Tendencias

En su carrera contra las amenazas, las reales y las sobredimensionadas, proveedores y consultoras de seguridad encontraron en el empleado a una nueva fuente de temor para los CIOs e incipientes CSOs.

La seguridad paranoica

Nada es seguro. Bajo esa premisa, los jugadores del mercado de protección de datos no paran de crecer intentando alcanzar un objetivo que ellos mismos reconocen como inalcanzable: la empresa impenetrable. Las amenazas constantes y el valor cada vez más alto de la información que acumulan las compañías conducen a que, con una pequeña ayuda del marketing de los proveedores, la inversión en este tipo de tecnologías no pare de crecer.

Según un informe de PricewaterhouseCoopers (PwC), al que tuvo acceso exclusivo INFORMATION TECHNOLOGY, en la Argentina el 44 por ciento de las empresas aumentó su inversión en seguridad y sólo un 3 por ciento la disminuyó. De acuerdo con Edgardo Sajón, socio de PwC, dos fuentes explican este crecimiento. "Una regulatoria, que es clave, y otra es la necesidad crítica del negocio por proteger su información", fundamenta.

"Los datos son vitales en segmentos como telecomunicaciones, bancos y otros similares —prosigue Sajón—. Pero cada vez más la preocupación por la calidad de la información ingresa a lugares hasta hace poco impensados, como un canal de televisión o una radio."

Por su parte Andrés Gil, socio de Servicios de Riesgo Empresarial de la consultora Deloitte, reconoce que ve en las empresas "una conciencia mayor" con respecto a la seguridad. "Las compañías se dieron cuenta de que los ataques las afectan más allá de los sistemas. Sin embargo, en lo que hace a presupuesto y estructura todo es muy incipiente", reconoce.

Enemigo interno

Una tendencia que crece desde hace unos años es ver a los empleados como la fuente más probable de un ataque. Según los datos de PwC, mientras que en 2005 sólo el 33 por ciento de las empresas lo marcaban como una preocupación y en 2006 ese número se mantenía estable en 32 por ciento, durante 2007 esta inquietud se extendió al 48 por ciento de los encuestados. Por el contrario, el 21 por ciento de las compañías manifestó temores hacia ex empleados y el 41 hacia hackers.

Si bien estos datos son mundiales, en la Argentina el temor al atacante interno no es la principal preocupación: es una prioridad para el 33 por ciento de las empresas, mientras que la amenaza del hacker encabeza el podio de las pesadillas del 47 por ciento de los CIOs.

Diego Taich, gerente de PwC, cree que esta tendencia está creciendo desde hace tiempo. "Antes el miedo mayor era al hacker, pero ahora hay mucho temor al empleado —explica—. Esto se debe a que esta persona tiene acceso a datos sensibles por su función de negocio, pero la empresa no sabe qué hace ese trabajador con esa información." Además, según Sajón, los miembros de una firma saben cómo son los procesos del negocio y pueden usar ese conocimiento contra la propia compañía en caso de decidir hacerlo.

Desde RSA, empresa de seguridad informática adquirida por EMC, Antonio Moraes, director de Ventas para América latina, remarca que "estas amenazas son mayores en las empresas grandes. En una compañía de 20.000 empleados siempre va a haber una manzana podrida. Hay que tener mucho cuidado porque a esto se le suma el hecho de que los datos están en movimiento. Primero están en el data center, luego en una planilla de cálculo y todo puede terminar en un e-mail o en un pendrive. Hay que hacer un monitoreo muy cercano para ver qué está pasando".

Para disminuir la importancia de este factor en el rango de posibles ataques, hay que tener en claro cuál es el rol de la capacitación. Sin embargo, Gil cree que tampoco se pueden esperar milagros. "Aún con cursos y clases al respecto, el punto más débil es el usuario. Por eso, si hay una puerta virtual que no se debe abrir, el empleado no debe tener posibilidad física de hacerlo".

El ejecutivo destaca que actualmente otras preocupaciones de las

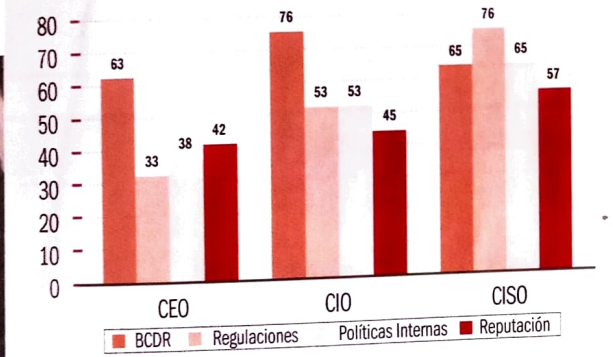
empresas son las notebooks y los teléfonos celulares como portadores de información. El hecho de que un empleado pueda conectarse en un bar y luego ingresar a la red corporativa con la máquina infectada genera mucha preocupación en los CIOs, quienes así se encuentran frente a una elección difícil: los beneficios productivos de la libertad o un ambiente más controlado.

Riesgo positivo

Pese a todas las herramientas disponibles, la seguridad total no existe. De hecho Moraes, pese a ser proveedor —o quizás por eso mismo—, reconoce que "desafortunadamente" no existe riesgo cero. "Esto sería estar encadenado, cerrar las puertas y que nadie trabaje. Y, como obviamente eso no se puede hacer, hay que realizar un análisis de hasta qué punto se puede llegar —indica el ejecutivo de RSA—. Es importante que todos sepan que al no llegar a las precauciones máximas, lo que sería costosa seguridad militar, se elige correr un riesgo. Hay que poner esa discusión sobre la mesa; no es grave y es importante que el directorio esté al tanto."

Motores del gasto

Causas que llevan a aumentar la inversión en protección en las empresas relevadas. Segmentación por cargos.



Fuente: PricewaterhouseCoopers.

En este contexto, la encuesta destaca que en la Argentina existe poca información —aunque mayor que el promedio mundial— sobre la cantidad de incidentes ocurridos. Durante los últimos 12 meses, el 34 por ciento de los consultados por PwC (en una muestra de 189 ejecutivos locales) dijo no saber cuántos incidentes sufrió. Y en seguridad la falta de información se paga.

En esto puede ser importante el rol que juegan los terceros con quienes interactúa una empresa. Sajón cree que muchas veces las compañías tienen normas férreas hacia adentro pero comparten datos con el exterior, por ejemplo un proveedor, vía intranet o web, sin mayores precauciones. El ejecutivo afirma que "pocas veces la empresa le presta atención a este tema y muchas veces la información que viaja de un lugar a otro no está encriptada".

En cuanto a los errores más comunes que se cometen en este segmento, Sajón le da importancia a la cultura de la firma: "No creo que los problemas se limiten a un tema de inversión, ya que en muchos casos los errores son de procedimiento".

En sintonía, Fabián Domínguez, gerente de Desarrollo de Negocios en Tecnologías Avanzadas de Cisco Sudamérica Sur, agrega, no sin ironía, que "el usuario, por más que esté entrenado, pulsa la tecla 'Aceptar', 'Aceptar', 'Aceptar' cuando se le abre una ventana, aunque así instale un programa malicioso. La red debería estar capacitada para determinar cuándo alguien hace eso o, por ejemplo, 'apa-

"No creo que los problemas se limiten a la inversión, ya que en muchos casos los errores son de procedimiento"

EDGARDO SAJÓN (der.), socio de PwC, junto a Diego Taich, gerente de la consultora

Foto: Gustavo Fernández

ga el antivirus, como a veces hacen los empleados para que la máquina sea más rápida".

Gil, de Deloitte, ubica el tema en un marco claro: "Antes, nadie se preocupaba por el riesgo interno porque se basaban en la confianza de sus empleados, que era gente de la empresa muy cercana al área de Sistemas. Hoy la tecnología llega a todas las áreas, es lógico que el fraude se empiece a relacionar con la IT. Hay mucha más conciencia del nivel de exposición que se tiene internamente. Después, que se protejan o no es otra cosa. Pero hay que capacitar más".

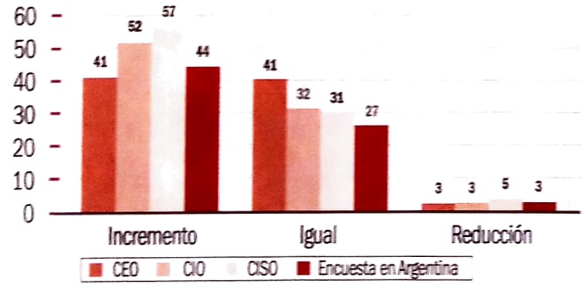
A cargo

De a poco la seguridad va tomando peso propio. Sajón considera que "es clave la creciente importancia que gana este tema en las gerencias de las compañías. Actualmente, casi el 60 por ciento de las empresas cuenta con un responsable de seguridad informática, más allá del puesto jerárquico que tenga".

Con números similares, desde Cisco afirman que un 30 por ciento de las grandes empresas no tiene responsable de seguridad. "Cuando la pregunta avanza y se habla de un departamento exclusivo dedicado al tema, la mayoría dice que no lo posee. De hecho, muchas veces el máximo responsable del área reporta al CIO y eso no tiene que pasar. El problema está en que el gerente de Sistemas no va a promover que haya un par de Seguridad (CSO) porque se va a sentir controlado", explica Domínguez, de Cisco.

Evolución de la inversión en seguridad

Crecimiento de la inversión contra el año anterior. En porcentaje. Segmentado por cargos.



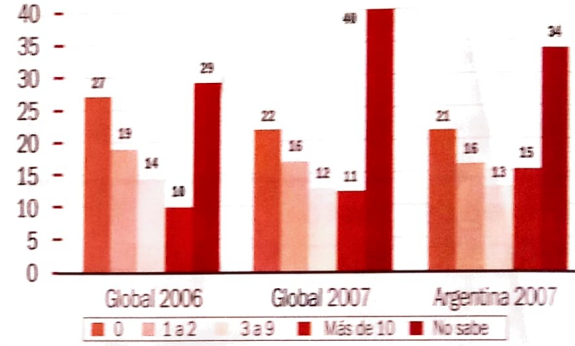
Fuente: PricewaterhouseCoopers.

Andrés Gil cree que la mayor preocupación por este tema se relaciona con la normativa y no con algún tipo de sensibilidad repentina de las empresas. "La atención a la seguridad en sí no cambia mucho, salvo que venga alguien que te presione para cambiar —observa el consultor—. En el sector financiero la percepción sobre el tema cambió con la norma A4609 del Banco Central, que marca la cancha más claramente. Y eso que no pide cosas muy extrañas: el Central la venía exigiendo hasta cierto punto y ahora avanzó. La clave, y por eso todos se preocuparon, es que ahora si hay un error no se pide la cabeza del gerente de Sistemas sino la del directorio." En cuanto a la presión normativa, Sajón sostiene que el driver regulatorio es muy fuerte en la Argentina. El ejecutivo cree que si se analiza el servicio financiero luego de la comunicación del Banco Central, la seguridad pasó a tener un rol más importante simplemente porque se formó agenda por la fuerza. En relación con los tiempos que corren, Moraes les suma una nueva preocupación a los CIOs y CSOs: las redes sociales. "Son un riesgo también para las empresas. Antes los datos eran robados, pero ahora son las mismas personas y empresas las que brindan información sensible. Si tengo el perfil profesional de alguien en Linkedin y el personal en Facebook u Orkut, uno las puntas y hago un ataque de ingeniería social. Sin embargo, esta es una época muy interesante porque vamos a tener discusiones que no existían en el pasado. Hay mucho para hacer", cierra el ejecutivo que, por supuesto, tiene perfil en Linkedin. ■

Pablo Martín Fernández

Riesgo medido

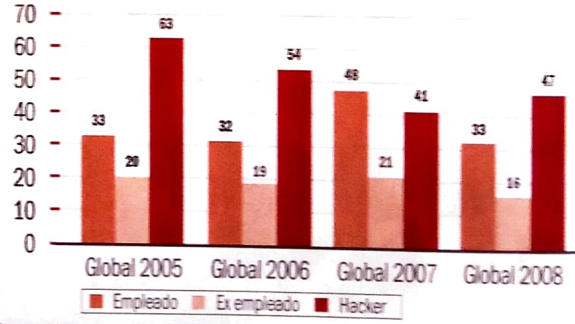
Cantidad de incidentes de seguridad ocurridos en los últimos 12 meses dentro de la compañía.



Fuente: PricewaterhouseCoopers.

Amenaza cercana

Mayores factores de riesgo potencial para la empresa.



Fuente: PricewaterhouseCoopers.