006 gehonoreerd zijn. In dit artikel beschrijven we de eerste resultaten van de zes projecten die in 2005 van start zijn gegaan. Elk van deze projecten duurt ongeveer vier jaar.

systeem architectuur ontwerpen met een bijbehorend programmeerparadigma. Doel zijn juist die ambient applicaties waarbij een grote hoeveelheid smartcards en embedded systemen betrokken zijn. Het deelnemende bedrijf is Chess.

Voortgang in 2006

De onderzoekers hebben een 'secure network of objects' paradigma gemaakt waarmee ontwerpers kunnen specificeren aan welke veiligheidsspecificatie objecten en communicatie tussen objecten moeten voldoen. Het JASON platform vertaalt die specificaties automatisch in een veilige (software)implementatie. Bedrijven als Chess kunnen hier bijvoorbeeld veilige betaalterminals of park & pay systemen mee maken.

Daarnaast is onderzocht hoe voor JASON veilige en afgescheiden delen gemaakt kunnen worden, zodat applicaties hun eigen afgesloten omgeving hebben en geen invloed kunnen uitoefenen op andere applicaties die op hetzelfde platform draaien. De onderzoekers hebben gekozen voor de Java Sandbox en het Xen systeem. Voor de afgescheiden delen hebben ze ook een experimenteelplatform gemaakt.

Voor Chess is van belang hoe een goede betaalterminal gemaakt kan worden. Dat is nodig omdat deze aan steeds strengere internationale veiligheidseisen moeten voldoen. Chess kan de ontwikkelingen rond JASON hierbij goed gebruiken, want het is voor hen van groot belang dat er een (computer)taal is waarmee veiligheidspecificaties kunnen worden vastgelegd en getoetst. Hierdoor ontstaat er een methode waarmee de betaalterminals veilig ontworpen kunnen worden.

- IPID, *Integrated Policy-based Intrusion Detection*
prof.dr. Roel Wieringa, dr. Pascal van Eck

en prof.dr. Pieter Hartel, Universiteit Twente

De onderzoekers ontwikkelen een methode om bestaande technologie voor het detecteren van indringers, zoals worms en hackers in computersystemen, beter te kunnen inzetten in organisaties. Het doel is om hele bedrijfsinfrastructuren, zoals bijvoorbeeld het netwerk van ministeries of de databank van de sociale dienst, efficiënter en effectiever te beschermen tegen nieuwsgierige blikken en aanvallen van buitenaf (zoals bijvoorbeeld aanvallen op betaalsystemen). De deelnemende bedrijven zijn Rabobank Nederland en TNO ICT.

Voortgang in 2006

De methode bestaat uit twee aspecten: een organisatorische en een technische. De organisatorische onderzoekt hoe veranderingen in een organisatie of van personen die van functie veranderen in een organisatie, invloed hebben op de configuratie van de beveiligingssystemen van die organisatie. Een organisatie heeft vaak een bepaalde security policy en het kan lastig zijn om daaraan te blijven voldoen als iemand een andere functie krijgt, omdat bij een andere positie een andere policy hoort. Sommige oude rechten moeten ingenomen worden en nieuwe moeten worden toegekend. Het automatisch koppelen van een security policy aan toegangscontroles, autorisaties voor systemen en organisatorische bevoegdheden is gecompliceerd. Het technische aspect onderzoekt hoe dat dan gemaakt moet worden. Na een literatuurstudie is zo'n methode ontwikkeld. Daarnaast zijn er twee intrusion detection systemen gemaakt, Poseidon en Aphrodite. Beide systemen zijn gebaseerd op patronen die afwijken van de normale patronen. Op een bekende



DARPA testset geeft dit een hogere detectie en lager aantal false positives dan PAYL en PHAD, twee systemen die in de onderzoekswereld als standaard gelden. Verder hebben de onderzoekers twee onderzoeksvorstellen ingediend in de 2006 Sentinels ronde. Beide voorstellen zijn gehonoreerd.

In grote bedrijven zoals Philips en TNO is het vaak complex om te bepalen wie wat op welk moment mag en ook wat iemand niet mag. De resultaten uit dit onderzoek kunnen deze bedrijven strategieën leveren om deze security policies ook geldig te houden in geval van organisatiewijzigingen.

- *Practical Approaches to Secure Cooperation*

prof.dr. Ronald Cramer, Centrum voor Wiskunde en Informatica & Universiteit Leiden

De onderzoekers willen een brug slaan tussen cryptografisch onderzoek en de 'echte' wereld zodat fundamentele security tools uit die onderzoekswereld ook echt toegepast gaan worden. Deze methoden en technieken moeten tot de standaard gereedschapskist van de security engineer gaan behoren. Hiermee kunnen applicaties of protocollen gemaakt worden die veiliger zijn dan nu mogelijk is.

Het project richt zich specifiek op secure computation. Dit vakgebied houdt zich bezig met scenario's waarbij twee of meer partijen een bepaalde gemeenschappelijke taak moeten uitvoeren, maar waarbij partijen elkaar niet vertrouwen en gevoelige informatie voor elkaar geheim willen houden. Toepassingen van dit onderzoek liggen bijvoorbeeld op het gebied van digital rights management (DRM), biometrische authenticatie en secure datamining. Het deelnemend bedrijf is Philips Research.

Voortgang in 2006

In 2006 is een protocol voor 'bit sharing' ontwikkeld, een probleem dat na twintig jaar eindelijk is opgelost. Dit bit sharing protocol is een fundamenteel protocol dat toestaat dat een aantal andere belangrijke standaard problemen opgelost kunnen worden, zoals het vergelijken

van een gemeenschappelijk gegeven door twee partijen zonder aan elkaar kenbaar te maken dat een partij dat gegeven heeft. Toepassingen zijn bijvoorbeeld het veiliger worden van elektronisch stemmen en van online veilingen zoals op ebay. Daarnaast is een methode ontwikkeld waardoor public key infrastructure (PKI) systemen eenvoudiger gemaakt kunnen worden door identiteiten als publieke sleutel te gebruiken. Voor Philips is dit onderzoek onder meer interessant omdat bij matching van biometrische templates de informatie in het template geheim gehouden moet worden, terwijl er wel een vergelijking gedaan moet worden om te bepalen of iemand toegang kan krijgen tot iets. Dit onderzoek kan daarbij helpen.

- *ProBiTe, Protection of Biometric Templates*

dr.ir. Raymond Veldhuis, Universiteit Twente

De onderzoekers willen biometrische identificatie, zoals vingerafdrukherkenning en irisscans, integreren in security systemen. Bijvoorbeeld om met je vingerafdruk toegang te krijgen tot een huisnetwerk waarin DVD-spelers, computers en televisies met elkaar verbonden zijn. De templates die voor de herkenning gebruikt worden, moeten ook beschermd worden tegen misbruik. Hoe zorg je ervoor dat de opgeslagen templates geen informatie bevatten over de vingerafdruk? En hoe maak je in dat geval de herkenning zo betrouwbaar mogelijk? Het deelnemende bedrijf is Philips Research.

Voortgang in 2006

De onderzoekers hebben onderzoek gedaan naar het verbeteren van vingerafdrukherkenning en hoe je in templates opgeslagen informatie over vingerafdrukken kunt beschermen. Gewenst is bijvoorbeeld dat templates robuust zijn, dat ze een goed onderscheid maken tussen afdrucken van verschillende personen en dat ze een vaste lengte hebben zodat vergelijking met in een database opgeslagen templates efficiënt is uit te voeren. Ook moeten ze bestand zijn tegen ruis en moeten ze de variatie in verschillende afdrucken van dezelfde persoon aankunnen. Daarnaast is er een eerste ontwerp gemaakt voor een vingerafdrukherkenningssysteem, gebruikmakend van

genoemde resultaten. De template bescherming is in samenwerking met Philips ontwikkeld en blijkt erg goed te werken. Daarom wordt nu aan een octrooiaanvraag gewerkt.

Voor Philips is dit project interessant, omdat zij erg actief is op het gebied van bescherming van elektronische gegevens zoals muziek en films met technieken als digital rights management (DRM). De template bescherming kan daarbij helpen. Ook kan de samenwerking met de Universiteit Twente nieuwe methoden en technieken leveren.

- *DeWorm, Worm monitoring on Internet backbones*

dr.ir. Herbert Bos, Vrije Universiteit

De onderzoekers willen een methode ontwerpen om computers te beschermen tegen wormen, zichzelf vermenigvuldigende programma's die zich via netwerken razendsnel over de hele wereld kunnen verspreiden en allerlei onheil kunnen aanrichten. De onderzoekers richten zich zowel op de detectie van de wormen als op de vernietiging ervan. Het deelnemende bedrijf is TNO ICT.

Voortgang in 2006

Argos, een systeem om netwerkgegevens te analyseren en waarschuwingen te geven bij verdacht verkeer zoals de hierboven genoemde wormen, is verder ontwikkeld. Het bleek zo succesvol te zijn dat de software vrij beschikbaar is gemaakt (www.few.vu.nl/argos) en daardoor vele malen is gedownload. Hierdoor is Argos een basiscomponent geworden voor een aantal wereldwijde researchprojecten. Argos is een systeem voor netwerkservern, maar aangezien er steeds meer aanvallen komen op clients (bijvoorbeeld spam en phishing), wordt nu ook een versie voor clients gemaakt. Argos is in 2006 ook op een groot aantal plaatsen in het nieuws geweest, zoals in de Computable, Metro en Spits en is ook besproken op diverse websites.

Voor TNO ICT is dit project interessant, omdat het met de resultaten uit dit project hun netwerk monitoringsysteem Lobster Network Telescope verder hebben kunnen aanpassen. Naast TNO maken andere organisaties eveneens actief gebruik van Argos. Zo gebruikt SURFnet Argos om nieuwe (zero-day) netwerkaanvallen te detecteren. Het Franse Eurecom gebruikt Argos in een project in combinatie met andere detec-

tietechnologie. En de makers van de Nepenthes honeypot technologie (Duitsland) hebben actief bijgedragen aan uitbreidingen van Argos.

- *PINPAS JC, Program Inferred Power Analysis in Software for Java Card*
dr. Erik de Vink, Technische Universiteit Eindhoven

JavaCard lijkt een de facto standaard te worden voor smartcards. De onderzoekers willen een methode ontwikkelen die bescherming biedt tegen aanvallen op dit soort kaarten. In het bijzonder zullen de zogenaamde side-channel attacks onderzocht worden. De deelnemende bedrijven zijn STMicroElectronics en BrightSight (voorheen TNO ITSEF).

Voortgang in 2006

De onderzoekers hebben een aantal JavaCards getest die alom gebruikt worden. Het blijkt dat deze kaarten niet helemaal aan de standaardspecificaties voldoen, waardoor hun gebruik bij onverwachte gebeurtenissen (zoals het uit de kaartlezer trekken van de kaart voordat de identificatie voltooid is) minder veilig is dan verwacht. Hierdoor kan de beveiligde informatie die op die kaarten staat, toch leesbaar worden voor onbevoegden. Deze tekortkomingen zijn besproken met de instantie die gaat over het opstellen van standaards voor JavaCards. STMicroElectronics kan de resultaten van dit project gebruiken in de ontwikkeling van systemen waar smartcards onderdeel van uitmaken. Eén van de diensten van BrightSight is certificering van systemen met de Common Criteria. Zij kan de resultaten gebruiken bij evaluatie en certificering van smartcard en JavaCard systemen.

Sentinels ambassadeur

Drs. Fred Eisner, bestuurskundige met veel ervaring met ICT-industrie, overheden en onderzoek is de Sentinels ambassadeur.

Kennisuitwisseling is de belangrijkste doelstelling van de Sentinels ambassadeur. In feite is de Sentinels ambassadeur hét contactpunt voor bedrijven en instellingen die op zoek zijn naar kennis over computerveiligheid. Hij draagt resultaten uit en bemiddelt tussen vraag en aanbod. In 2008 wordt ook een Sentinels Vici-onderzoeker aangesteld, iemand die in feite hetzelfde doet, maar dan vanuit de universitaire wereld. Met de Sentinels

ambassadeur en de Sentinels Vici-onderzoeker hopen we een algemene, makkelijk toegankelijke kennisbron te hebben voor heel Nederland op het gebied van veiligheid van computers en computernetwerken.

Voortgang in 2006

In 2006 is een groot aantal gesprekken geweest met (a) bedrijven en bedrijvenkoepels zoals VNO-NCW, ECPNL en ICT-Office; (b) kennisinstellingen, Sentinels-projecten, NWO en STW; en (c) overheden, zowel over beleid (EZ en BZK) als over uitvoering (ICTU, GovCERT).

Daarnaast is Sentinels in de persoon van de ambassadeur op een aantal events vertegenwoordigd geweest.

Alle genoemde contacten, inclusief natuurlijk de 'omringende' contacten via telefoon en e-mail, worden gebruikt voor meerdere doelen. Het zijn het altijd tweerichtingsgesprekken, waarbij zowel informatie ten behoeve van Sentinels en zijn onderzoekers wordt gevraagd, als informatie gegeven wordt over Sentinels en het belang van security-onderzoek.

Uiteraard wordt ook een basis gelegd om kennis verder uit te dragen en om samenwerkingsrelaties te starten of te versterken. Sentinels is elke week in 2006 ergens op ambassadeursniveau vertegenwoordigd geweest. De actieve benadering, de contacten en de inhoud worden zeer op prijs gesteld.

Conclusie

In de eerste drie jaar van haar bestaan heeft Sentinels bewezen in staat te zijn interessant en uitdagend onderzoek te genereren. Concrete resultaten zijn onder meer de intrusion detection systemen Poseidon en Aphrodite uit het IPID project en het systeem tegen wormen Argos uit het DeWorm project. Bedrijven als Philips kunnen biometrische systemen veiliger maken door beter gebruik van templates (project ProBite), en - wat verder in de toekomst - de resultaten van het project Practical approaches to secure computation. Ook voor DRM bieden beide projecten nieuwe benaderingen. Met het JASON platform kunnen veiliger applicaties gemaakt worden, en met de resultaten van PINPAS kunnen systemen die JavaCards gebruiken verbeterd en gecertificeerd worden.

Een ander resultaat van Sentinels is dat de verschillende Sentinels-bijeenkomsten en samenwerkingsvormen hebben geleid tot een veel coherenter, publiek-privaat

georganiseerde onderzoeksgemeenschap. Ook de security professional kan deze bijeenkomsten gebruiken voor het opdoen van nieuwe kennis en het leggen van contacten met andere security professionals, beleidsmakers en onderzoekers.

Relaties met overheden en de Europese Unie zijn in 2006 ook versterkt. Veel Sentinelsonderzoekers zijn actief in EU-projecten en ook de Sentinels ambassadeur onderhoudt actief contact met EU-organisaties (zoals ENISA). Daarnaast zit een lid van de ENISA Management Board in de programmacommissie van Sentinels.

Terugkijkend kan worden geconcludeerd dat Sentinels bij velen goed op de kaart staat, en bij velen ook aanzien geniet. Sentinels onderzoek en onderzoekers zullen hier ook in de toekomst van kunnen profiteren.



Meer informatie

Meer informatie over Sentinels kan op de Sentinels website gevonden worden (www.sentinels.nl). Recente publicaties zijn het Sentinels jaarplan 2007 met onder meer de plannen van de hierboven besproken projecten in 2007 (www.sentinels.nl/library/yearplan2007.pdf) en het Sentinels jaarverslag 2006 met onder meer een uitgebreide beschrijving van de hierboven genoemde resultaten over 2006 (www.sentinels.nl/library/yearreport2006.pdf).