



Entrevista a Bruce Schneier

**Fundador y CTO
BT Counterpane**

REALIZADA POR
Antonio Ferrer

Bruce Schneier es un tecnólogo, especializado en seguridad, reconocido mundialmente. La revista "The Economist" lo considera un "gurú de la seguridad", pero en realidad es más conocido como comentarista y crítico de temas de seguridad que está dotado de una gran lucidez. Cuando la gente quiere saber cómo funciona realmente la seguridad recurre a Schneier.

Es también un autor de libros especializados en seguridad que se han convertido en superventas. El primero que escribió es "Applied Cryptography", en donde explica como funciona realmente la misteriosa ciencia de los códigos secretos. La revista "Wired" comentó que es el libro que la Agencia Nacional de Seguridad de EE. UU. hubiera deseado que no se publicara nunca.

Su segundo libro, titulado "Secrets and lies" sobre seguridad de redes y ordenadores, es considerado por la crítica como "una caja de sorpresas útiles". Su último libro es "Beyond Fear". Se trata de una serie de pensamientos sensatos sobre seguridad en un mundo sin certezas. Aquí se analizan los grandes y pequeños problemas de la seguridad, ya sea personal, corporativa o nacional.

Desde hace 7 años Schneier publica la newsletter Crypto-Gram, un



referente para los profesionales de la seguridad y donde pueden encontrarse tanto críticas mordaces como debates de alto nivel sobre seguridad.

En su actividad profesional, Schneier es fundador y Director Técnico (CTO) de BT Counterpane, la empresa líder en protección de la información que circula por las redes.

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

Sin duda es el mayor problema que tenemos. Cada día hay más cibercriminales, que actúan más sofisticadamente y con mayor rapidez que los fabricantes de los sistemas de protección. Y no podemos hacer otra cosa que sobrevivir y aplicar más reglamentaciones. El crimen es muy

grande en Internet y no deja de crecer.

¿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?

No, en absoluto. En las guerras la gente se mata. En estos ataques, que sin duda son muy molestos, no muere nadie. Cuando hace unos meses se habló de una ciberguerra entre Rusia y Estonia, se estaba minimizando lo que una guerra es realmente. Hay o ha habido mucho *hacking* político, por ejemplo ente India y Pakistán, entre Rusia y Estonia, o entre demócratas y



republicanos en los EE. UU. pero no es una guerra. Hay mucha diferencia entre guerra y *hacking*. Tanto la inseguridad informática como la guerra tienen muchas consecuencias económicas, pero no son lo mismo. La guerra implica muerte y destrucción y la ciberguerra también. Cuando haya una ciberguerra de verdad lo notaremos.

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

La seguridad de la información es importante porque la información es importante. Fundamentalmente la información es importante porque

pensamos que es importante, si no fuera así no tendríamos este trabajo. Es muy sencillo. Lo que pensamos que es importante acaba siendo importante.

¿Existe realmente en las empresas y organizaciones ese concepto del valor de la información?

No se puede generalizar. Existen empresas que se toman el tema de la seguridad muy en serio y gestionan sus riesgos muy bien. Otras, por el contrario, no son conscientes del problema. La razón de esto es porque la seguridad es tanto un sentimiento como una realidad. Podemos sentirnos seguros sin estarlo y viceversa. Ante

situaciones nuevas, las personas y también las empresas reaccionan de maneras distintas.

Los medios de comunicación especializados estamos preocupados, muy preocupados, por la seguridad de la información. Seguramente porque manejamos mucha información sobre muchos problemas de seguridad. ¿Qué podríamos hacer para ayudar a incrementar los niveles de seguridad?

El papel de los medios de comunicación es un tema muy delicado y no existe una sola respuesta. No me gusta cuando están



todo el tiempo señalando problemas pero tampoco me gusta cuando los ignoran. Para mi es difícil criticar a los medios de comunicación. Por otra parte pienso que tratan de hacer lo mejor. Yo simplemente diría que deben informar al público de lo que pasa. Sencillamente eso.

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?

Sin embargo, pienso que hay que informar, dando a conocer, divulgando, los casos que se quieren tapar, haciendo públicas las consecuencias económicas de la falta de seriedad en la gestión de la seguridad de la información. Los departamentos de comunicación de las empresas tratan

de evitar salir en la primera página de los periódicos por estos temas. Es cierto que, por ejemplo, hay bancos que tratan a toda costa de evitar que se conozcan sus incidentes de seguridad porque eso daña su reputación.

¿Cómo puede un usuario particular de un ordenador personal aumentar su seguridad?

Muchas veces me pregunto como ha podido la industria informática crear un dispositivo tan inseguro como es un ordenador personal. Pero esa es la realidad que tenemos. Y es poco realista exigir a los usuarios que sean expertos en seguridad. Por tanto la única buena solución es que sean los proveedores de conexión a Internet los que actúen como departamentos técnicos de los usuarios y que cuiden de su seguridad. No veo porque no pueden disponer de conexiones limpias para

los usuarios domésticos. Esa es la única vía. En todo caso, y mientras esto llega, no me cansaré de insistir en la perentoria necesidad de hacer copias de seguridad de nuestra información.

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

La lista es larga, destacaría los siguientes: el valor económico de la información para las empresas; la importancia de los sistemas por encima de la propia información, la falta de protección del usuario, el aumento de la complejidad de los sistemas con el mayor riesgo que ello supone, la incapacidad de las empresas y autoridades para proteger los servidores, la necesidad de una mayor regulación y una aplicación de nuevos modelos económicos en el sector de las TIC. ♦