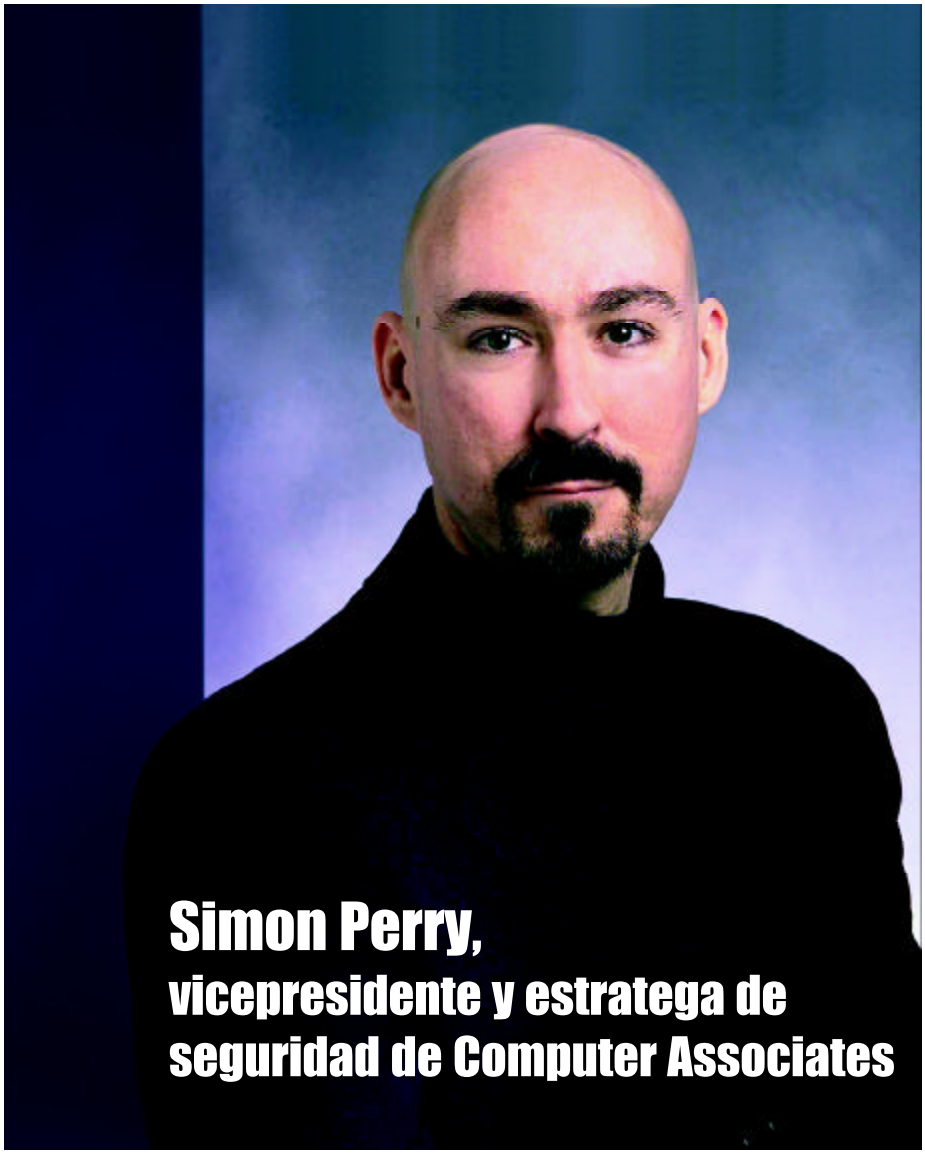
"Hay que evitar cualquier fragmentación de la arquitectura de seguridad y gestionarla bajo un único punto de control"



Simon Perry, vicepresidente y estratega de seguridad de Computer Associates

El mes pasado Computer Associates anunció la puesta de largo de su estrategia de seguridad para los tiempos de 'apertura' que corren, definitivamente marcados por un inevitable pero controlado mundo transparente de información junto con un uso extensivo de los medios electrónicos para la operativa inter-empresarial. En este contexto, el núcleo de sus eTrust se sustenta en tres pilares: las identidades, los accesos y las amenazas, todos ellos controlados de manera holística por un sofisticado paraguas gestor: el Security Command Center. De estos y otros asuntos relacionados con la protección, SIC ha mantenido una entrevista con Simon Perry, vicepresidente y estratega en la materia de la multinacional del software estadounidense.

– Además de asumir la dirección estratégica de la marca eTrust en CA, usted viene trabajando en estrecha colaboración con el FBI y las fuerzas de Defensa de EE.UU y Europa para analizar el surgimiento de amenazas y para determinar las técnicas y tecnologías necesarias para contrarrestarlas. ¿Cómo está el panorama?

– En líneas generales la sociedad ha asumido la existencia de la infoseguridad y la prevención de delitos cometidos por medios electrónicos, si bien es cierto que no toda en igual medida; la sensibilización en las organizaciones no es la misma que la percibida por los usuarios personales, además a éstos lo que les afecta prioritariamente son las cuestiones de protección personal y privacidad.

La realidad es que las sociedades avanzadas, empujadas por las TI, nos están abocando a lo que denomino "un mundo transparente de información", cuyo trasiego será cada vez más personalizable; al mismo tiempo, y paradójicamente, se está demandando acotar y controlar los accesos a esa información pero a gran escala.

– Las relaciones negociales globales con usuarios externos, sean socios o clientes autorizados, obligan a dotar de suficiente flexibilidad a la hora de implementar las políticas de acceso, respetando una permisividad controlada… ¿Se avecinan conflictos por un choque de intereses?

– No hay que olvidar que hoy y ahora las empresas quieren dirigirse a los individuos, no al consumidor, respondiendo en gran medida al propio deseo de ese consumidor de ser atendido personalmente. Por tanto preveo una tendencia clara a valorar crecientemente la autenticación, ya que cada vez más la identificación será determinante e inevitable, pese a que cause conflictos con esa intimidad que antes mencionaba.

Igualmente, en el escenario empresarial, la implantación dinámica de las reglas de protección será imprescindible para poder hacer un seguimiento adecuado de todo lo que sucede. Bajo una óptica tecnológica, a los ISP's les va a sobrevenir mucho trabajo, especialmente el relacionado con las capacidades de almacenamiento y detección, y mayores exigencias de confidencialidad; por su parte, a las organizaciones aún les aguarda un despliegue a gran escala de sistemas cortafuegos, antivirus e IDS personales.

– Queda entonces mucho por hacer …

– Sí, aunque el avance también resulta significativo, especialmente en áreas estándar de la seguridad; en otras, como la de los entornos *wireless*, aún no lo es tanto. Buena prueba de ello fueron los recientes descubrimientos de los servicios secretos estadounidenses de determinadas vulnerabilidades en entornos inalámbricos, los cuales dejaban su nivel de seguridad en entredicho.

Es una obviedad que la seguridad impenetrable no existe y también que no es ni blanca ni negra. Esos grises marcan la senda a encarar, teniendo muy en cuenta que hay tanta sobreabundancia de información técnica a la hora de gestionar las herramientas de seguridad, que esa tarea constituye todo un reto y lo que es peor, las implementaciones y el mantenimiento de las configuraciones en no pocos casos son muy malas.

Como sugerencia, me gustaría recomendar a sus lectores, sean proveedores de tecnología o gestores de seguridad TI en empresas, que traten de pensar con más frecuencia en cómo gestionaría un usuario la protección, ya que su punto de vista muchas veces muestra posibles defectos e indicios de cómo mejorar la calidad en los procesos. Ayudaría mucho.

– Computer Associates es la primera compañía de software TI en anunciar un sistema de seguridad completo e integrado capaz de abarcar las disciplinas de gestión de identidades, accesos y amenazas. ¿Se puede realmente?

– Pensamos que sí, y de hecho ya es una realidad. Hemos sido capaces de poner nuestra tecnología a disposición de los responsables de seguridad para que puedan tener una visión global, integral, incluso de parámetros físicos de la seguridad corporativa, incluyendo todos esos aspectos esenciales que usted menciona, que son los de la identidad, el control de acceso y los posibles puntos vulnerables.

Además, nuestra pretensión también es la de ayudar a racionalizar los procesos administrativos e implementar con mayor eficacia las mejores prácticas de seguridad.

– eTrust Security Command Center parece la solución definitiva…

– Hoy ya no parece razonable gestionar la seguridad a trozos. Por ello, en Computer Associates hemos realizado un considerable esfuerzo, bajo un exclusivo enfoque holístico, para integrar todas nuestras soluciones de seguridad informática eTrust con la tecnología de nuestros 'partners' y con nuestra nueva solución Security Command Center, que aporta una única consola con una visualización de tipo portal donde se centralizan las operaciones de seguridad de la empresa.

Esta solución podría definirse como un *Business Intelligence* de seguridad que rehuye lo fragmentario, reduciendo la duplicación de esfuerzos y las sobrecargas innecesarias.

– ¿Cómo actúa eTrust Security Command Center?

– Básicamente, recoge datos de todos los aspectos vinculados con la seguridad y trabaja de manera global con ellos. Esta información es correlacionada, procesada y evaluada posteriormente, contrastándola con los recursos de negocio almacenados en un catálogo centralizado. Mediante herramientas de visualización intuitiva, la información se nos aparece como la de un portal, en el cual es posible ver, controlar y gestionar las distintas disciplinas relativas a la seguridad, que nosotros segmentamos en identidades, accesos y amenazas. Como partes esenciales de la solución se incluyen los servicios de tratamiento de auditoría centralizada, denominada eTrust Audit, y otros de visualización, llamados eTrust 20/20, que ya anunciamos en abril pasado, los cuales incluso permiten correlacionar eventos de seguridad TI con otros de seguridad física.

"Sí es posible agrupar las disciplinas de gestión de la identidad, los accesos y las amenazas para una gestión eficiente de los sistemas de seguridad"

– CA dispone en la actualidad del mayor portafolio de soluciones de seguridad para la empresa, y es bastante lógico pensar que tiene resuelto el espinoso tema de la interoperabilidad para la gestión centralizada de sus propios productos, pero lo cierto es que los recursos de protección TI en las empresas son de muy variada procedencia …

– Aunque efectivamente no todos nuestros clientes cuentan sólo con nuestra tecnología, digámoslo 'propietaria', con su aparente facilidad de entendimiento, sí es verdad que estamos haciendo un gran esfuerzo de integración con las tecnologías de terceros más ampliamente extendidas, como por ejemplo con la gama de productos de Check Point.

Por otro lado, nuestra herramienta más reciente ofrece interfaces abiertas a través de un *kit* de desarrollo de software que ayuda a establecer una integración sin fisuras con multitud de herramientas de otros fabricantes, como son cortafuegos, detectores de intrusiones o dispositivos hardware. Y además, para ayudar a los clientes a implantar estas soluciones, estamos trabajando estrechamente a nivel mundial con *partners* de soluciones como Ernst & Young, EDS, Fujitsu Siemens Computers y SAP, entre otros.

– La hoy denominada 'gestión de identidades' es un asunto que viene preocupando a las grandes corporaciones con TI complejas desde hace ya mucho tiempo y por lo que parece está llamada a ocupar un creciente papel estelar en el mercado. ¿Para CA, en qué consiste?

– Efectivamente no es un tema nuevo pero sí que preocupa cada vez más y es más factible conseguirla. Es un término que afecta a las identidades de los usuarios y a su integración con las distintas aplicaciones empresariales. Consiste en un control preciso de las cuentas de acceso de éstos, desde que se crean hasta que se dan de baja, facilitando la automatización de todos los cambios que se hagan a lo largo de su ciclo de vida en la empresa. Naturalmente, esto implica que los usuarios sólo van a poder acceder a las aplicaciones de negocio para las que están autorizados, pudiendo hacerlo cómodamente, utilizando una única contraseña o entrada única para todos los sistemas que precisan para sus funciones, desde cualquier lugar y mediante cualquier dispositivo.

– El segundo pilar de su estrategia, la gestión de accesos, también es una prioridad clásica de protección de las organizaciones …

– Es cierto. Nuestra intención es ofrecer una protección proactiva de los recursos de una compañía acorde con la política de seguridad corporativa que haya establecido, permitiento conocer quién accede a qué y cómo se utilizan los recursos a los que se le ha autorizado, todo ello aplicable a los distintos sistemas operativos y aplicaciones de negocio, y proporcionando la mayor disponibilidad para los sistemas críticos.

– Dentro de la visión de CA de la gestión de la infoseguridad integral, ustedes encuadran a las amenazas como la tercera área. ¿Por qué?

– Hoy no es posible ignorar las amenazas y las vulnerabilidades, cualesquiera que sean. Nos hemos centrado en disponer y agrupar herramientas muy interrelacionadas para detectar, analizar, aislar, avisar, prevenir y responder de forma automática, sean esas amenazas de procedencia interna o externa. Afortunadamente, en CA disponemos de un gama muy completa y avanzada de productos para afrontar anomalías y ataques, que también impiden la interrupción de la actividad empresarial y facilitan una valoración en tiempo real de las vulnerabilidades existentes, con lo cual resulta fácil conocer qué aspectos conviene mejorar para reducir riesgos. n

Texto: **Luis G. Fernández**
Fotografía: **Computer Associates**