

INTERNE VEILIGHEID BLIJFT STIEFKIND

Consul Risk Management

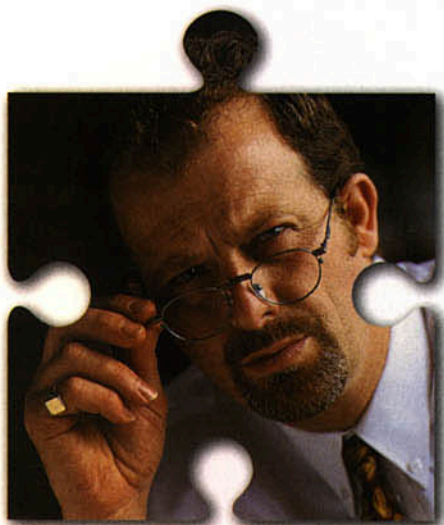
Er wordt nog immer te weinig gedaan aan interne IT-veiligheid. Te vaak wordt gekeken naar de beveiliging van het netwerk voor indringers van buitenaf, terwijl juist de meeste inbreuken op de security policy komt vanuit de organisatie zelf. Aangezien ook in de media vrijwel geen aandacht is voor het onderwerp en ook regeringsleiders zich meer richten op cyberterrorisme, komt het bewustwordingsproces bij het hoger management over dit onderwerp slechts traag op gang.

Dat waren zo'n beetje de conclusies tijdens de bijeenkomst *Omgang met risico's en bedreigingen in de samenleving ten gevolge van open IT-netwerkomgevingen*, gehouden op het

hoofdkwartier van Consul Risk Management in Delft. De bijeenkomst werd gehouden vanwege de lancering van twee nieuwe versies van Consuls belangrijkste producten eAudit en zSecure. Onder meer Chris Verhoef, Professor Computerwetenschappen en Informatie Management aan de VU, Eric Nieuwland, manager IRM bij KPMG, Paul Wielaard, Programmamanager Informatiebeveiliging bij het Ministerie van Verkeer en Waterstaat en Jos Jennekens van IBM gaven daar hun visie over IT-beveiliging.

Volgens een onderzoek van KPMG eerder dit jaar blijkt in Europa slechts de helft van al het geïmplementeerde veiligheidsbeleid vastgesteld te zijn op directioniveau. Maar liefst 29 procent van iets wat op een veiligheidsbeleid lijkt, is niet formeel goedgekeurd. Overigens steken deze cijfers nog goed af bij de Amerikaanse cijfers, waar maar liefst 43 procent van de bedrijven zonder officieel vastgesteld veiligheidsbeleid de dagelijkse routine afdraait. Vervolgens blijkt dat de meeste aandacht binnen dat wel of





niet officieel vastgestelde beleid gaat naar de beveiliging van Internet en Intranet plus een virusafweersysteem. Het rapporteren van incidenten staat vrijwel het laagst op de beveiligingsladder, hoewel dat vergeleken met de aandacht voor de beveiliging van PDA's en handhelds nog meevalt. 54 Procent om 34 procent!

Opmerkelijk is verder dat veel ondernemingen de *security-awareness* bij henzelf groter acht dan die bij hun klanten. De meesten vinden hun klanten zelfs amper op de hoogte van security noodzakelijkheden. Niettemin bleek uit de *security survey* van KPMG dat slechts 35 procent van de ondervraagden een gestandaardiseerde meetmethode gebruikt om de uitvoering van de security policy te controleren.

CEO Koen Bouwers van Consul Risk Management is eveneens altijd goed zijn toehoorders schrik aan te jagen. Hij presenteerde cijfers van het Amerikaanse Federal Bureau of Investigations (FBI) en die zijn niet mis. Zo heeft 85 procent van de bedrijven in 2001



gaten in de beveiliging ontdekt. Het totale verlies van 35 procent van die bedrijven zou 378 miljoen dollar bedragen. Zo'n 80 procent van de fraude via het bedrijfsnetwerk komt van binnenuit, zo hield Bouwers zijn gehoor voor.

In de Verenigde Staten gaan de uitgaven in security in de komende tien jaar het tienvoudige omhoog. Daarnaast gooit het gros, 80 procent, het eigen netwerk nog meer open door het Internet in toenemende mate te gebruiken als key port voor business processen. 'Het wordt steeds lastiger voor IT-beveiligingsfunctionarissen een oplossing te zoeken waarmee de veiligheid van meerdere platforms en applicaties is gewaarborgd', zegt Bouwers.



De diverse administrator- en auditing tools geven ieder hun eigen meldingen en rapporten, waaruit ook nog eens niet altijd valt op te maken of het een vals alarm is, zo geeft Bouwers aan.

Meer informatie:
www.consul.com
www.nexteconomy.nl/magazine

NIEUWE VERSIES

Consul Riks Management heeft nieuwe versies gelanceerd van twee audit- en admin-applicaties.

CONSUL EAUDIT 4.0

eAudit meet en managed essentiële onderdelen van de IT-netwerkbeveiliging. Het organiseert onoverzichtelijke registraties van uiteenlopende netwerkactiviteiten van diverse platforms en toepassingen naar een geïntegreerd security managementsysteem.

De nieuwe versie zorgt voor een real-time overzicht in een zo geheten dashboard. Security professionals kunnen met het dashboard elke gebeurtenis snel en in detail doorgronden en direct op een werkelijke dreiging reageren. Daarnaast is een wizard toegevoegd dat het opstellen van een security policy makkelijker maakt. Vanaf dat fundament is het mogelijk een specifiek allesomvattend beveiligingsbeleid te creëren. Door de toevoegingen in de rapportage van de twee elementen *waarheen* en *waarvandaan* is het nu ook mogelijk valse alarmeringen eruit te filteren.

CONSUL ZSECURE 1.3

zSecure meet en managed mainframes. Het is geoptimaliseerd voor IBM's nieuwe z/OS, maar werkt ook op andere platformen als OS/390, VM/ESA en z/VM. zSecure is verkrijgbaar voor RACF of ACF2 onder OS/390 2.6+ of z/OS. De compatibiliteit met IBM's z/OS 1.3 is in de nieuwe versie geoptimaliseerd. 'Vergeleken met de standaard RACF interface is het gebruik van zSecure 50 procent kostenverlagend. Het biedt meer functies dan zijn voorganger is is nog gebruikersvriendelijker', zegt Bouwers.