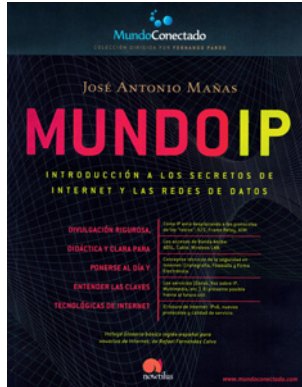


MUNDO IP Introducción a los secretos de Internet y las redes de datos

Autor: José Antonio Mañas
Editorial: Nowtilus
Colección: Mundo Conectado
Año: 2004 - 367 páginas
ISBN: 84-9763-026-2
www.mundoconectado.com



Para los lectores de SIC, el autor del libro aquí mencionado no necesita presentación. De la mano de la editorial Nowtilus y al cobijo de la colección acogida en su seno Mundo Conectado, José Antonio Mañas desembarca en el mundo de la creación literaria focalizada en el campo de las TIC acreditando una obra que, aunque bien pudiera parecer de escasa ambición y en absoluto novedosa a tenor de su título y subsiguiente subtítulo, por el contrario sí constituye una referencia más que recomendable.

En primer lugar, porque para muchos Mundo IP puede ser un libro necesario, aún a estas alturas. No por las cosas que cuenta sino por cómo las cuenta. En las trescientas páginas de su cosecha —el resto se destinan a anejear el bien conocido glosario terminológico para usuarios de Internet inglés-español de Rafael Fernández Calvo— se detallan las interioridades del, sin duda, protocolo tecnológico con mayor predicamento en entornos telemáticos y, ya puestos, transcendencia social. Con todo, esto no tendría nada de novedoso si no fuera por un pequeño pero nuclear matiz, que es la cuasi 'legendaria' pericia divulgadora del catedrático de la UPM para atinar en sus aseveraciones, haciendo sencillo lo complejo sin desvirtuarlo.

Es, pues, un libro de divulgación en su auténtico sentido. Ágil y aclarador, resume de un tirón la atribulada singladura de Internet y las telecomunicaciones: desde el archifamoso e inconsciente parto en cuna no civil y su crianza en regazos universitarios hasta su actual adolescencia, tan llena de esperanzas y sueños, aunque no exento de espinillas y achaques prematuros (¿cuándo llegará a su auténtica madurez?).

Sucintamente, sus tripas se desgranar en dieciséis capítulos, éstos: Redes de ordenadores; OSI: el mundo de los estándares; Internet: funciona ino lo toques!; TCP: red de transporte; El problema de las direcciones; El problema de las rutas; Multicast; La calidad del servicio; La gestión de la red; Transmisión de datos; Los problemas de seguridad; Redes privadas virtuales; Tecnologías para prestar servicios; Servicios IP; Servicios Internet; Cierre.

Naturalmente, el epígrafe de la seguridad es abordado por el autor —como no podría ser de otra manera dado su pedigrí— con especial esmero, presagiando —sin duda— próximos alumbramientos creativos de un mayor calado en la materia y en aquella otra que también domina como pocos, la actividad mercantil mediante operativa TIC a través de soportes electrónicos.

En este epígrafe, dice algunas cosas de encantador y refrescante perogrullo como por ejemplo que *“Los objetivos de seguridad casi nunca se consiguen en blanco y negro. Raramente es tan simple como estar seguro o no estarlo. Lo habitual es estar más o menos seguro, en proporción inversa a que sea más o menos fácil violar el objetivo de seguridad correspondiente”*.

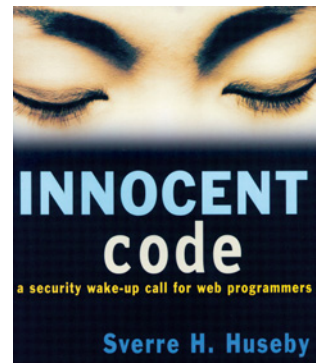
Para finalizar, cabe reseñar que es pretensión del autor ir actualizando la obra vía Internet, idea loable e ingeniosa de la editorial que le cobija, si bien resulta chocante en estos tiempos que en cambio no haya considerado apropiado que la versión en papel de la obra no vaya acompañada de un cd-rom con su homónima en soporte digital.

En resumen, es un libro absolutamente recomendable tanto para neófitos que no quieran atragantarse drásticamente en su desembarco en el Mundo IP como para aquellos otros que precisen refrescar conceptos y su tiempo sea oro.

Luis Fernández Delgado

INNOCENT CODE A security wake-up call for web programmers

Autor: Sverre H. Huseby
Editorial: John Wiley & Sons
Año: 2003 - 226 páginas
ISBN: 0-470-85744-7
www.wiley.com



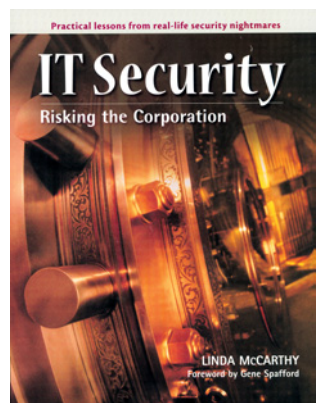
La existencia de libros como el aquí mencionado tienen sencilla justificación. Sin ir más lejos, no hace ni un mes que vió la luz un informe bastante inquietante de WebCohort centrado en las debilidades de seguridad de las aplicaciones web constatadas en los últimos cuatro años. Según el susodicho, tan solo un 10 por ciento de estas aplicaciones pueden considerarse seguras ante cualquier tipo de ataque. Los datos hacían referencia a sitios de comercio electrónico, banca en línea, B2B, etc. Entre las conclusiones se precisa que al menos un 92% de las aplicaciones web eran vulnerables a algún tipo de ataque.

Sverre H. Huseby, el autor finlandés de 'Código inocente', es simple y llanamente un programador web escarmentado. Por ello, en su obra vierte toda la sapiencia recopilada encaminada expresamente a advertir sobre la histórica banalización de esta práctica al tiempo que enuncia las mejores acciones para minimizar la inseguridad de las mismas.

El libro comprende 8 capítulos, los siguientes: 1) Lo básico; 2) Pasando los datos a los subsistemas; 3) Entrada de usuario; 4) Manipulación externa: el problema del cross-site scripting; 5), Troyanos web; 6) Contraseñas y otros secretos; y 7) Enemigos del código seguro. La obra se completa con 4 apéndices, referencias y acrónimos.

IT SECURITY Risking the Corporation

Autor: Linda Spafford
Editorial: Prentice Hall
Año: 2003 - 366 páginas
ISBN: 0-13-101112-X
www.phptr.com



Con excesiva frecuencia, abordar hoy la lectura de libros de seguridad TIC supone el tedioso reto de sumergirse en miríadas de referencias, tragarse interminables listados de comandos de aviesas intenciones y también desgarrar reveladores referencias web proporcionadas por el autor de turno.

El parecer sobre este libro de Linda McCarthy —experimentada pieza clave del comité ejecutivo de la multinacional Symantec— puede cambiar, a decir del célebre Gene Spafford en su introducción, la forma en cómo ha de pensarse la seguridad, lo cual descansa curiosamente en que hay que pensar no tanto en la 'informática' como en la 'información'.

Estas reflexiones y sus interesantísimas consecuencias se plasman con acierto en el despliegue capitular de la obra: 1) Respuesta a ataques; 2) Seguridad out-of-the-box; 3) Soporte ejecutivo; 4) Acceso a la red; 5) Formación en seguridad; 6) Seguridad no planeada; 7) Mantenimiento; 8) Seguridad de la red interna; 9) Seguridad externalizada; 10) Correo-e inseguro; 11) Mirando atrás: ¿qué viene ahora?; 12) Paseo de un intruso a través de la red.