

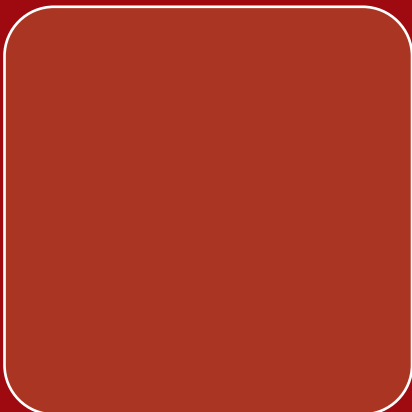
RONDE TAFEL

# Computerbeveiliging



**Eddy Dobbelaere,**  
Managing Director Porthus

**Louis Lempereur,**  
General Manager Celem  
Computers



**Peter Ryckaert,**  
CEO DigiPoint



**Fabrice Wuyts,**  
Afgevaardigd beheer-  
der Proximedia

**Marc Van De Verre,**  
Oprichter Extra Consult



## Hoe zit het met de veiligheid van uw computers?

Het gebruik van informatica schept heel wat mogelijkheden voor het bedrijfsleven. Helaas zijn maar weinig ondernemers zich bewust van de risico's die zij daardoor lopen: virussen, gegevensvervalsing, diefstal van materiële dragers, vernietiging van hard- en software bij voorbeeld wanneer er brand uitbreekt, bij wateroverlast, blikseminslag, enz...  
Wat voor voorzorgen nemen de KMO's?

**D**AT DE GEVOLGEN VAN EEN ONVOLDOENDE beveiliging van het systeemmateriaal desastreus kunnen zijn voor de zaak, wordt bevestigd door de zeven deelnemers aan de 'Ronde Tafel'. De problemen waarmee zij te maken kregen, zijn overigens zeer uiteenlopend van aard. Virusat-tacks komen veelvuldig voor. Nog fris in het geheugen ligt het 'I LOVEYOU' virus dat enkele jaren geleden de kop opstak. Eén van de deelnemers heeft na dit virus de e-mail filtering verscherpt, zodat actieve componenten uit alle binnenkomende e-mails worden verwijderd. Elders waren er problemen met een ex-medewerker die met het paswoord van een collega via een modemconnectie probeerde binnen te dringen in het netwerk. Anderen hebben dan weer last van denial-of-service attacks, virussen allerhande of brutale force password attacks. Ook zien zij het SPAM-verkeer hand over hand toenemen.

**Louis Lempereur:** "Er wordt nog altijd niet genoeg in computerbeveiliging geïnvesteerd, veel mensen nemen zelfs niet de moeite om reservekopieën te maken, wat nochtans heel simpel is. Wij van onze kant hebben al last gehad van virussen, en onze site is al meerdere malen "aangevallen". ▶

### Deelnemers

**Pascal Saesen**, ICT Manager Microfibres Europe

**Wim Polfliet**, Manager EM DataCenter, member of EM Group

**Marc Van De Verre**, Oprichter Extra Consult

**Eddy Dobbelaere**, Managing Director Porthus

**Peter Ryckaert**, CEO DigiPoint

**Louis Lempereur**, General Manager Celem Computers

**Fabrice Wuyts**, Afgevaardigd Beheerder Proximedia



**Wim Polfliet:** *"Dit is ons allemaal gespaard gebleven, tot nog toe, maar wij hebben dan ook een uitstekende firewall en virusbeveiliging."*

**Fabrice Wuyts:** *"Als leverancier van internetdiensten krijgen wij dagelijks met zulke problemen te maken. Met de regelmaat van een klok proberen hackers onze webservers binnen te dringen, maar goed dat die beschermd zijn. Wij hebben zo'n 10 000 mailboxen waar iedere dag minstens 40 000 mails binnenkomen, wel 40% daarvan worden door onze antivirus server geblokkeerd, en dit is nog maar één voorbeeld."*

**OMZETVERLIES.** Dat 'aanvallen van buitenaf' tot omzetverlies leiden, lijkt logisch, maar ook op dit punt krijgen wij heel uiteenlopende verhalen te horen. Een deelnemer heeft door dergelijke aanvallen wel 15 werkdagen verloren zien gaan, gespreid over één of meerdere jaren. Bij een ander heeft de omzet niet geleden, wel ging er veel tijd verloren. Als gevolg van die aanvallen worden ook maatregelen genomen om mensen en materieel te beschermen.

**Peter Ryckaert:** *"Dankzij onze beveiliging hebben 'aanvallen van buitenaf' geen impact op de omzet. Aan de andere kant zijn er wel extra kosten: er zijn extra manuren door de overbelasting van het beveiligingssysteem en dit heeft dan weer gevolgen voor de rendabiliteit."*

**Fabrice Wuyts:** *"Onze omzet heeft daar gelukkig nog niet onder geleden, maar dit is ook normaal, want ten slotte is informaticabeveiliging een onderdeel van onze bedrijfsactiviteit."*

**WIE BEVEILIGT?** Alle deelnemers om de tafel zijn het met mekaar eens: computerbeveiliging is een interne kwestie. De een heeft daar speciaal opgeleide technici voor, een ander zet daar sinds kort twee medewerkers voor in, en zij doen dan het meeste beveiligingswerk. Een derde deelnemer heeft daar eveneens twee mensen voor ingezet, en nummer vier heeft een security officer, hij rapporteert aan de managing director en wordt geassisteerd door een security engineer. Daarnaast heeft de firma een support-

overeenkomst met een externe security-specialist. Een van de rondetafelgasten vertrouwt op de eigen expertise: de eigen medewerkers worden op tijd en stond bijgeschoold om op de hoogte te blijven van de nieuwste anti-virus en firewalling technieken.

**Pascal Saesen:** *"Wij beveiligen intern, maar we schakelen ook een externe firma in. De interne medewerker houdt zich bezig met het strategiedeelte. De systeembeheerder gaat over de antivirus- en antispamprogramma's."*

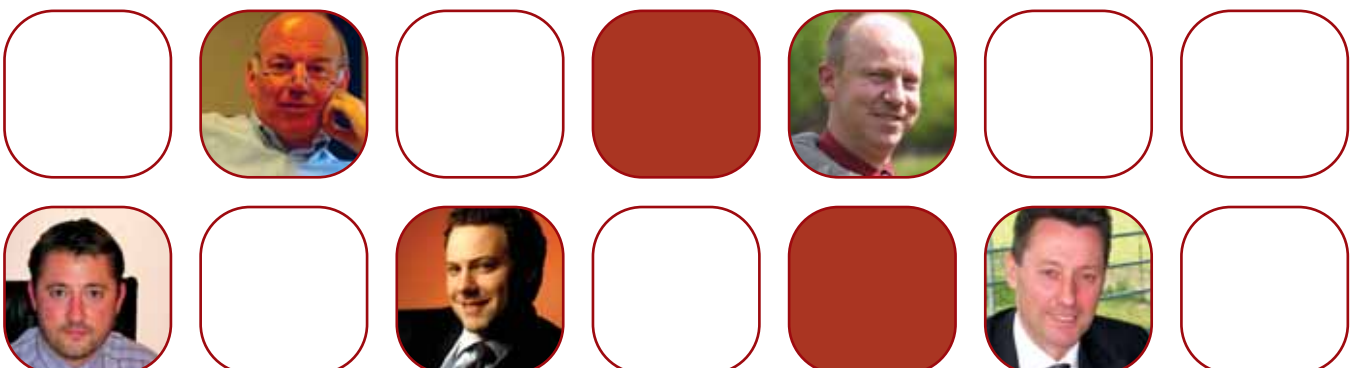
**Fabrice Wuyts:**  
**"Onze omzet heeft daar gelukkig nog niet onder geleden, maar dit is ook normaal, want ten slotte is informaticabeveiliging een onderdeel van onze bedrijfsactiviteit."**

**BEVEILIGINGSBELEID.** Veel bedrijven hebben nog steeds geen duidelijk beveiligingsbeleid maar dit begint nu stilaan te veranderen. Eén van onze sprekers heeft een portal site waar de klant informatie over de projecten kan opvragen en (vertrouwelijke) gegevens uitwisselen met andere bezoekers, maar men kan gerust zijn: de portal is zowel on als off line beveiligd. Elders wordt de omgang met kritieke informatie geregeld in de arbeidsovereenkomst. Of er

zijn policies rond security ontwikkeld. Hierin staat onder meer hoe men dient om te springen met security updates afkomstig van software vendors, met de toegang tot de data, de back-up, de restore, de VPN toegang van internet, enz... Eén van de deelnemers geeft toe dat er geen strikte controle is op in- en uitgaand dataverkeer, behalve als men vermoedt dat er misbruik in het spel is.

**Fabrice Wuyts:** *"Ons reglement is heel simpel: alle gegevens worden twee keer gesaved, en dit gebeurt extern en on line aan de hand van onze back-up software."*

**CONCREET.** Een voor de hand liggende maatregel, zijn de back-ups. Een van de deelnemers aan het debat heeft een Uninterruptable Power Supply beveiliging of UPS voor zijn server, om netwerkstoringen te voorkomen. De kritieke gegevens worden twee keer per dag op een laptop opgeslagen en 's avonds komt er nog eens een volledige back-up op een externe harde schijf. Die harde schijf gaat dan mee naar huis. Binnenkort zullen de gegevens van de server weggeschreven worden naar een tweede computer ►



die in een dedicated room bij een externe firma komt te staan. Een andere deelnemer meldt dat de belangrijkste informaticacomponenten extra muros zijn opgeslagen in beveiligde, brandvrije back-up ruimtes.

**Louis Lempereur:** "Als concrete maatregel geldt bij ons dat alle kopieën het huis uitgaan."

**Fabrice Wuyts:** "Daar hebben wij ons eigen on line back-up programma voor, Dataprotex, dat wij trouwens ook in de handel brengen. Wij werken met twee gedecentrali-

seerde back-up servers (in twee telecom-centers), waar de gecodeerde back-ups van onze klanten (en die van ons ook natuurlijk), veilig onder de pannen zijn. Wij hebben trouwens ook een Belgische portaalsite voor computerbeveiliging [www.dataprotex.be](http://www.dataprotex.be)."

**Eddy Dobbelaere:** "Onze firma heeft al het mogelijke gedaan om computerschade te voorkomen, en op die manier zijn wij uitgekomen op een 'state of the art' data-center met waterpreventie, UPS om stroomuitval op te vangen, en een dieselgenerator als bescherming tegen een eventuele UPS-uitval. Indien deze maatregelen toch onvoldoende zouden blijken, ligt er in ieder geval een compleet rampenplan klaar waarin alles keurig geregeld is: de restauratie van de meest kritische bedrijfsgegevens, de opbouw van een werkomgeving in een remote datacenter."

**INVENTARIS.** Niet alle ondernemingen beseffen hoe belangrijk het is om hun systeemateriaal jaarlijks te inventariseren, hoewel er forse bedragen mee gemoeid zijn. Aan tafel wordt grif toegegeven dat men op dit punt wel eens verstek laat gaan. Eén van de deelnemers beschikt over een gegevensbank waarin alle servers opgenomen zijn naast de netwerkcomponenten met hun configuratie.

**Louis Lempereur:** "Wij hebben een inventaris opgesteld van al ons computermateriaal, zowel hard als soft; daarnaast heb je natuurlijk veel programma's die direct van het internet komen en die kun je moeilijk opnemen."

**Fabrice Wuyts:** "Wij hebben ook zo'n inventaris van al ons huidig materiaal."

**NOODPLAN.** Hoewel een noodplan essentieel is om bepaalde situaties het hoofd te kunnen bieden, hebben niet alle bedrijven er een, laat staan dat zij zo'n plan op zijn operationele waarde zouden hebben uitgetest. Eén van de deelnemers zegt geen officieel plan te hebben, maar als de nood aan de man komt heeft men alles bij de hand. Iemand anders heeft het over een automatische systeem monitoring en een 24 op 24 uur permanentie voor noodgevallen.

Een derde heeft zelfs meerdere noodplannen klaarliggen afhankelijk van de aard en de ernst van het incident.

**Marc Van De Verre:** "Extra Consult heeft een heel kleine structuur en kan daardoor flexibel reageren op tegenslagen. Valt er een server weg, dan kan dit in één dag rechtgezet worden. Binnen een tijdspanne van acht uur staat de nieuwe server er al, geconfigureerd en wel, klaar voor gebruik. Als klant/leverancier zal men daar niets van merken omdat hier iedereen een laptop van de zaak en thuis een internetaansluiting heeft. Wij zijn met ande-

re woorden nooit volledig afhankelijk van de server in de Brusselse hoofdzetel."

**Fabrice Wuyts:** "Wij hebben hier ook al enkele schijven zien crashen, en toen hebben wij iedere keer een nieuw back-upstelsel moeten opstarten. Nu, dit ging allemaal gesmeerd, precies omdat wij iedere dag back-uppen, daar hebben wij namelijk een programma voor dat alles automatisch doet."

**Pascal Saesen:**  
"Wij beveiligen intern, maar we schakelen ook een externe firma in. De interne medewerker houdt zich bezig met het strategiegedeelte. De systeembeheerder gaat over de antivirus- en antispamprogramma's."

