



## Entrevista a Thomas Raschke

*Independent Security Analyst*

REALIZADA POR  
**Antonio Ferrer**

FOTOS  
**Carlos Useros**

**T**homas Raschke es analista independiente y uno de los principales expertos en seguridad informática y gestión de riesgos. Durante más de 10 años ha cubierto el mercado de la seguridad desde prácticamente todos los ángulos, incluyendo antivirus, firewalls, IDS/IPS, gestión de identidades, encriptación, gestión de la seguridad y seguridad de la información, especialmente prevención de fugas de datos (DLP).

También ha puesto en marcha, con gran éxito, los servicios de investigación en Europa de IDC y Forrester.

Thomas es asimismo un experimentado consultor en asesoramiento estratégico a los proveedores de seguridad y a los usuarios finales. Conviene señalar también que es frecuentemente el principal orador en los eventos más importantes de la industria de la seguridad y es citado regularmente por la prensa especializada.

Nacido en Copenhague, Dinamarca, Thomas Raschke posee un Master por la Universidad de Paderborn, habla inglés y danés además de su alemán nativo y ya empieza a conocer algunos vocablos en español... gracias a nuestra revista, por supuesto.



### ¿Por qué es tan importante la prevención de las fugas de datos?

En la "era de la información" los datos y la información son el alma de la mayoría de las organizaciones. Hoy en día, los datos están disponibles en diversos formatos electrónicos y son almacenados, copiados, y transmitidos - a menudo sin el consentimiento del titular de los datos- con gran profusión. El resultado es que la mayoría de las empresas simplemente no conocen los activos de sus datos y la importancia que tienen para su negocio, tampoco donde está ni como se mueve su información sensible.

Por lo tanto, si las organizaciones no saben lo que tienen ni la importancia de las cosas para ellos,

será prácticamente imposible proteger su información sensible adecuadamente.

### ¿Son las empresas y las organizaciones públicas conscientes del valor de la información?

Lamentablemente, la mayoría de las organizaciones no son conscientes de la importancia de sus datos. Empresas y organizaciones públicas a menudo carecen de sistemas elementales de búsqueda y análisis de información. Si bien algunas organizaciones utilizan categorías sencillas como "reservado" frente a "público", la mayoría necesita mucho más que eso, pero a menudo se asustan por la complejidad que implica el análisis basado en el riesgo.



La complejidad se deriva del hecho de que los datos y la información deben ser claramente clasificados y gestionados por los propietarios y directivos de la empresa. Por ejemplo, el Director de la Investigación y Desarrollo es probablemente la persona mejor posicionada para señalar qué información sobre I + D es extremadamente valiosa para la empresa, y qué documentos requieren niveles más bajos de protección. Sin embargo, en la práctica, los responsables de seguridad son quienes dan respuestas técnicas a problemas que en realidad son del negocio y de la clasificación de los datos y su seguridad.

**¿Cuáles son las cuestiones más importantes a las que enfrenta el SIO de una organización? ¿Por qué?**

Lo que más preocupa a los responsables de seguridad de las organizaciones, según la mayoría de los estudios y encuestas independientes, es la seguridad de los datos y la adecuada protección de la información sensible como son los registros de clientes, los números de tarjetas de crédito y la información financiera, así como diversos tipos de información con propiedad intelectual, por ejemplo, códigos fuente, planes de negocio, recetas, etc. Todo esto va claramente por delante de otros problemas como son la continuidad del negocio, la seguridad de aplicaciones, y la gestión de identidades.

Los responsables de seguridad han entendido también el hecho de que es necesario no sólo proteger el perímetro empresarial contra amenazas externas, como hackers y virus, sino que es necesario salvaguardar lo que tiene mayor valor, tanto para la organización como para los posibles atacantes.

Por otra parte, el hecho de que



hasta un 70% de los incidentes suceden hoy en día dentro de los límites del firewall implica que hay que dedicar atención y recursos adicionales para la protección contra las amenazas internas.

**¿Cuáles son las medidas esenciales para evitar la fuga de información?**

La prevención eficaz de fugas de datos (DLP) empieza por la identificación y clasificación de los datos sensibles (descubrimiento y clasificación).

A continuación las herramientas DLP sugieren o ayudan a establecer políticas basadas en los contenidos y en el contexto de la información (política de gestión).

Seguidamente, se permite la circulación de los activos de datos en un contexto legítimo de negocios interceptando y analizando el tráfico de datos, por ejemplo, mensajes de correo electrónico o actividades como copiar un archivo en una memoria USB. (vigilancia y cumplimiento).

Por último, las soluciones DLP informan, auditan y documentan los incidentes para actualizar y mejorar sus capacidades de análisis.

La prevención de fuga de datos se realiza típicamente sobre los datos en movimiento (Data In Motion, DIM) en los puntos de salida de la red, sobre los datos utilizados (Data-In-Use, DIU) en los puntos de usuario y sobre los datos en reposo (Data-At-Rest, DAR) en la investigación y clasificación de los datos almacenados.

**¿Cómo hacer frente al problema de la pérdida de información en una época de escasos recursos económicos? ¿Existen herramientas para evaluar las pérdidas económicas de la información?**

Las fugas de información adquieren mayor importancia durante los tiempos económicos difíciles debido a que el gran número de empleados descontentos o despedidos incrementa el riesgo de que se lleven consigo información de gran valor.

Efectivamente, existen una serie de instrumentos para medir el retorno de la inversión en las implementaciones DLP. Sin embargo, el costo unitario de una pérdida de datos se puede estimar en aproximadamente 200 dólares por registro. Todo lo cual no hace sino subrayar la importancia de las DLP.



**¿Cómo ve la situación en los próximos meses? La actual preocupación por la seguridad de la información, ¿es una moda o se adoptarán medidas eficaces? ¿Cómo podemos saberlo?**

Creo que la preocupación actual por la seguridad y la gestión de los riesgos en general y de los datos en particular seguirá reflejándose como elevada dentro de las previsiones de gastos en la mayoría de las organizaciones. Sin embargo, los primeros podrían sufrir un estancamiento o disminución leve mientras que las DLP seguirán creciendo aun en tiempos de recesión. Los resultados de las encuestas actuales y los datos históricos sobre gasto de las organizaciones avalan esta afirmación.

**En su opinión, ¿qué tiene más importancia, la pérdida no deseada de datos, como olvidar un pen-drive con información sensible en un bar, o los ataques de la ciberdelincuencia?**

En mi opinión, la mayoría de los problemas que se producen son el resultado de la pérdida accidental o del extravío. Los dispositivos de almacenamiento extraíbles, en particular, son muy peligrosos, cuanto más pequeños peor, y suelen ser objeto de robos o pérdidas.

Sin embargo, la utilización malintencionada de información privilegiada por parte de un usuario interno puede crear un daño mucho mayor, especialmente si tiene acceso a grandes cantidades de datos sensibles.

Un cibercriminal que accede desde fuera de la organización está interesado principalmente por datos que puedan reportarle beneficios económicos, por ejemplo, direcciones de correo electrónico que se puedan vender a los *spammers*. En última



instancia, las empresas deben evaluar sus riesgos y disponer de los mecanismos de seguridad adecuados para todos los vectores de amenaza.

**¿Dónde podemos encontrar al peor enemigo, dentro de una organización o fuera? ¿Por qué?**

En informes como el Verizon Business Data Breach Report 2009 se puede encontrar información forense muy valiosa sobre la fuga de datos corporativos. Este estudio sugiere que es conveniente vigilar a las terceras partes externas que tienen acceso temporal a información sensible, tales como consultores y proveedores de servicios. Asimismo, también sufren a menudo pérdidas de datos las organizaciones que implican altas tasas de desgaste y las que disponen de grandes equipos de ventas en movilidad.

**¿Hay algún país que sobresalga, en sentido positivo, porque tanto**

**las empresas como los organismos gubernamentales hayan establecido buenas prácticas para evitar las fugas de datos?**

Con la excepción de América del Norte y el Reino Unido, no creo que haya países o regiones especialmente avanzados en lo que respecta a la DLP. Los EEUU y varias industrias verticales (por ejemplo, los servicios financieros y las tarjetas de crédito) han establecido un estricto marco normativo que se ha traducido en un mayor rigor en la seguridad de los datos.

**¿Le gustaría añadir algún comentario?**

Me gustaría señalar que el problema de las amenazas internas no está resuelto ni mucho menos, - nos vamos en encontrar con más datos, mayor movilidad, nuevas normativas, es decir, mayores volúmenes de información - por lo que esto es sólo el principio. ♦