



SECURITY LOG MANAGEMENT Identifying Patterns in the Chaos

Autores: Jacob Babbin, Dave Kleiman, Dr. Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutiérrez
Editorial: Syngress Publishing, Inc
Año 2006 – 334 páginas
ISBN: 1-59749-042-3
www.syngress.com

Como administrador de sistemas o profesional de la Seguridad TIC, es probable que en más de una ocasión se haya encontrado inundado por un diluvio de registros *log* aparentemente incontables. A pesar de la proliferación de herramientas de *reporting* y generación de *logs*, los autores de este volumen señalan que la obtención de información útil de *logs* continúa siendo una labor ardua, ya que los ordenadores siguen estando lejos de ser todo lo inteligentes que se desearía. Por ello, el propósito principal de este libro es ilustrar el uso de la combinación de software de código abierto, como Tcpsdstat y Snort para crear informes concretos y significativos que den una idea real de la salud de la red. En este sentido, la obra pretende enseñar a los profesionales cómo analizar, manejar y automatizar los archivos *log* de seguridad para generar información útil, y cómo optimizar las herramientas

para un uso más eficiente y seguro de sus redes.

El libro propone en su comienzo el "Top 10" de *logs* de seguridad que los profesionales de TI deberían analizar regularmente (desde el envío y recepción de datos en las grandes estaciones de trabajo a través de un cortafuegos, hasta las alertas IDS más significativas). El segundo capítulo aborda las posibilidades de realizar informes de los sistemas de detección de intrusiones, mientras que el tercero se centra en los informes de cortafuegos. Los siguientes capítulos realizan un recorrido por los informes de sistemas y dispositivos de red, la creación de una infraestructura de *reporting*, y las soluciones escalables para empresas. Finalmente, la última parte del libro analiza la gestión de archivos *log* con Log Parser, la investigación de intrusos con Log Parser y la gestión de alertas de Snort con Microsoft Log Parser. ■



REAL DIGITAL FORENSICS. Computer Security and Incident Response

Autores: Keith J. Jones, Richard Bejtlich, Curtis W. Rose
Editorial: Addison- Wesley
Año 2006 – 650 páginas
(incluye CD-Rom)
ISBN: 0-321-24069-3
www.awprofessional.com

No se puede tener éxito en el campo de las técnicas de análisis forense informático sin la práctica sobre el terreno y, paralelamente, no se puede conseguir esta práctica sin verdaderos datos forenses. Esta es la llamada que realiza el libro *Real Digital Forensics*, en el cual un equipo de expertos en análisis forense informático desarrolla seis investigaciones forenses detalladas, desde una perspectiva muy cercana a la realidad. Además, en el DVD que se adjunta en el libro se incluyen todos los datos que se necesitan para que el lector pueda llevarlos a la práctica.

Las pruebas que aportan el volumen y el DVD fueron recopiladas y analizadas usando los mismos instrumentos empleados por los autores en sus investigaciones, en todos los casos, herramientas de fuente abierta.

Entre sus contenidos, la obra hace referencia a casos que tienen como protagonistas a instituciones financieras o empresas de software, entre otros, y delitos que van desde el robo de propiedad intelectual a uso fraudulento de datos financieros. Además, el análisis paso a paso de cada investigación permite descubrir las técnicas más frecuentes de los profesionales informáticos forenses. ■



LA PRIVACIDAD ELECTRÓNICA. Internet en el centro de protección

Autor: Luis Ángel Ballesteros Moffa
Editorial: Tirant Lo Blanch
Año 2005 – 348 páginas
ISBN: 84-8456-490-8
www.tirant.com

Hoy en día, las comunicaciones electrónicas suponen un punto de inflexión en la tutela jurídica de los datos personales. Por ello, cualquier análisis que se lleva a cabo ha de partir de la defensa del derecho a la protección de los mismos. Así, este libro trata de poner de manifiesto la interacción que se da entre las redes de comunicación y los tradicionales ficheros o bancos de datos, con el fin de analizar de forma crítica el fenómeno de la privacidad electrónica, dentro del contexto por la tutela de la información personal.

Para el autor, el gran reto es conjugar los avances tecnológicos con el respeto a los derechos fundamentales, entre los que se encuentra el Derecho a la Protección de Datos.

En la obra, prologada por José Luis Piñar Mañas, Director de la Agencia Española de Protección de Datos (AEPD), se lleva a cabo un riguroso análisis

del sector de las telecomunicaciones y nuevas tecnologías, abordando temas como el tratamiento de datos de tráfico y localización, *cookies* y otros dispositivos invisibles; o el fenómeno del *spam*. La obra, además, también analiza la respuesta que el derecho ha querido dar para tutelar y garantizar el respeto a la protección de datos. La profundidad del estudio del profesor Ballesteros ha sido merecedor del VIII Premio "Protección de Datos Personales", correspondiente al año 2004, convocado por la AEPD.

La presente obra se divide en tres capítulos generales: **1. Las comunicaciones electrónicas como punto de inflexión en la tutela jurídica de los datos personales;** **2. Nuevos retos y avances en el marco de una institución consolidada;** **3. La protección de datos frente a las modernas tecnologías de la comunicación.** ■



SEGURIDAD EN INTERNET

Autor: Gonzalo Asensio
Editorial: Nowtilus
Año 2006 – 318 páginas
ISBN: 84-9763-293-5
www.nowtilus.com

Seguridad en Internet, de Gonzalo Asensio, se presenta como una obra completa para proteger el ordenador con software gratuito. Como bien sabrá el lector de SIC, no se trata de la primera obra, ni la última, que aborda este tema en formato generalista, pero hay que reconocer, a favor del autor, que lo aborda de una forma sencilla y comprensible para la mayoría de los lectores, al utilizar un lenguaje directo y claro. Es una obra dirigida a un público poco versado, de ahí que en la primera parte del libro se explique incluso qué es Internet y los principios básicos de la seguridad informática. Según se avanza en su lectura, el autor explica ejemplos de cómo recuperar un sistema operativo, cómo navegar por Internet de manera segura y anóni-

nima o cómo librarse del *spam* en los correos electrónicos.

Asimismo, la obra también aborda otros temas como el uso de los sistemas de detección de intrusos (IDS), la seguridad en los programas de intercambio P2P o cómo configurar un *firewall* seguro y evitar ataques.

Al final del libro, el autor incluye dos anexos donde explica cómo analizar y valorar la seguridad de los datos, y ofrece una lista con 50 webs de habla hispana que contienen en su mayoría los aspectos básicos en temas de seguridad. El epílogo del libro, que ha contado con el apoyo de Red.es para su elaboración, es de José Barberá Heredia, Asesor del Secretario de Telecomunicaciones y para la Sociedad de la Información. ■