



VISITA RECOMENDADA

Taosecurity.blogspot.com



propone dar prioridad a las pruebas de seguridad en sistemas en producción, preferiblemente en tiempo real, en detrimento de la mera comprobación de la conformidad (*compliance*) de nuestros sistemas con las políticas de

El invierno es una época del año que invita a reflexionar. Propongo, para ello, un sitio que plantea visiones alternativas sobre aspectos de seguridad de la información: es el *blog* de **Richard Bejtlich** en *blogspot.com*, **Taosecurity**. Los temas que aborda merecen algo de tiempo libre para poder meditarlos. Es posible que nos influyan al establecer una estrategia de gestión de la seguridad a medio plazo en nuestras compañías o en nuestros clientes.

Richard Bejtlich es un acreditado experto en seguridad y autor de varios libros de seguridad en redes y análisis forense. Dos de sus obras más conocidas son *"The Tao of Network Security Monitoring"* y *"Extrusion Detection"*. Desde mediados de 2007, Bejtlich está a cargo del grupo de respuesta a incidentes de General Electric, una de las multinacionales que, como él menciona, "aparece en la lista de las Fortune 5 mundiales".

Taosecurity toma el nombre de la pequeña compañía de seguridad creada por el señor Bejtlich en el año 2000. El primer artículo data de enero de 2003. Desde entonces, cada año, el autor publica de 200 a 500 artículos. El objetivo inicial del *blog* era publicar críticas de los libros de seguridad que, paulatinamente, iban apareciendo. En la actualidad, los escritos que encontramos en su *blog* versan sobre temas de seguridad digital como la monitorización de redes, la respuesta a incidentes y el análisis forense.

Me gustaría resaltar tres ideas que, con frecuencia, encuentran su espacio en los artículos de Taosecurity.

- La primera es bastante heterodoxa: en estos tiempos de estándares, certificaciones y homogeneización de plataformas tecnológicas, Bejtlich

seguridad que hayamos definido. Para él, es más importante verificar la seguridad real de un sistema que el cumplimiento de un control de seguridad. Por ello, propone métricas relacionadas con la "resistencia" y la "capacidad de supervivencia" de un sistema.

- La segunda pone de relieve el contraste entre la forma de tratar la seguridad en el mundo de la seguridad física y en el mundo digital. El autor argumenta que la mayoría de las medidas de seguridad digital se aplican sobre vulnerabilidades, mientras que las medidas más efectivas que se implementan en seguridad física tratan de controlar amenazas. Su propuesta es aplicar esta filosofía en el mundo de la seguridad digital de un modo más sistemático.

- La tercera versa sobre cómo las compañías que sufren incidentes de seguridad digital no sufragan la mayor parte del coste que estos incidentes generan. Son sus clientes y, en última instancia, los ciudadanos, quienes soportan las mayores pérdidas (por ejemplo, en robos de identidad).

Estas ideas, se esté o no de acuerdo con ellas, así como muchas otras que aparecen en *taosecurity.blogspot.com*, hacen muy recomendable su lectura.

Una incógnita por resolver es cómo el señor Bejtlich encuentra tiempo, tras gestionar la respuesta a los incidentes de seguridad en General Electric, para mantener, no sólo su *blog* *taosecurity*, sino también para leer y comentar cerca de 20 libros de seguridad cada año, como menciona en su página personal <http://www.bejtlich.net/reading.html>.

Alberto Partida Rodríguez
Especialista en Seguridad TI
Securityandrisk.blogspot.com

Sugerencias y comentarios:
apartidar@gmail.com

