

CincoRed

La industria de la seguridad se vuelca en el fraude interno

Decenas de 'start-ups', como Kinamik o GuardTime, apuestan por tecnologías alternativas de seguridad corporativa

MANUEL ÁNGEL MÉNDEZ Barcelona

Ha sido hasta hoy el mayor fraude bancario de la historia: 4.900 millones de euros esfumados y Sociét Générale, el segundo banco francés, al borde del colapso. El supuesto culpable, el broker Jérôme Kerviel, utilizaba las credenciales de otros empleados para ganar acceso privilegiado a los sistemas de transacción. La amenaza dormía dentro.

El caso Soc-Gen promete ser sólo la punta del iceberg. Según la Asociación de Inspectores Certificados de Fraude (ACFE, en sus siglas en inglés), las grandes corporaciones en EE UU pierden cada año un 5% de sus ingresos anuales en estafas internas, unos 415.700 millones. En Europa, Ernst & Young calcula que el 22% de las compañías sufre casos de fraude corporativo. La clave: el 90% de los intrusos dentro de una empresa tienen acceso privilegiado a los sistemas de información.

Conscientes de la oportunidad, decenas de *start-ups* se han lanzado a cubrir un mercado que explotará en los próximos años. Detrás, gigantes como Symantec, McAfee o VeriSign esperan talonario en mano en busca de la mejor adquisición. Kinamik, con 15 empleados y sede en España, es una de ellas. Finalista en el RedHerring Europe del 2007, ha recibido dos millones y medio de financiación y prueba sus soluciones con los primeros clientes en el sector público y financiero.

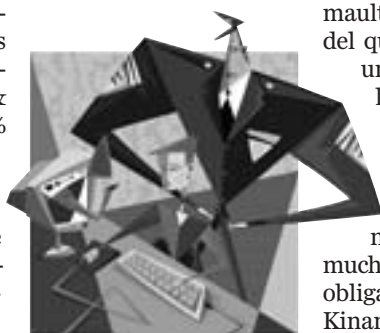
"Los directores de sistemas empiezan a darse cuenta de que el fraude interno es un serio problema. Se ha invertido mucho en el perímetro de seguridad, cada vez es más difícil romperlo. Pero si actúas desde dentro, es un bufé libre", explica Christophe Primault, consejero delegado de Kinamik. Su aplicación permite una auditoría en tiempo real de la situación, movimientos y modificaciones de datos e información electrónica confidencial. Aseguran un tiempo de proceso 300 veces menor al necesario con firmas digitales, como la generada por el DNI electrónico. La tecnología complementa soluciones tradicionales de gestión de identidad y control de acceso.

Según Primault, "la mejor forma de evitar el fraude de un empleado es dejándole claro que controlas todos sus movimientos con datos confidenciales".

El mercado de software de seguridad interna crecerá un 125% en los próximos años, frente a un estanco 3% en soluciones de seguridad externa, según datos de varias consultoras. Filtrado de información, modificación de datos, pérdida de portátiles, *spyware* interno... Las compañías se la juegan a dos bandas. Por un lado, el impacto financiero derivado de las estafas puede ser decisivo. Por otro, las pérdidas asociadas al daño en imagen y reputación, incalculables. El fraude corporativo real, añade Primault, es mucho mayor del que sale a la luz. "Es una cuestión cultural: las empresas se avergüenzan de que esto ocurra dentro de sus organizaciones y prefieren no hablar de ello. En muchos casos, la ley no les obliga a hacerlo público". Kinamik ya planifica su entrada en EE UU y los países nórdicos.

Otras *start-ups* despuntan en seguridad interna con tecnologías alternativas. GuardTime, en Estonia, sella criptográficamente los datos e información digital sin necesidad de *passwords*. La entidad inversora ASI, de los ingenieros fundadores de Skype, ha firmado con ellos la segunda ronda de financiación. En EE UU, Chronicle Solutions permite analizar y grabar las comunicaciones internas de empleados a través de *email*, mensajería instantánea, blogs o voz sobre IP. Imperva, del fundador de Check Point, y Sentrigo, controlan y protegen en tiempo real las bases de datos con información confidencial, mientras que Aveksa o SailPoint monitorizan la actividad de empleados de alto riesgo.

Cifrado de datos y equipos
En España, Secuware, con 50 empleados y oficinas en cuatro países, es una de las especialistas en cifrado de datos y equipos, desde discos duros, y redes de comunicación a sistemas de almacenamiento. Utiliza el DNI digital y otras tarjetas inteligentes para la gestión de accesos. La consultora Gartner les situó



LA CIFRA

125%

es lo que se prevé que crezca el mercado de software de seguridad interna en los dos próximos años.



Las empresas deben ampliar sus medidas de seguridad internas. BLOOMBERG

El riesgo de la empresa extendida

Es una pesadilla para las grandes corporaciones. ¿Cómo impedir que el número creciente de dispositivos móviles y la mayor colaboración se traduzca en fraudes y filtración de datos? Portátiles, PDA, USB, chats, blogs... extienden la empresa más allá de su perímetro tradicional. "Las redes de alta velocidad y la informática móvil para compartir y acceder a información añaden un nuevo nivel de ries-

go", señala Gómez. Para Primault "conceptos como SOA [arquitectura orientada a servicios], software como servicio, virtualización o computación distribuida incrementan la movilidad de los datos y el perímetro cambia, se mueve". Según un estudio del Ponemon Institute en Reino Unido, el coste de la filtración de información puede ascender a 60 euros por dato comprometido.

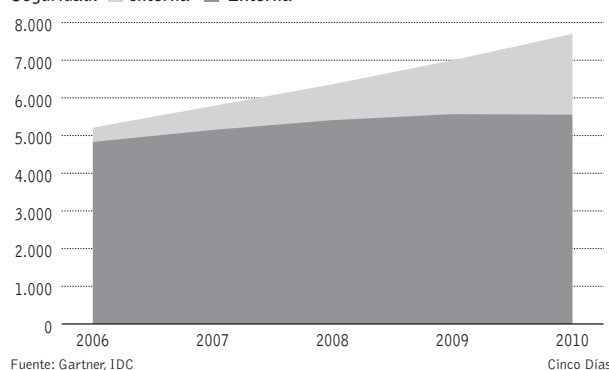
La pérdida de portátiles y móviles sigue siendo la principal fuente de problemas de seguridad. La progresiva dependencia de socios tecnológicos externos y *outsourcers* difumina aún más las fronteras. ¿Quién es el propietario de los datos? ¿Cómo se definen los niveles de seguridad? A más partes implicadas más riesgo de pérdida de información. La clave, según los expertos, pasa por

establecer diferentes niveles de propiedad y confidencialidad. Carlos Jiménez aboga por modelos de seguridad multinivel. "No todo necesita estar protegido de igual forma, es absurdo cifrar un portátil si sólo se usa para hacer notas. Pero, los servidores propios o gestionados y las bases de datos contienen información muy sensible". Hay que concentrar la seguridad allí donde se necesita.

Software de seguridad empresarial

Gasto mundial en millones de euros

Seguridad: ■ Interna ■ Externa



"Se ha invertido mucho en el perímetro de seguridad. Dentro, es un bufé libre", dice Kinamik

En España, Secuware, con 50 empleados y oficinas en cuatro países, es una de las especialistas en cifrado de datos y equipos, desde discos duros, y redes de comunicación a sistemas de almacenamiento. Utiliza el DNI digital y otras tarjetas inteligentes para la gestión de accesos. La consultora Gartner les situó finales del 2007 como visionarios en la protección de la movilidad, liderada por la alemana Utimaco Safeware. "El incremento en la utilización de sistemas de encriptación está siendo exponencial", asegura Carlos Jiménez, fundador y presidente de Secuware y asesor en materia de seguridad en la OTAN y la Unión Europea. Coincide en señalar el aspecto cultural. "Los empleados pueden percibir las medidas de seguridad interna como un menoscabo a su profesionalidad. La dificultad está en reencaminar esa cultura empresarial".

Mientras los pequeños proveedores de software buscan su hueco, los grandes fabricantes aguardan para hacerse con el más innovador. "Dejan a las compañías jóvenes crear nuevas tecnologías, esperan a que estén maduras, y las compran para completar su oferta", señala Primault. El sector de encriptación hierve en adquisiciones. McAfee compró SafeBoot el pasado noviembre, Check Point se hizo con PointSec y Symantec firmó un acuerdo con GuardianEdge hace apenas un mes.

La prevención de pérdida de datos (DLP, en sus siglas en inglés) es otro de los puntos calientes. Los casos de documentos extraviados son constantes. El último lo protagonizó el HSBC, primer banco en Reino Unido, al admitir la desaparición de un CD con los datos personales de 370.000 clientes. "Las soluciones de DLP permiten precisamente controlar dónde se almacena la información, cómo se utiliza y establecer medidas para evitar su pérdida", explica Gerardo Gómez, director de servicios y consultoría de Symantec Ibérica. La compañía pagó en noviembre 224 millones de euros por el proveedor Vontu, especialista en prevención de pérdida de datos. No habrá que esperar mucho para conocer la siguiente operación.