



OPEN SOURCE SYSTEMS SECURITY CERTIFICATION

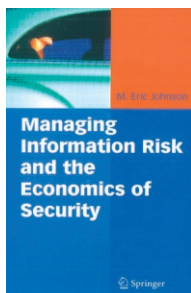
Autores: Ernesto Damiani, Claudio Agostino Ardagna y Mabil El Ioini
Editorial: Springer
Año: 2009 – 202 páginas
ISBN-13: 978-0-387-77323-0
www.springer.com

Quienes estén interesados en desarrollar, desplegar y adoptar sistemas de software de fuente abierta (OSS), pero carezcan de suficientes conocimientos sobre algunas propiedades no-funcionales de este tipo de sistemas, como las relacionadas con la seguridad, encontrarán de gran utilidad este volumen que introduce nociones básicas sobre control de accesos y sobre las certificaciones de seguridad basadas en pruebas y basadas en modelos.

En la obra se exponen también diversos estándares para certificar la seguridad, entre los que figura el estándar internacional para certificar productos de TI Common Criteria (ISO/

IEC 15408) (CC 2006); y se abordan los aspectos técnicos y científicos de la certificación de seguridad de los OSS a través de casos de estudio sobre las certificaciones Linux, ICISA y CCHIT. Además, los últimos capítulos de la obra proporcionan una visión general sobre el papel de los laboratorios virtuales de pruebas y sobre las certificaciones de seguridad de OSS a largo plazo.

Cabe señalar igualmente que los autores del libro abogan en estas páginas por la certificación de la seguridad como vía para fomentar la adopción del OSS en ciertos ámbitos en los que la seguridad es crucial, como el de las telecomunicaciones, el gubernamental o el militar. ■



MANAGING INFORMATION RISK AND THE ECONOMICS OF SECURITY

Autor: M. Eric Johnson
Editorial: Springer
Año: 2009 – 332 páginas
ISBN: 978-0-387-09761-9
www.springer.com

En lugar de centrarse en los aspectos más técnicos de la seguridad de la información, el presente volumen pone el foco en la gestión de los riesgos que la acechan y en el impacto económico de esos peligros, tanto para las empresas como para los países. Asimismo, es interesante destacar que muchos temas que se tratan en esta obra fueron presentados y debatidos en el *2008 Workshop on the Economics of Information Security (WEIS)*; una conferencia que reunió a más de cien expertos en seguridad de la información, provenientes de diversos países de los cinco continentes.

Algunos de estos temas, analizados con detalle en las páginas del libro, son: la idoneidad o no de los mecanismos empleados para proteger los pagos realizados a través de los llamados *nonbanks*, o negocios que, sin ser bancos, ofrecen los mismos servicios que éstos; las políticas establecidas en la Unión Europea para proporcionar seguridad a su economía

y a su mercado interno, protegiendo las comunicaciones electrónicas; la herramienta BORIS (*Business Oriented Management of Information Security*), que enlaza los objetivos del negocio con los de la seguridad de la información; los efectos que tiene sobre la economía la inversión óptima en seguridad de la información; cómo lograr que los directivos sean capaces de comprender, comparar y evaluar los riesgos para la seguridad y sus consecuencias económicas; cuáles son los costes tecnológicos y humanos así como los beneficios de proteger los lápices USB en las compañías; cómo utilizar una política de controles e incentivos para que los empleados no pongan en peligro la integridad de la información; la rentabilidad económica de las redes robot o *botnets*; cuáles son los beneficios concretos del diseño e implantación de las políticas de seguridad adecuadas; o las implicaciones sociales de la transparencia a la hora de procesar datos personales. ■



SECURITY MONITORING Proven Methods for Incident Detection on Enterprise Networks

Autores: Chris Fry y Martin Nystrom
Editorial: O'Reilly
Año: 2009 – 227 páginas
ISBN: 978-0-596-51816-5
www.oreilly.com

Chris Fry y Martin Nystrom han plasmado en esta obra su dilatada experiencia respondiendo a incidentes de seguridad para proteger la red global de Cisco Systems, con el objetivo de ayudar a los lectores de la misma a desarrollar las estrategias y las técnicas más adecuadas para detectar incidentes en las redes de sus empresas, utilizando un método que han denominado “monitorización basada en políticas”.

Para ello, ambos expertos comienzan exponiendo en qué consiste esta particular filosofía de la monitorización para después profundizar en cada uno de los seis pasos que, según esta filosofía, es necesario adoptar si se quiere mejorar la monitorización de la red de una empresa.

Cada uno de estos pasos está recogido en un capítulo del libro, el pri-

mero de los cuales enseña a desarrollar políticas definiendo las reglas, regulaciones y criterios de monitorización; a continuación, se muestra cómo mejorar el conocimiento de la infraestructura de la red usando, para ello, telemetría de red; luego, se dice cómo seleccionar las infraestructuras que deben ser monitorizadas y se identifican los tipos de eventos que hacen falta para descubrir violaciones de políticas; el siguiente capítulo aporta los conocimientos necesarios para recopilar datos, generar alertas y sincronizar los sistemas utilizando, para ello, información contextual; y, finalmente, los lectores aprenden a evitar que se produzcan vacíos de seguridad a la hora de recopilar y monitorizar eventos. La obra ilustra cada uno de estos pasos con ejemplos reales de cada uno de ellos y casos de estudio. ■



BEAUTIFUL SECURITY Leading Security Experts Explain How to Think

Autores: Andy Oram y John Viega
Editorial: O'Reilly
Año: 2009 – 281 páginas
ISBN: 978-0-596-52748-8
www.oreilly.com

La presente antología se compone de 16 ensayos –cada uno escrito por un autor diferente– en los que se proponen nuevas vías para afrontar la seguridad lógica y que están dirigidos, fundamentalmente, a estudiantes de Informática, o a personas con conocimientos de programación, que no necesitan ser expertos en seguridad, aunque a los versados en la materia también les puede servir de guía en sus investigaciones.

El principal objetivo de la obra consiste en despertar el interés del lector en el campo de la seguridad, e incitarle a trabajar en el desarrollo de nuevas técnicas de protección; y para ello, en sus páginas, se muestran ejemplos de fallos clásicos; se explica por qué las conexiones inalámbricas son un campo fértil para la ingeniería social; se reivindica la importancia de las métricas de la seguridad, como

herramientas imprescindibles para poder valorar el grado de peligrosidad de las amenazas y así tomar las decisiones más apropiadas; se diserta sobre la economía sumergida de las brechas de seguridad; se propone un nuevo modelo de protección del comercio electrónico; y se sugiere cómo lograr que la publicidad *on-line* esté más protegida.

También dedica la obra un capítulo al popular PGP (*Pretty Good Privacy*), que supuso, en 1991, la popularización del uso del cifrado fuerte, hasta entonces reservado a los gobiernos; y otro a los sistemas de fuente abierta de detección proactiva de vulnerabilidades; mientras que en los restantes ensayos que conforman el texto se enumeran los requisitos de la herramienta ideal de gestión de *logs*, o se subraya la importancia de disponer de distintas fuentes de datos para mejorar los ratios de detección de incidentes, entre otros aspectos. ■