

# Persbericht

## CONTACTPERSONEN:

**PricewaterhouseCoopers**  
Daniel Evrard, partner  
E-mail: [daniel.evrard@pwc.be](mailto:daniel.evrard@pwc.be)  
Tel.: 02/710.72.00

**CIO Magazine**  
Karen Fogerty  
[fogerty@cxo.com](mailto:fogerty@cxo.com)  
508-935-4091 (kantoor)

**PricewaterhouseCoopers**  
Marc Sel, directeur  
E-mail: [marc.sel@pwc.be](mailto:marc.sel@pwc.be)  
Tel.: 03/259.34.10

## VERANTWOORDELIJKE COMPUTERBEVEILIGING HEBBEN ZWARE DOBBER AAN VEILIGHEIDSBEDREIGINGEN

*'s Werelds grootste computerbeveiligingsstudie van CIO Magazine en PricewaterhouseCoopers LLP onthult een zwakke strategische planning en gebrekkige naleving van de regelgeving*

**Brussel – 07 oktober 2005** - Meer dan 8.200 verantwoordelijken computerbeveiliging (waarvan 31% in Europa) hebben een zware dobber aan veiligheidsbedreigingen en -incidenten, volgens 'State of Information Security 2005', 's werelds grootste computerbeveiligingsstudie die uitgevoerd werd door CIO Magazine van IDG en PricewaterhouseCoopers. In 2004 werden er gemiddeld 704 veiligheidsgelateerde gebeurtenissen gemeld. In de studie van dit jaar is dit cijfer opgelopen tot 862, een stijging met 22,4%. 22% van de organisaties zegt financiële verliezen geleden te hebben door deze gebeurtenissen, een significante stijging ten opzichte van de 7% van vorig jaar. De meeste gebeurtenissen zijn te wijten aan hackers, zij zijn verantwoordelijk voor 63% van de aanvallen, in vergelijking met 66% in 2004, gevolgd door werknemers (33% versus 28%) en voormalige werknemers (20% versus 21%). Voor het tweede jaar op rij is kwaadaardige code (bijv. computervirussen) de meest voorkomende soort aanval: dit jaar 59% van de aanvallen; het jaar voordien 53%.

Scott Berinato, hoofdredacteur van de magazines CIO en CSO, licht toe: "In alle domeinen van beveiliging volgen de geleidelijke verbeteringen elkaar op, ook in het domein van de uitgaven. Toch worden die verbeteringen ver overtroffen door de complexiteit en de omvang van de dreigingen waarmee de professionals van computerbeveiliging te maken krijgen. In de strijd met uiterst intelligente tegenstanders slagen ze er gewoonweg niet in om een kwetsbare IT-infrastructuur te verdedigen en beheren."

Als een gevolg van de voortdurende bedreigingen zijn de beveiligingsuitgaven globaal bekeken gestegen van 11% van het IT-budget van de onderneming in 2004 tot 13% dit jaar. In Europa ligt deze verhouding op 12,3%, maar bijna 40% van de Europese deelnemers geeft een status-quo aan in vergelijking met 2004. Het geld voor de beveiligingsuitgaven is volgens de respondenten afkomstig van verscheidene interne groepen. Volgens 58% van de respondenten gaat de IT-afdeling over het beveiligingsbudget, volgens 19% is dit de financiële afdeling.

Dit jaar stelt zo'n 40% van de respondenten dat de onderneming een chief information security officer (CISO) of chief security officer (CSO) in dienst heeft, tegenover 31% in 2004. Die functies rapporteren aan het Directiecomité (17%), de Algemeen Directeur (29%), de Directeur Informatica (25%) of andere directie- of managementfuncties.

Wat de strategie betreft, zegt slechts 37% van de respondenten dat er in zijn onderneming een beveiligingsplan werd ingevoerd. Slechts 24% verwacht dat er in het komende jaar zo'n plan opgesteld zal worden. Bij de organisaties die een CISO of CSO hebben, bedraagt het percentage dat beschikt over een beveiligingsplan 62%.

De studie wijst uit dat, al liggen de Europese ondernemingen binnen het gemiddelde dat qua informaticastrategieplan op wereldvlak wordt genoteerd, ze minder actief zijn op het vlak van de implementatie van effectieve maatregelen zoals een gecentraliseerd beheer van de beveiliging en de periodieke evaluatie van de met veiligheid samenhangende risico's. Als factoren die naar voren worden geschoven als hindernissen voor een goede implementatie van beveiliging beschouwen de Europese ondernemingen de volgende als de belangrijkste: een beperkt budget (meer dan 55%), een tekort aan personeel (40%) en het feit dat beveiliging te weinig tijd en prioriteit toebedeeld krijgt (40%).

“Beveiliging is geen doel op zich”, verklaart Daniel Evrard, Partner bij PricewaterhouseCoopers Enterprise Advisory. “Beveiliging moet een antwoord bieden op de strategische en operationele bekommernissen van de onderneming, zoals het zich openstellen voor handelspartners of het opnemen van nieuwe entiteiten binnen een groep, en tegelijkertijd ermee rekening houden dat het noodzakelijk is dat de vertrouwelijke commerciële gegevens worden beveiligd en de reglementaire verplichtingen in acht worden genomen. De dialoog tussen de directie en de informaticadiensten is van essentieel belang om te verzekeren dat de ingezette middelen toereikend zijn voor de noden. Hoewel de studie wat beveiliging betreft op een betere samenwerking tussen IT en de rest van de onderneming wijst, hebben de ondernemingen het nog moeilijk om de problematiek in haar geheel te beschouwen.” Marc Sel, Director binnen de afdeling Process Improvement – Information Protection van PwC Enterprise Advisory, vult aan: “Om tot een efficiënte beveiligingsoplossing te komen, moet men in de hele onderneming – niet alleen maar op het niveau van het departement Informatica, tot een evenwicht komen tussen mensen, processen en technologieën. De onderneming die deze principes effectief instelt heeft meer kans om tot een veiligheidsniveau te komen dat aangepast, efficiënt en economisch verantwoord is.”

De resultaten van het onderzoek worden uitvoerig besproken in het nummer van *CIO Magazine* van 15 september en het oktobernummer van *CSO Magazine* in een reeks artikels van de hand van Berinato en onderzoeksredacteur Lorraine Cosgrove. De besprekingen zullen ook on line beschikbaar zijn op [www.cio.com](http://www.cio.com) en [www.csonline.com](http://www.csonline.com). Informatie over het onderzoek is ook te vinden op [www.pwc.com/security](http://www.pwc.com/security).

## Methodologie en profiel van de respondenten

'Global State of Information Security 2005', een wereldwijde studie door *CIO Magazine* en PricewaterhouseCoopers, werd online uitgevoerd van 14 maart tot 23 april 2005. Lezers van *CIO Magazine* en *CSO Magazine* en cliënten van PricewaterhouseCoopers over heel de wereld hebben deelgenomen aan het onderzoek via e-mail. De resultaten zijn gebaseerd op de antwoorden van meer dan 8.200 CEO's, CFO's, CIO's, CSO's, vice-presidenten en personen die instaan voor IT en gegevensbeveiliging uit 63 landen. De foutmarge voor deze studie is 1%.

De studie vertegenwoordigt een hele waaier sectoren, waaronder computergelateerde productie en software (11%), advies en professionele dienstverlening (11%), financiële diensten/banken (9%), regering (9%), onderwijs (7%), gezondheidszorg (5%), telecommunicatie (5%) en transport (5%).

Tweëndertig procent (32%) van de kaderleden die deelnamen aan het onderzoek, werkt in een organisatie met een totale jaaromzet van minder dan 100 miljoen USD. Volgens zeventien procent (17%) van de respondenten bedraagt de jaaromzet van hun organisatie tussen de 100 miljoen en 999,9 miljoen USD en volgens eenentwintig procent (21%) is deze groter dan 1 miljard USD. 17% van de respondenten werkt in een non-profitorganisatie en kon bijgevolg geen omzetcijfer meedelen. 12% heeft ervoor gekozen deze vraag niet te beantwoorden.

54% van de respondenten bekleedt een IT-functie, waaronder CIO, CTO (chief technology officer), vice-president, directeur en manager, terwijl 10% computerbeveiligingsspecialist is. Twaalf procent (12%) van de respondenten is CEO, CFO of niet-IT-directeur, terwijl 24% "andere" ingevuld heeft als functie.

## Over *CIO Magazine*

*CIO Magazine* werd voor het eerst gepubliceerd in 1987. Het behandelt onderwerpen die van vitaal belang zijn voor het succes van chief information officers (CIO's) over heel de wereld. De CIO-portfolio omvat een website ([www.CIO.com](http://www.CIO.com)), CIO Executive Programs en de CIO Executive Council™. CIO voorziet technologie- en bedrijfsleiders van analyses en uitleg inzake tendensen op het gebied van de informatietechnologie en een duidelijk inzicht in de rol die IT speelt in het bereiken van de bedrijfsdoelstellingen. De Amerikaanse uitgave van het tijdschrift en de website heeft totnogtoe 140 prijzen gewonnen, waaronder twee 'Grand Neals' van Jesse H. Neal National Business Journalism Awards en twee keer 'Magazine of the Year' van National Society of Business Publication Editors. *CIO Magazine* wordt uitgegeven in meer dan een dozijn landen, waaronder Australië, Canada, China, Frankrijk en Duitsland. De CIO Executive Programs - een reeks fysieke conferenties, waaronder CIO Perspectives® en CIO 100 Awards & Symposium™ - bieden opleidings- en netwerkkansen voor voorgekwalificeerde ondernemings- en regeringsleiders. De CIO Executive Council is een professionele organisatie van CIO's die werd opgericht om blijvende verandering tot stand te brengen in kritieke sector-, universiteits-, media- en regeringsgroepen. *CIO Magazine*, *CIO.com*, de CIO Executive Programs en de CIO Executive Council zijn een product van CXO Media Inc., de bekroonde bedrijfseenheid van International Data Group.

## Over PricewaterhouseCoopers

PricewaterhouseCoopers ([www.pwc.com](http://www.pwc.com)) verleent sectorgerichte diensten op het vlak van audit, fiscaliteit en adviesverlening voor klanten in zowel de openbare als de privé-sector. Meer dan 120.000 medewerkers in 144 landen delen, onderling en met de klant, hun inzichten, ervaring en oplossingen. Dat heet 'connectedthinking\*'. Deze manier van werken versterkt het publieksvertrouwen in de bedrijfswereld en creëert extra waarde voor de klant en zijn stakeholders. 'PricewaterhouseCoopers' verwijst naar het netwerk van firma's die deel uitmaken van PricewaterhouseCoopers International Limited. Elke firma is een afzonderlijke en onafhankelijke juridische entiteit.

Het PwC Information Protection Team in België heeft een ruime ervaring in het uitvoeren van beveiligingsopdrachten. Dit omvat het uitwerken van de strategie en beleidslijnen voor computerbeveiliging, alsook het opstellen en uitvoeren van een beveiligingsplan inclusief het definiëren van processen en procedures voor beveiligingsbeheer. Verder beschikt het team over ervaring met smart cards zoals de elektronische identiteitskaart en de nieuwe tachograaf. In het kader van deze projecten analyseert PwC ook de uitvoerbaarheid en opportuniteit van het invoeren van geavanceerde technologieën zoals versleuteling, biometrie en pet's (privacy enhancing techniques). Uiteraard behoren gespecialiseerde security reviews ook tot het takenpakket. Voor meer informatie kunt u contact opnemen met Daniel Evrard (02/710.71.02) of Marc Sel (03/259.34.10).

###