MEDIA PLANET

SECURITY SOLUTIONS

PROFESSIONELE BEVEILIGING OP ALLE VLAKKEN

OKTOBER 2008

OOK BEDRIJFSNETWERKEN HEBBEN EEN VERZEKERING NODIG

Stroompannes, brand, overstromingen – het zijn maar enkele van de rampen die een bedrijf tot stilstand brengen. Een business continuity/disaster recovery-plan is dan ook geen overbodige luxe

Lees blz. 6-7

BELGISCHE TECHNOLOGIE BEVEILIGT BANKTRANSACTIES

Bankfraude is niet nieuw, zolang er banken zijn is er altijd wel een of ander individu geweest dat aan de haal probeert te gaan met andermans centjes. Alleen steekt de Belgische Digipass daar een stevig stokje voor

Lees blz. 6-7

NETWERKBEVEILIGING IS EEN GIGANTISCHE KARWEI

Netwerkbeveiliging gaat dus veel verder dan louter het netwerk zelf, want naast het netwerk moet ook aandacht geschonken worden aan de beveiliging van computers

Lees blz. 9

WIE WORDT ER VERANTWOORDELIJK VOOR DE BEVEILIGING?

Een veiliger Internet begint bij beter beveiligde toepassingen en een meer bewuste eindgebruiker. Maar alleen eindgebruikers verantwoordelijk stellen voor beveiliging is onrealistisch

Lees blz. 10

iStockphoto

niet

huidige navolgerspositie moeten loslaten. En dat wordt moeilijk. Mozilla, de organisatie achter Firefox, kan jaarlijks bogen op 60 miljoen dollar van Google. OpenOffice moet het hebben van sponsoring van Sun Microsystems en zit krapper bij kas.

Daarnaast is het de vraag of OpenOffice zich niet veel meer zou moeten richten op de ontwikkeling van onlinediensten. Een teken aan de wand is dat de Amerikaanse stad Washington D.C. een contract ter waarde van 500.000 dollar met Google heeft afgesloten. Zo'n 38.000 gemeentewerkers gaan voortaan Gmail en Google Apps gebruiken, oftewel onlinekantoorapplicaties. De gemeente wil de kosten van het gebruik en het onderhoud van software zoveel mogelijk temperen.

Jan Libbenga

continu via telemetrie in de gaten gehouden. De positie van de trein werd tijdens de reis van ruim 10.000 kilometer door merendeels verlaten gebied met gps in de gaten gehouden. FOTO: REUTERS

eerplannen

versie van Microsoft Visual Studio – waarschijnlijk de 2010-versie. Parallel daaraan zullen de volgende versies van andere Microsoft-producten, zoals System Center, BizTalk Server, BizTalk Services en het .NET Framework 4, geschikt zijn om samen met Oslo te gebruiken. Die integratie wordt gefaciliteerd door het gebruik van XAML, de taal die in Windows Workflow Foudation al wordt gebruikt om workflows te definiëren.

Microsoft stelt de eerste 'community technology preview' (CTP) van Oslo beschikbaar voor ontwikkelaars op zijn Professional Developers Conference aan het eind van deze maand. De definitieve roadmap is overigens nog niet vastgesteld.

Freek Blankena/f.blankena@sdu.nl

Vaste patchdag niet ideaal voor beveiliging

■ Voorspelbaarheid goed voor beheerder, en hacker

Microsoft en Apple brachten deze week beide een serie patches uit. Microsoft doet dat elke maand op dezelfde dag. Apple doet het als het dat nodig acht. Voor beheerders is de methode van Microsoft erg werkbaar. Voor de kwaliteit van de beveiliging is dit echter niet de ideale methodiek.

Natalie Lambert, analist bij Forrester, vindt het patchproces van Microsoft beter, maar zij kijkt daarbij alleen naar de kant van de beheerders. "Zij weten zo precies wanneer ze zich moeten voorbereiden op de patches. Veel organisaties plannen diensten van hun IT'ers rond patchdinsdag zodat ze de patches kunnen doorvoeren zodra ze binnen zijn. Bij Apple kun je je niet voorbereiden op de patches. Daardoor worden beheerders gedwongen er hapsnap op te reageren."

Eddy Willems, beveiligingsspecialist bij Kaspersky, geeft de voorkeur aan de methode van Apple. "Qua beveiliging is het beter patches te laten komen als ze nodig zijn. Soms kunnen patches niet wachten. En een maand wachten op patches vind ik te lang. Een tussenoplossing zou beter zijn: twee keer per maand of zelfs wekelijks op een vast moment patches uitbrengen. Wij brengen zelf ook patches onmiddellijk uit als ze nodig zijn, desnoods elk uur."

Het bestaan van een vaste patchdag, of dat nu wekelijks of maandelijks is, heeft als nadeel dat ook criminelen van deze kennis misbruik kunnen maken.

Een maand wachten op patches is te lang

Zo werd deze week op patchdinsdag een valse e-mail uitgestuurd met een trojanvirus daarin, die van Microsoft afkomstig leek. Ook geeft het ze dan kans op zijn minst een maand nieuwe lekken te misbruiken.

Graham Titterington, analist bij Ovum, prefereert de vaste patchdag, vooral om het voordeel voor de beheerders. "Dat is zeker beter bij veel patches, maar gaat het om een paar patches, dan is sporadisch patchen ook goed. De beveiliging is er wel meer bij gebaat als er snel wordt gereageerd. Maar de meeste lekken worden pas misbruikt als de patches uit zijn en de hackers er reverse engineering op hebben toegepast."

Overigens komt Microsoft met zijn maandelijkse routine veel vaker met patches dan Apple, dat ook weleens een kwartaal op zich laat wachten. De patches die Microsoft deze week uitbracht, moeten twintig lekken dichten in onder meer Windows Vista, Server 2008, Server 2000 en Office. Daarvan zijn er negen kritiek. Daarbij gaat het om lekken die problemen opleveren in Active Directory, Excel Host Integration Server en Internet Explorer.

Tanja de Vrede/t.vrede@sdu.nl

uistheid van de geregistreerde adressen van hun inwoners

registratie blijkt onbekend

leiding, die echter nog wel gevolgd moet worden door een beschrijving van concrete stappen. Het gaat om de betrouwbaarheid van het belangrijkste onderdeel van het stelsel van basisregistraties, waarvan de hele publieke sector zich afhankelijk moet maken, maar Bijleveld legt weinig gevoel van urgentie aan de dag, vonden PvdA, CDA, VVD en SP.

Het had hun ook verbaasd dat ze geen percentage had genoemd als foutenmarge en dus ook geen termijn waarop ze als doel gehaald wilde zien dat gemeenten daarbinnen blijven. In het debat vorig najaar, aanleiding voor de motie van Heijnen en Bilder, had Bijleveld gezegd dat het foutenpercentage in de GBA op 3 à 4 procent lag. Dat in haar plan nu een percentage ontbrak, bracht Heijnen tot de vraag of Bijleveld dat cijfer dan 'uit haar mouw geschud' danwel 'maar wat geroepen' had. Daar kwam het wel op neer, bleek uit Bijlevelds antwoord. Ze voelde wel degelijk urgentie, maar was bij de voorbereiding van haar plan op 'complicaties' gestuit. Het vorig jaar genoemde foutencijfer was gebaseerd op onderzoek uit 1998 en 2002 toen 97 procent van de GBA-gegevens bleek te kloppen. Maar voor het heden was het meer een slag in de lucht, bekende ze. "Er is onvoldoende cijfermatig inzicht in de betrouwbaarheid van de GBA. Daarover hebben we onvoldoende materiaal."

Kamer wil dat foutenpercentage onder de 1 procent blijft

Bijleveld gaat nu een nulmeting doen in de vorm van een 'representatieve steekproef' uit GBA-V, het centrale verstrekkingssysteem met alle gemeentelijke bevolkingsbestanden. "Hoe bestáát het," liet Heijnen zich vervolgens ontvallen.

Bijleveld erkende dat haar Kamerbrief een lange inleiding had, maar toch ook negen maatregelen opsomde. Zoals de aanwijzing van de GBA als basisregistratie met terugmeldverplichting, de modernisering van de GBA (ligt stil wegens onvoorziene complexiteit en financieringsperikelen) en een knelpunteninventarisatie. Daarvoor was 20 augustus een bijeenkomst op haar ministerie gehouden, maar dat was volgens de staatssecretaris te kort geleden om iets over de uitkomst te zeggen. Toch is er al een verslag met een bijlage, die 94 knelpunten annex verbetersuggesties beschrijft.

Zo merkte iemand op dat een kwart van de gevallen niet is op te lossen; dan blijft een adres 'in onderzoek' staan. Tot Bijlevelds maatregelen behoren ook bestuurlijke boetes (voor burgers die zich niet adequaat laten inschrijven; wetsvoorstel komt volgend voorjaar) en de opstelling van kwaliteitsnormen, waartegen gemeenten kunnen worden geauditeerd. Willibrord van Beek (VVD) vond het maatregelen die horen bij een situatie "waarin 98 procent goed is" en om de gegevenskwaliteit op peil te houden. Maar over een aanpak om de achterblijvende kwaliteit op peil te brengen, had hij te weinig gehoord.

Er bestaan al GBA-audits waarbij alle gemeenten elke drie jaar worden getoetst op de onderdelen bestandsinhoud, verwerkingsprocessen en privacymaatregelen. Alle gemeenten zijn al tweemaal aan de beurt geweest; sinds midden 2007 loopt de derde cyclus. PricewaterhouseCoopers Advisory en KEMA Quality (die laatste in samenwerking met BMC) voeren de audits uit. Automatisering Gids heeft eind augustus gevraagd naar de uitkomsten van de eerste twee auditcycli, maar een woordvoerder van Binnenlandse Zaken, waar BPR onder valt, was er tot woensdag niet in geslaagd daar cijfers los te krijgen. "Ik beproef dat BPR heel terughoudend is en probeer dat weg te masseren."

Intussen is wel duidelijk dat de tot nu toe gehanteerde aanpak niet werkt. Die zegt iets over een 'administratieve werkelijkheid', terwijl juist zekerheid is gewenst omtrent de feitelijke situatie. Bijleveld laat nu onderzoek doen naar kwaliteitsnormen als basis voor een 'beleidskader' voor een vernieuwde audit. Wat PvdA-Kamerlid Heijnen betreft mag ze onmiddellijk beginnen om in de grote gemeenten een wijk te kiezen en huis aan huis te checken of de GBA klopt. **Peter Mom**

Atos Origin bereidt marine voor op NH90

Een van het Duitse leger geleende NH90 maakt een demonstratievlucht boven Brussel. Deze week werd bekend dat de Nederlandse Defensie een beroep doet op Atos Origin voor de technische invoering van SAP-toepassingen die nodig zijn voor onderhoud, logistiek en configuratiemanagement van de NH90's die de Koninklijke Marine in bestelling heeft. Eerder al verzorgde Atos de defensiebrede technische implementatie van de financieel-administratieve SAP DFPS-module.
De nu verstrekte opdracht maakt deel uit van het SPEER-project 'luchtketen', dat samen met 'zeeketen' en 'grondketen' de volgende stap moet zijn in het stroomlijnen van de materiële logistiek van Defensie. Het SPEER-programma is de grootste ERP-implementatie binnen de rijksoverheid, waaraan behalve Atos Origin ook partijen als IBM en PricewatehouseCoopers meewerken.

FOTO: ANP/BELGA

QUOTE

"De IT-industrie is de enige bedrijfstak die meer modegedreven is dan vrouwenmode"

Richard Stallman, motor achter de 'free software'-beweging, breekt de staf over cloud computing in een interview met The Guardian.

Clickjacking baart zorgen

■ Beveiligers uit voorzorg terughoudend met informatie

Beveiligers laten weinig los over de werking van clickjacking, waarbij hackers gebruik kunnen maken van een fundamenteel probleem dat in vrijwel alle browsers is te vinden.

Bij clickjacking wordt een kwaadaardige webpagina onder een legitieme webpagina geschoven. De gebruiker ziet daar niets van. Als hij op bepaalde plekken klikt, klikt hij in feite op knoppen van de malicieuze webpagina, die allerhande criminele acties tot gevolg kunnen hebben.

Hoe het invoegen van die kwaadaardige webpagina onder de legitieme nu precies in zijn werk gaat, houdt men angstvallig geheim. Dat moet de browserleveranciers wat extra tijd geven om een oplossing voor het probleem te ontwikkelen. De Poolse beveiligingsspecialist Michal Zalewski omschrijft het als volgt: "Een kwaadaardige pagina in domein A kan een IFrame maken dat wijst naar een applicatie in domein B waar de gebruiker op dit moment geautoriseerd is met cookies. De bovenste pagina bedekt dan delen van het iFrame met andere visuele elementen om alles te verbergen met een enkele UI-knop in domein B, zoals 'delete alles' of 'click om Bob toe te voegen als een vriend'. Dan kan het een misleidende UI aanbieden die inhoudt dat de knop een ander doel dient en deel is van site A, waarbij gebruikers uitgenodigd worden erop te klikken."

Eddy Willems, beveiligingsspecialist bij Kaspersky Labs, houdt het er voorlopig op dat "het veel weg heeft van cross-site scripting". Symantec kan ook weinig details prijsgeven, maar benadrukt "de gebeurtenissen te monitoren en onderzoek te doen". Er is nog geen sprake van een wijdverbreid misbruik van het probleem. Willems: "Maar als er niet snel iets komt, zitten we mogelijk wél met grote problemen. Zo'n aanval stop je niet zomaar. Gaat het om een bestand dat op je systeem geplaatst wordt, dan is het minder erg. Dat kun je tegenhouden met antimalware- en antivirussoftware." Hij wijst erop dat het probleem heel snel evolueert. "Theoretisch zijn massale aanvallen wel mogelijk. Dit is geen klein probleem. Een patchje is hiervoor niet genoeg; dit vereist een zeer serieuze ingreep in de browsers."

Een workaround is er al wel. Door alle browserplug-ins en scriptings uit te zetten, wordt het risico sterk verkleind. Dat beperkt echter weer wel het internetgebruik. **Tanja de Vrede**/t.vrede@sdu.nl

Mythes en paranoia over IT-gevaren rem op innovaties

■ Geïntegreerde beveiliging meer dan pointsolutions

Mythevorming over vermeende grote ICT-beveiligingsgevaren houdt veel organisaties zo bezig dat ze er niet aan toe komen de juiste zakelijke beslissingen te nemen over ICT-beveiliging. Men rent achter de vermeende gevaren aan en beperkt zich daardoor tot brandjes blussen. Bovendien wordt het budget hierdoor aan de verkeerde dingen uitgegeven. Dat stelt Gartner-analist Andrew Walls.

Volgens Walls zijn er diverse mythen die pertinent onjuist zijn. Zo is hij ervan overtuigd dat niet de hackers maar de beveiligingsindustrie aan de winnende hand is. Als bewijs hiervoor ziet hij de steeds geavanceerdere aanvallen van hackers. Als hackers de strijd hadden gewonnen, hoefden ze niet zoveel moeite te doen nieuwe aanvalsmethoden te ontwikkelen, zo redeneert Walls.

Een mythe is eveneens dat een hoger beveiligingsbudget een betere beveiliging oplevert. Uit onderzoek van Gartner blijkt juist het tegengestelde. De meeste organisaties besteden 3 tot 7 procent van het totale IT-budget aan beveiliging. Wie meer dan 7 procent hieraan uitgeeft, is zelfs slechter beveiligd dan gemiddeld omdat men dan reactief te werk gaat. Men werkt dan met pointsolutions die niet geïntegreerd zijn en tot een onoverzichtelijk geheel leiden. Wie minder te besteden heeft, werkt vaak juist veel efficiënter, stellen de onderzoekers van Gartner. Aangeraden wordt dan ook IT-beveiliging simpel te houden.

Beveiligingsdeskundigen laten zich echter te veel leiden door mythen, foute veronderstellingen en paranoia. Daardoor maken zij het voor de business moeilijker. Gartner stelt dat IT-beveiligers er juist voor moeten zorgen dat ze de business nieuwe mogelijkheden bieden en zich niet door angst laten regeren. Als voorbeeld geeft Walls het gebruik van internet en draadloze netwerktechnologie. Die technologieën werden lange tijd als onveilig beschouwd en dus weinig zakelijk gebruikt. Doordat de beveiligers een redelijk veilig framework hebben ontwikkeld waarbinnen men kan werken, rekening houdend met geaccepteerde risico's, worden deze technologieën nu alom zakelijk gebruikt.

'Niet de hackers maar de beveiligingsindustrie is aan de winnende hand'

"Veranderingen blijf je houden en bedreigingen blijven toenemen en zich ontwikkelen. Zeker is dat je je niet overal tegen kunt beveiligen. Wel kun je bepalen tegen welke bedreigingen je je wél moet wapenen en tegen welke niet. Dat scheelt al heel veel geld. Daarmee wordt beveiliging juist een middel voor zakelijke innovatie en niet langer een beperking."

Mythen zijn tevens dat hackers de industrie zouden helpen door problemen te vinden en ze te publiceren en dat wie aan de compliancy-eisen voldoet, zijn beveiliging daarmee geheel op orde zou hebben.

Tanja de Vrede/t.vrede@sdu.nl