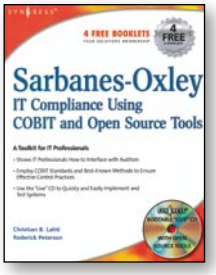


SARBANES-OXLEY

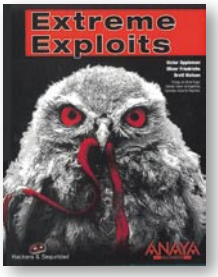
IT Compliance using Cobit and Open Source Tools

Autores: Christian B. Lahti y Roderick Peterson
Editorial: Syngress
Año 2005 – 333 páginas (incluye CD)
ISBN: 1-59749-036-9
www.syngress.com

Esencialmente técnico, este título acerca al lector a las tecnologías de código abierto y los estándares Cobit articulándolos en la esfera del cumplimiento de la normativa Sarbanes-Oxley, no tanto desde una perspectiva puramente de implementación, sino principalmente de negocio. En este sentido, el libro primero ahonda en argumentos organizativos y de procesos de negocio relativos a SOX y al *open source*, y posteriormente en herramientas específicas y estrategias de implementación para el mejor uso de las tecnologías de código abierto.

Además, se incluye un CD con una versión de Linux y una colección de software y herramientas *open source* diseñadas como complemento a los ejemplos incluidos a partir del capítulo 5 del libro.

Sucintamente, algunas de las cuestiones fundamentales a las que responde el contenido del volumen son: Cómo organizar los recursos de TI en el cumplimiento de SOX; Conocer las penas asociadas al no cumplimiento; Cómo implantar los estándares Cobit y los mejores métodos en la organización; Crear una política de cumplimiento de SOX; Planificar y organizar la estrategia COBIT como soporte de los objetivos de negocio; Cómo incorporar las aplicaciones necesarias e implementar el plan; o cómo controlar el proceso de despliegue de COBIT. ■

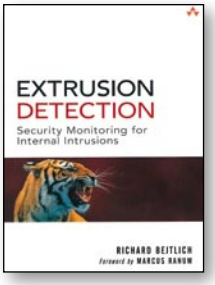


EXTREME EXPLOITS

Autores: Victor Oppleman, Oliver Friedrichs y Brett Watson
Editorial: Anaya Multimedia
Año 2006 – 544 páginas
ISBN: 84-415-2009-7
www.anayamultimedia.es

A lo largo de los 18 capítulos, estructurados en cuatro partes, en los que se divide *Extreme Exploits*, los autores de la obra se proponen ayudar a comprender y afrontar el gran auge de amenazas actuales en el ámbito de la seguridad de la información. Para ello, ponen a disposición del lector los conceptos y técnicas adquiridos por ellos mismos en la defensa de algunas de las redes de información más importantes y que son objetivos de ataque continuado. Para lograr este fin, el libro aborda las amenazas conceptualmente y analiza la base principal sobre las que se asientan para que el lector tenga una comprensión más detallada de las tácticas implicadas, tanto en la defensa como en la agresión. De este modo, a lo largo de sus capítulos, se adentra desde el perímetro de una organización hasta la realización de un análisis forense digital del portátil de un empleado.

En la primera parte, **Infraestructura de Internet para profesionales de la seguridad**, se explican los peligros que suelen pasarse por alto con respecto al enrutamiento y al Servicio de Nombres de Dominio (DNS) en Internet. En la segunda parte, **Defensa del perímetro e infraestructura crítica de Internet** se aborda el filtrado de paquetes, la detección y prevención de intrusiones o la defensa de aplicaciones críticas habituales, entre otras cuestiones. Posteriormente, en **Asesorías de vulnerabilidad de red** se desgrana el proceso para la realización de asesorías de vulnerabilidad y, finalmente, en el último bloque temático, **Diseño de contramedidas para las amenazas del mañana**, se exploran los métodos forenses digitales, el *malware* y los detalles del desarrollo de software de seguridad. ■



EXTRUSION DETECTION

Security Monitoring for Internal Intrusions

Autor: Richard Bejtlich
Editorial: Addison-Wesley
Año 2006 – 385 páginas
ISBN: 0– 321–34996-2
www.awprofessional.com

La obra centra su planteamiento en los ataques lanzados contra la seguridad de los activos de la información dentro de las compañías por parte de intrusos que comprometen los buscadores web de los usuarios, los correos electrónicos y *chats* clientes o cualquier otro software conectado a Internet. Por ello, el autor propone proteger sistemáticamente el software cliente y monitorizar el tráfico que genera. La obra se presenta como una guía para prevenir, detectar y mitigar las brechas de seguridad que se producen desde dentro hacia fuera. Su autor ofrece unas explicaciones comprensibles sobre las actuales amenazas basadas en cliente, y soluciones paso a paso contra el tráfico real y de datos. De esta forma, el lector podrá aprender a evaluar las amenazas de los clientes internos, a diseñar redes para detectar anomalías en el tráfico saliente, configurar redes para hacer frente a los ataques internos y, especialmente, a poder responder a ellos de forma eficaz cuando se produzcan.

En sus diez capítulos repartidos en tres partes (**Detección y Control de Intrusiones**, **Operaciones de Seguridad de la Red**, e **Intrusiones Internas**), se proponen teorías, herramientas y técnicas para la creación de redes defensivas; la defensa contra sitios maliciosos, *exploits* de Internet Explorer, *bots*, troyanos, gusanos y otros ataques; la implantación efectiva de un control de acceso a la red en la tercera capa, o cómo responder a los ataques internos con herramientas de análisis forense pormenorizado, entre otros temas. La obra está prologada por **Marcus Ranum**, renombrado experto en el diseño y puesta en práctica de sistemas de seguridad e impulsor del primer cortafuegos comercial. ■

MEASURES AND METRICS IN CORPORATE SECURITY

A Workbook for Demonstrating How Security Adds Value to Business

Autor: George K. Campbell
Editorial: CSO Executive Council
Año 2006 – 127 páginas
www.csoexecutivecouncil.com

El presente libro se propone como una guía para el desarrollo de un programa de métricas de seguridad aplicable a las operaciones corporativas críticas. La perspectiva de la obra va más allá de un "cómo hacerlo", abordando la gestión de la organización de seguridad y su alineación con los objetivos de negocio. A lo largo de los tres grandes bloques en que se divide la misma (**Fundamentos**, **Tipos de Métricas e Indicadores de Rendimiento**, y **Cómo construir un modelo adecuado a las necesidades de la organización**), el autor busca dar respuesta a la pregunta "¿por qué métricas de seguridad?".

Asimismo, el volumen proporciona 375 ejemplos reales de métricas de seguridad clasificadas en 13 categorías (Tendencias relacionadas con la seguridad; Comunicar el conocimiento sobre el riesgo; Implicaciones de la Auditoría; Investigaciones previas; Exámenes *due diligence*; Riesgo reputacional y conducta de negocio; Investigaciones e incidentes delictivos; Operaciones de seguridad, Seguridad física y Protección de premisas; Gestión del riesgo informativo; Planes de contingencia y Continuidad de negocio; Programas de seguridad basados en el negocio; Confianza con las funciones de seguridad corporativas; y Gestión, Desarrollo profesional y Satisfacción del empleado).

El libro va dirigido tanto a los sectores público como privado, a CSOs nuevos o ya experimentados, CISOs, gestores de riesgo, auditores o ejecutivos con responsabilidades de seguridad e, incluso, a postgraduados y estudiantes avanzados en el campo de la seguridad. ■