

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar agujeros en el diseño, configuración y operación de los sistemas de seguridad de las empresas. En la actualidad se considera que las compañías europeas dejan de mejorar en

productividad por esta cuestión casi 50.000 millones. Y a ofrecer seguridad informática se dedica Manuel Antonio Roa, director general de Seprola, una de las nuevas compañías llegadas recientemente al campo de la gestión documental y recuperación de la información.

Al día se roban y/o pierden en el mundo más de 2.000 ordenadores portátiles.

—¿Cómo se posiciona España frente a otros países a este respecto?

—A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas informáticos. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc). Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para

Manuel Antonio Roa, director general de Seprola

“La externalización de la custodia de la información impide posibles intrusos”

■ M. Tortajada

—Las empresas europeas podrían estar perdiendo un aumento potencial de los beneficios de 46 mil millones de euros como consecuencia de los métodos ineficientes existentes utilizados para procesar la información. ¿Cómo debe custodiar una compañía su información?

—Idealmente la información crítica de las compañías debe estar siempre protegida en centros de custodia especializados. El control de accesos mediante varios niveles de seguridad es un punto muy importante. Al ser crítica, la información debe estar disponible en todo momento y de forma inmediata. Terminado su ciclo de vida, debe destruirse de forma confidencial para evitar usos no previstos y que puedan implicar riesgos para el negocio y/o incumplimiento de las leyes.

El simple hecho de externalizar la custodia de información aumenta su seguridad ya que, una vez fuera de su ubicación natural en la empresa, queda lejos del posible error humano y fuera del alcance de posibles "intrusos".

—¿En qué consiste la seguridad informática?

—Generalmente, la Seguridad Informática consiste en asegurar que los recursos del sistema de información, es decir, software, hardware y datos de una organización sean utilizados de la manera como se planeó. Hoy en día, los sistemas informáticos son herramientas muy útiles. Básicamente, en ellos, se registra y procesa la información de las empresas, pero son susceptibles de amenazas; por tal razón, la Auditoría Informática se encarga de evaluar si se están cumpliendo con las medidas de control para minimizar los riesgos que conlleva la utilización de sistemas informáticos. Según las fuentes de amenazas, estos riesgos clasifican en Seguridad Lógica y Seguridad Física. El activo más importante de una organización es la información; por ello, es necesario contar con planes y políticas para protegerla.

—¿Se usan muchos métodos incorrectos para evitar la fuga de información?

—Por desgracia, el robo de información está creciendo de manera exponencial en los últimos años. Las empresas afectadas, lejos de ponerse en manos de profesionales, muchas veces usan métodos incorrectos en el momento de impedir que esto suceda. La manera más fácil de robar es mediante un usuario de la empresa que consiga acceso a la información deseada, como registro de clientes, números de cuentas, etc. En este sentido, no debemos olvidar nunca que el robo de información puede ser vista por muchas personas



AL TIMÓN

Manuel Antonio Roa, director general de Seprola, es licenciado en Derecho y con un MBA Internacional, cuenta con una experiencia de más de 20 años en puestos de liderazgo para compañías internacionales. En

todo este tiempo ha desarrollado un profundo conocimiento del sector que le ha llevado a poner en marcha esta nueva aventura. En su trayectoria profesional ha desempeñado cargos que han desde el sector de

Ventas y Marketing hasta la Dirección General, consiguiendo grandes mejoras en el crecimiento corporativo y en la mejora del clima organizativo. La música clásica y el baloncesto son sus grandes pasiones.

“Por desgracia, el robo de información está creciendo de manera exponencial en los últimos años y las empresas afectadas suelen usar métodos incorrectos”

operacionales. En definitiva hablamos de organizaciones más centradas en su negocio y por ello más eficientes, más seguras y solventes. Esto cobra especial relevancia en el sector financiero donde muchos de los documentos utilizados tienen un valor económico intrínseco.

Dos cifras para ilustrar lo lejos que estamos de una correcta gestión de la información: El coste de recuperar información para una organización llega a ser de casi 100 euros por documento no encontrado y hay empresas que gestionan decenas de millones de documentos al año.

“La información crítica de las compañías debe estar siempre protegida en centros de custodia y debe destruirse cuando ya no nos sirva”

realizarlos. El aprendizaje de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hacker" bulletin boards y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

A pesar del avance, muchas organizaciones siguen sin contar con una correcta política de gestión de la información. Y lo peor de todo es que hay muchas que ni siquiera son conscientes de ello. Hace falta profundizar en la comunicación para educar a la sociedad y a las organizaciones en materia de seguridad de la información y protección de datos personales.

—¿Cómo se analiza la seguridad informática en una empresa?

—La Seguridad puede estudiarse dependiendo de las fuentes de las amenazas a los sistemas: la Seguridad Física y la Seguridad Lógica. La Seguridad Física trata de la protección de los sistemas ante amenazas físicas. Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas, ante amenazas a los recursos e información confidenciales. Forman parte de este tipo de seguridad: Desastres naturales, Sabotajes internos o externos, etc. Por otro lado, la Seguridad Lógica protege la información dentro de su propio medio mediante el uso de herramientas de seguridad. Por lo tanto, la Seguridad Informática se puede definir como conjunto de operaciones y técnicas orientadas a la protección de la información contra la destrucción, la modificación, la divulgación indebida o el retraso en su obtención.

—¿Qué soluciones ofrecen en gestión documental?

—Ayudamos a las compañías a procesar sus documentos y a mantenerlos actualizados. Somos eficientes, por lo que les proporcionamos un ahorro de costes, y trabajamos de forma profesional con una metodología que garantiza la localización eficiente y precisa de los documentos archivados.

Hay estudios que indican que las compañías invierten hasta 90 euros en recuperar cada documento no encontrado. Nuestra función es ahorrarles los costes y riesgos que implican una mala gestión de la información, entre ellos los derivados del incumplimiento de la normativa vigente en materia de protección de datos, que puede implicar multas de hasta 600.000 euros.

en caso de ser publicada en una web no protegida adecuadamente. Por lo tanto, es imprescindible tener un proceso estructurado de seguridad de la información para obtener un control básico. Continuidad en los controles y profesional capacitado para la gestión de la seguridad son factores fundamentales para tener éxito.

—¿Qué beneficios aporta a las empresas una correcta gestión de la información?

—Los principales beneficios son una reducción de costes y de riesgos