



Entrevista a Byron Acohido

Especialista Cibercrimen
USA TODAY

REALIZADA POR
José Luis Anduix

Con motivo del **First Security Blogger Summit**, patrocinado por Panda Security, vino a Madrid **Byron Acohido**, redactor de **USA Today** especializado en investigación sobre el cibercrimen que ha tenido a bien responder a unas cuestiones de actualidad. **Byron Acohido** es periodista del **USA Today** y autor del libro **"Zero Day Threat"**. Escribe regularmente en su blog **Zero Day Threat** además de cubrir los temas de seguridad para su periódico. **Acohido** es experto en desmitificar asuntos complejos. Empezó a trabajar como periodista tres días después de graduarse en la Escuela de Periodismo de la Universidad de Oregon en 1977. Su detallada investigación publicada en **The Seattle Times** sobre los problemas de control del Boeing 737 contribuyó a que la FAA (*Federal Aviation Administration*) exigiera mayores requisitos de seguridad y le valieron 11 destacados premios periodísticos entre los que se cuenta el **Premio Pulitzer**.

¿Qué importancia tiene para usted el cibercrimen en nuestros días?

Es muy importante. He estado cubriendo el tema durante 13 años y puedo afirmar que es un fenómeno que ha crecido de forma exponencial. Hasta



alrededor del año 2000 los *hackers* buscaban impresionar a los demás pero ahora son verdaderas mafias, grupos organizados que tienen como objetivo conseguir dinero. De hecho, según las estimaciones más conservadoras, podemos hablar de unas estafas que rondan los doscientos millones de dólares al año, lo que supone un negocio mayor que el de las drogas.

¿Cuál es su opinión sobre la importancia de los ataques cibernéticos contra grandes instituciones de un país realizados por grupos terroristas o incluso por otras naciones? ¿Podemos estar ante un nuevo tipo de guerra?

Los *hackers* saben muy bien la importancia económica que supone la información para una empresa. Por eso, se está atacando directamente a las grandes corporaciones y lo que estamos observando es que ni las empresas ni los gobiernos están preparados para evitar el cibercrimen. Pienso que es muy importante que las compañías y los gobiernos empiecen a colaborar conjuntamente y compartan información sobre cómo han sido atacados y mejorar así los niveles de defensa en la industria.

Por otro lado, y respondiendo a la segunda pregunta, estamos observando un nuevo tipo de terrorismo y guerra política. Los hechos ocurridos recientemente en Estonia o Georgia, por ejemplo muestran que este tipo de ataques está creciendo mucho. Lo interesante de este asunto es ver cómo unos y otros usan los mismos ataques y las mismas herramientas, en particular *botnets*, con lo que sería muy fácil acabar con ellos si se quisiera.

¿Por qué la seguridad de la información es un factor estratégico en una empresa?

Para las empresas la información es su activo más valioso. Si la pierden o la dejan accesible a los ciberdelincuentes corren el riesgo no sólo de perderla, y perder por lo tanto su negocio, sino también de lastrar la confianza de sus socios, accionistas y clientes. Un claro ejemplo de esto es el ataque sufrido hace poco por **Monster.com**, el buscador de empleo más importante del mundo. Un grupo de *hackers* consiguió acceder a la base de datos con toda la información de empresas y demandantes de empleo, lo que ha supuesto una pérdida muy importante de su credibilidad ante el mercado.

¿Existe realmente en las empresas y organizaciones ese concepto del valor de la información? ¿Qué podríamos hacer para ayudar a incrementar los niveles de seguridad?

Depende mucho del tipo de empresa y del sector en el que se mueva. Así por ejemplo, los más concienciados son, sin duda, operadoras y entidades financieras. Es fundamental la concienciación para todo tipo de organizaciones, sobre todo las empresas más pequeñas, que no siempre se dan cuenta de la importancia de contar con soluciones de seguridad y políticas de acceso a la información coherentes y prácticas.



Informar de lo que pasa quiere decir que hay que decir que hay empresas y organismos que no se toman en serio sus responsabilidades en materia de seguridad. Y eso puede crear sensación de inseguridad. ¿No es verdad?

Muchas organizaciones sólo se dan cuenta de la importancia de mantener políticas de seguridad internas cuando conocen los millones en pérdidas de empresas con agujeros en sus sistemas, por lo que no creo que sea una mala estrategia la de informar de la irresponsabilidad de muchos consumidores y empresas. Sobre todo si pensamos en lo que nos puede ayudar para que en el futuro todas las empresas se encuentren securizadas.

¿Cuáles son los aspectos más importantes a tener en cuenta de cara al futuro en materia de seguridad?

Hay que tener en cuenta dos aspectos. Por un lado, el consumidor o ciudadano tiene que tener mucho cuidado al usar Internet y ser responsable de lo que realiza cuando se conecta; por otro, en las empresas, los ejecutivos tienen que tener mucho cuidado con los datos que manejan y las amenazas a las que están expuestos. Las empresas deberían

tratar la información que utilizan como si fuera ORO.

¿Cuáles son hoy en día los principales retos relacionados con la seguridad de la información, la privacidad de la información y la confianza?

Sin duda, el objetivo primordial de la industria debe ser reducir el número de cibercriminales. Pero para ello es precisa la colaboración de los Estados ya que muchos ataques proceden de lugares en los que no existe un control de este tipo de actividades ilegales, como Ucrania, Rusia o Turquía. Los ISPs de estos países conocen perfectamente lo que hacen sus usuarios pero miran a otro lado porque también hacen negocio con los ataques. En el otro lado, países como Alemania y Suecia son punteros en el control del cibercrimen.

Algunas cifras que manejan varios fabricantes de soluciones de seguridad indican que cerca del 50% de los ordenadores personales están infectados por algún tipo de *malware* y esto está sucediendo a pesar de contar con buenas herramientas de protección. ¿Cómo cree que esto podría afectar a la privacidad de la información de los usuarios? ¿Qué pueden hacer los usuarios?

Los últimos datos que he leído indican que el 80% de los correos electrónicos que circulan son *spam* y el 90% de ese *spam* es fraudulento. En este sentido, he de destacar que me han sorprendido las políticas de protección de datos que existen en Europa, mucho más avanzadas que en Estados Unidos, donde la mayoría de las veces se presupone que el usuario acepta la recepción de mensajes sin su consentimiento.

En su opinión, ¿cómo se podría mejorar la privacidad de la información, tanto en las empresas privadas como en los organismos gubernamentales?

Como decía en la respuesta anterior, pienso que Europa está más preparada que EEUU sobre la protección de datos. En Europa los usuarios tienen que, proactivamente, autorizar a usar los datos privados. En USA, no.

¿Es la confianza una cuestión estratégica para empresas y gobiernos? ¿Por qué?

Sin duda, como decía al principio de la entrevista, los clientes y socios de una empresa, y los ciudadanos cuando realizan transacciones con el Estado, basan las relaciones en la confianza y esa confianza se obtiene cuando los usuarios están seguros de que la información que intercambian con las empresas o la Administración no va a llegar a terceros.

Si una organización le pidiera las grandes líneas de una Política Integral de Privacidad, ¿cuál sería su respuesta?

Es esencial tener, en primer lugar, una política de seguridad correcta y global que involucre a todos los responsables de la organización. Una vez estipulado esto, la organización debe contar con herramientas profesionales que permitan controlar los activos más valiosos de la organización. ♦

