

FOCUS

Beschikbaarheid



Hoe Kwetsbaar is uw Informatievoorziening	10
Elke Minuut telt bij KBC Securities	12
Vijf Negens op een Windows Server	14
Wie nodigde u uit? Toegangscontrole op de iSeries	16
Waarborgen voor elektronisch Zakendoen	19

News & Analysis

Solution Centre

Sign-On: Standaardisatie is niet Standaard	4
Microsoft betreedt iSeries platform	6
Consolidatiemogelijkheden iSeries uitgebreid	8
Het Laatste Woord: Benchmarking	34

Landal ontvangt 20.000 Bezoekers per Dag via Internet	1
Het Testen van Software is een Vaardigheid	24

IT Management

Basisvaardigheden voor iSeries Programmeurs: Het Begrijpen van Fysieke en Logische Bestanden	30
---	----

Product Update

Nieuwe Speler op High Availability Markt	27
Verbeterde Beveiliging bij Gebruik Host-Applicaties	27
High Availability voor combinatie xSeries & iSeries	27
noMax wordt volwassen	28

Reader Resources

Adverteerders Index	3
Agenda	33
Colofon	4
e-Server Market	32

Adverteerders Index

Adverteerder	Pagina
Bestmate	9
BlueWell	29
Brainforce	35
Brease	1
e-buzz	3
e-Finity	36
Eniac	26
Ilonx	18
Lansa	2
Rainbow Solutions	21
MSP	7
PQR	5
Symtrax	28

B-to-B e-commerce?

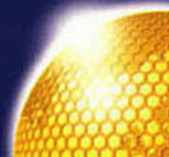
'Inkoop en verkoop via het internet'

easy-order[®]

méer dan 100.000 gebruikers via:

- Ahrend Office Products
- Corporate Express
- Despec Group
- VEN Versgroep
- Interkantoor

e-buzz bv
Tel. 0031 (0)23 555 49 49
www.e-buzz.nl





Hoe kwetsbaar is uw Informatievoorziening?

TECHNOLOGY INSIGHT

De beveiliging van automatisering mag zich niet in een warme belangstelling verheugen. Na het plaatsen van een firewall, het installeren van intrusion detection software om hackers op te sporen en het laden van antivirus software keert men terug tot de orde van de dag. Aan welke risico's een organisatie is blootgesteld, blijft meestal buiten beeld. Dat veiligheid zo'n abstract onderwerp is, komt vooral door een gebrek aan concrete informatie. Bedrijven waken er immers voor om opening van zaken te geven over wantoestanden. Juist daarom is het de moeite waard om te proberen een tip van de sluier op te lichten. Hoe kwetsbaar is uw informatievoorziening?

Door Joost Welten

Sterke Verhalen

Dat de beveiliging van computersystemen niet hoog scoort op de prioriteitenlijst van IT-managers spreekt eigenlijk vanzelf. Het is in eerste instantie een kostenpost waar geen directe baten tegenover staan. Het is verder een vertragende factor bij de oplevering van automatiseringsprojecten, die toch al onder tijdsdruk staan. Bovendien spreekt het beheersen van risico's sowieso niet tot de verbeelding, zo leert de psychologie. "Vergelijk het maar met condoor gebruik," legt Chris Verhoef uit, hoogleraar informatica aan de Vrije Universiteit van Amsterdam. "Iedereen snapt het belang van zo'n voorzorgsmaatregel, maar in de praktijk is lang niet iedereen bereid om dergelijke veiligheidsvoorzieningen ook te treffen."

De analogie met voorbehoedsmiddelen reikt nog verder. Ook in de automatisering is het namelijk betrekkelijk zinloos om mensen te willen veranderen door te wijzen op alle gevaren waaraan hun systemen bloot staan. "Als er weer eens een griezelverhaal in de krant staat over duizenden kredietkaart gegevens die voor het oprapen lagen, wordt dat al snel vermaak," vertelt Edo Roos Lindgreen, partner bij KPMG Information Risk Management en deeltijd hoogleraar IT & Auditing aan de Universiteit van Amsterdam. "Dergelijke berichten hebben eerder een averechts effect op het beveiligingsbeleid, omdat iedereen ervan uitgaat dat zijn organisatie niet zo lek is."

Muur van Zwijgen

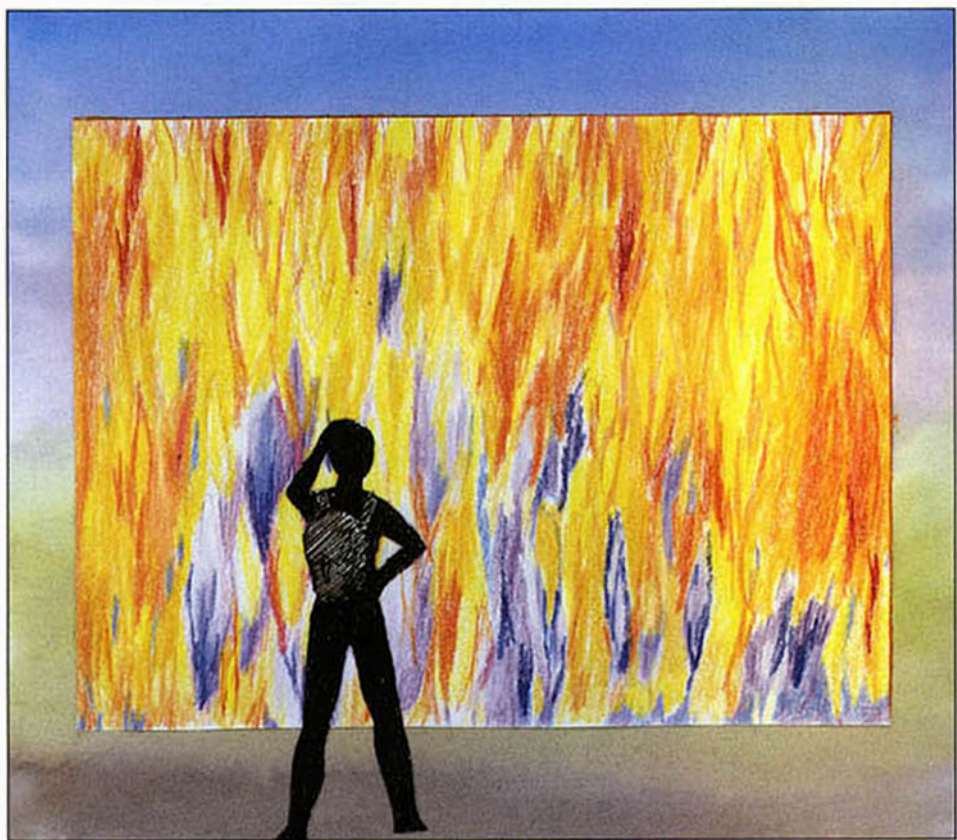
Laten we de aandacht derhalve niet richten op spectaculaire blunders of gewiekste computercriminelen, maar op de praktijk van alledag. Welke dagelijkse routines vormen de zwakke plekken in de beveiliging van automatiseringssystemen? En hoe zijn deze lekken te dichten?

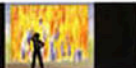
De beantwoording van deze betrekkelijk simpele vragen blijkt niet eenvoudig. De informatie die beschikbaar is over veiligheidsproblemen schiet namelijk schrome-

lijk tekort. De incidenten die bekend raken, betreffen bijna uitsluitend aanvallen van buitenaf: virussen, hacking, defacing van websites en het eerder vermelde openbaar maken van creditcard gegevens. Hoe vervelend deze vormen van computercriminaliteit ook zijn, ze vormen feitelijk slechts een randverschijnsel. Uit onderzoek blijkt keer op keer, dat 80% van veiligheidsincidenten intern plaatsvindt, waarbij eigen medewerkers de boosdoeners zijn.

Maar wat dienen we ons dienen voor te stellen bij dergelijke interne malversaties? Hier stuiten we op een muur van zwijgen. Bedrijven brengen automatiseringsproblemen en de daarmee samenhangende fraudezaken nooit in de openbaarheid, omdat de schade die ze lijden als gevolg van de negatieve publiciteit vele malen groter is dan de primaire schade.

Door dit grote zwijgen blijft er ook een geheimzinnige waas hangen rond veiligheidskwesties. Bij gebrek aan concrete





informatie rijzen al snel beelden op van zware criminelen die financiële applicaties manipuleren. De incidenten die wel in de openbaarheid zijn gekomen, laten echter zien dat de risico's in feite een alledaags en bijna banaal karakter hebben.

Gelegenheid maakt de Dief

"Dergelijke informatie komt eigenlijk alleen naar buiten als de staat zich ermee bemoeit," legt Chris Verhoef uit. "Bij parlementaire enquêtes en andere overheidsonderzoeken geldt immers het principe van openbaarheid." Zo bleek uit een onderzoek van de FBI uit het begin van de jaren negentig, dat iedereen bij een *information broker* voor 175 dollar binnen drie tot vijf dagen de volledige salarishistorie van een willekeurige Amerikaan kon kopen. Vooral werkgevers kochten deze informatie om scherpe salarisonderhandelingen te kunnen voeren met hun sollicitanten. De *information brokers* kochten deze informatie op hun beurt voor 25 dollar bij laagbetaalde werknemers van de overheid, die toegang hadden tot belastingdossiers.¹

"De gelegenheid maakt de dief," luidt het commentaar van Chris Verhoef. "Medewerkers dienen gewoon geen toegang te kunnen krijgen tot informatie die niet voor hen bestemd is." Zo iets is echter niet één twee drie geregeld. Bij de Amerikaanse belastingdienst kwam in de loop van de jaren negentig namelijk een ander schandaal aan het licht. Een medewerker van de belastingdienst, die lid was van de Ku Klux Klan, keek de belastingdossiers na van zijn mede Ku Klux Klan leden om te zien of deze geldontvingen van de FBI en dus informanten waren.²

Zowel Chris Verhoef als Edo Roos Lindgreen zijn ervan overtuigd, dat iedereen die daar enige moeite voor doet alle informatie kan inzien die binnen zijn organisatie beschikbaar is. Mijn eigen bronnen bevestigen dit. Bij verzekeringsmaatschappijen en pensioenfondsen in Nederland is het betrekkelijk eenvoudig om gegevens in te zien, bijvoorbeeld via PC's van collega's die pauzeren in de kantine terwijl ze hun applicaties open hebben laten staan. Misbruik van dit veiligheidslek kan vervelende gevolgen hebben. Voor een sollicitant kan het bijvoorbeeld onaangenaam zijn, als zijn beoogde werkgever beschikt over allerlei details uit zijn arbeidsverleden.

Het kan overigens ook anders. Zo krijgen de telefonistes van KPN geheime nummers niet op hun scherm, zodat ze ook niet in verleiding kunnen komen om die informatie toch prijs te geven. Dit laatste zou kunnen gebeuren als de beller aandringt en

een aannemelijk verhaal ophangt over kinderen die het slachtoffer zijn geworden van een ongeluk of iets dergelijks. In de Verenigde Staten is het voor medewerkers van de belastingdienst inmiddels strafbaar gesteld om bestanden in te zien die niet voor hen bedoeld zijn – een andere manier om misbruik in te perken.



Edo Roos Lindgreen, partner bij KPMG Information Risk Management en deeltijd hoogleraar IT & Auditing aan de Universiteit van Amsterdam



Chris Verhoef, hoogleraar informatica aan de Vrije Universiteit van Amsterdam

Kruipruimte

Dat gegevens gemakkelijk te raadplegen zijn, ook door personen voor wie ze niet bedoeld zijn, is eigenlijk inherent aan de automatisering. "Die automatisering is immers juist opgezet om de toegang tot data te vergemakkelijken," legt Edo Roos Lindgreen uit. Hij wijst daarnaast op een ander veiligheidsrisico, dat eveneens onlosmakelijk verbonden is met automatisering: de ongekende vrijheid die systeem- en netwerkbeheerders genieten. "De ICT-infrastructuur is de kruipruimte van een informatiesysteem, waar zelden licht binnenvalt," vertelt hij beeldend.

De systeem- en netwerkbeheerders hebben immers grote bevoegdheden om de ICT-infrastructuur naar eigen inzichten te configureren of om bestanden in te kijken. Bovendien worden zij nauwelijks gecontroleerd, simpelweg omdat niemand in de organisatie kan beoordelen wat zij nou precies doen.

"Wanneer de prestaties van netwerk en systeem tegenvallen, schakelt het management van een bedrijf vaak een externe deskundige in om een onafhankelijke audit te verrichten," zegt Edo Roos. "In veel gevallen blijkt de feitelijke configuratie van het netwerk er dan heel anders uit te zien als de officiële versie op papier." Meestal begint het met een systeembeheerder die zijn eigen homepage op de webserver van zijn baas zet. Daarna volgt de website van de voetbalclub waar de systeembeheerder lid van is. Aangemoedigd door het behaalde succes, laat hij zich daarna verleiden om tegen betaling sites van commerciële bedrij-

ven te hosten. "Vergis je niet," waarschuwt Edo Roos Lindgreen, "wij komen dit vaak tegen, ook bij gerenommeerde bedrijven. Vooral grote bedrijven met een complexe ICT-infrastructuur zijn hier vatbaar voor. Bij middelgrote organisaties met een overzichtelijke ICT-infrastructuur en één of twee systeembeheerders valt het wel mee met de wildgroei."

Een duidelijk Kader

Nou zijn systeem- en netwerkbeheerders niet uit ander hout gesneden als de rest van de bevolking. Als zij relatief vaak over de schreef gaan, komt dat doordat een duidelijk kader ontbreekt waarbinnen zij dienen te opereren. "Eigenlijk is het noodzakelijk om je bij het inzetten van ICT te houden aan de basisprincipes van de organisatiekunde," legt Edo Roos uit. "Iedereen die bedrijfskritische handelingen verricht, moet door een ander gecontroleerd worden." Van het instellen van een regelmatige audit gaat bijvoorbeeld een gezonde preventieve werking uit. Als systeembeheerders weten dat ze gecontroleerd worden, schrikken ze bij voorbaat terug voor het plegen van onregelmatigheden.

Er is ook speciale auditsoftware op de markt om de veiligheid van een automatiseringssysteem te vergroten. Dergelijke software, die bijvoorbeeld door het Nederlandse bedrijf Consul Risk Management wordt ontwikkeld, constateert afwijkend gedrag van zowel eindgebruikers als ontwikkelaars en systeembeheerders. "Het uitgangspunt is dat men niet op voorhand allerlei beperkingen in het systeem inbouwt, maar dat men eerst vastlegt wat normaal gedrag inhoudt," legt Koos Lodewijx uit, support manager bij Consul Risk Management. "Het is bijvoorbeeld normaal dat mevrouw Jansen van de boekhoudafdeling van maandag tot en met vrijdag tussen 8:00 en 18:00 uur mutaties invoert in een financiële applicatie. Wanneer zij dat op maandagavond om 23:30 uur doet, is dat echter vreemd. De software constateert dat en zendt automatisch een waarschuwing aan een beveiligingsexpert, die dan kan onderzoeken wat er aan de hand is." Eén van de grote voordelen van zo'n systeem is, dat het ook het gedrag van de systeembeheerders in de gaten houdt. Wanneer een systeembeheerder een personeelsdossier opent of code wijzigt in de financiële applicatie, komt dat meteen aan het licht.

Overigens kleven er ook beperkingen aan dergelijke auditsoftware. "In een stabiele omgeving werkt zo'n oplossing prima," verklaart Edo Roos. "Als er veel veranderingen plaatsvinden in een organisatie ➤ 31

Hoe kwetsbaar is uw Informatievoorziening?

➤ Vervolg van pagina 11

of in een automatiseringssysteem, kost het echter heel veel energie om alle instellingen actueel te houden." Voorts wijst hij erop, dat het lastig blijft om grote hoeveelheden data goed te scannen. "Een beveiligingsexpert raakt al snel overvoerd met irrelevante berichten, waardoor hij de zaken die werkelijk de aandacht vragen over het hoofd ziet," aldus Edo Roos. Verder helpt ook de beste software niet als misbruik plaatsvindt via reguliere wegen, zoals het indringen op de PC van een collega wiens wachtwoord bekend is.

Wild West Gebeuren

"Natuurlijk is het raadzaam om alle mogelijkheden aan te grijpen die op dit moment beschikbaar zijn om de veiligheid van automatisering te vergroten," geeft Chris Verhoef aan. Maar hij maakt meteen duidelijk, dat een structurele oplossing om de kwets-

baarheid van de informatievoorziening te verbeteren nog ver weg is. "De automatisering is nog steeds een Wild West gebeuren, zonder standaarden en zonder certificering."

Alleen aan de zogenaamde *embedded* software worden specifieke eisen gesteld op het gebied van veiligheid. Zo is de software voor de besturing van vliegtuigen bijvoorbeeld relatief betrouwbaar, omdat die moet voldoen aan de strenge eisen die in vliegtuig-industrie gelden. In de vrije markt van kantoor- en bedrijfsapplicaties is de consument echter overgeleverd aan leveranciers die producten leveren die aan geen enkele veiligheidseis hoeven te voldoen. "Als iemand zonder toestemming 100 Euro uitgeeft via een kredietkaart van zijn bedrijf, valt hij in een heel maas van regelgeving. Bedrijfskritische informatie die een vermoegen waard is, bevindt zich echter in een

organisatorisch vacuüm. Dat is toch eigenlijk onbegrijpelijk?" is de retorische vraag van Chris Verhoef. Veiligheid en automatisering zullen nog geruime tijd op gespannen voet met elkaar blijven staan... ■

Joost Welten is redacteur van BlueWell Magazine.

U kunt hem bereiken op J_Welten@bluewell.nl.

¹ Bron: Michael Betts, 'Personal data more public than you think', in: *Computerworld*, 09.03.1992, pag. 1

² Bron: Associated Press. 'Bill Would Tell I.R.S. Workers Not to Snoop', in: *New York Times*, 08.04.1997, pag. A9.