SEGURIDAD Y RESPONSABILIDAD EN LA INTERNET DE LAS COSAS (IOT)

Autora: Paloma Llaneza González
Editorial: Wolters Kluwer Año: 2018 – 356 páginas
ISBN: 9788490902929 https://tienda.wolterskluwer.es/

A finales de marzo de 2018, una mujer que cruzaba empujando su bicicleta a oscuras en Arizona, EE.UU., fue arrollada por un coche autónomo de Uber en pruebas. Tras el volante, tal como se aprecia en el vídeo publicado por la policía local, se observa que el conductor-controlador de seguridad no prestaba atención. Aunque era de noche, los sensores Lidar del vehículo deberían haber detectado a la ciclista, pero tampoco lo hicieron. Si hubiera sido un coche no autónomo y no conectado habríamos entendido que la responsabilidad recaía en mayor o menor medida en el conductor. Sin embargo, en el caso de Arizona, la cuestión de la atribución no es tan sencilla como no lo es, en general, en cualquier daño que las cosas conectadas o la Internet of Things –IoT– puedan ocasionar.

La alta complejidad del ecosistema IoT –que incluye objetos físicos, software, infraestructura de Internet, datos personales y no personales, comportamiento del usuario final, analítica de datos, etc.–, y la variedad de actores implicados –fabricantes de productos, fabricantes de sensores, productores de software, proveedores de infraestructura, otros actores involucrados en el suministro de diferentes servicios, usuarios finales, etc.–, hace que la labor de atribuir responsabilidades en caso de daño sea una tarea de enorme complejidad.

El lector encontrará en esta obra de **Paloma Llaneza** –solvente especialista jurídica de probada sagacidad– una utilísima y esclarecedora guía para entender la tecnología, su complejidad e interacciones, el estado del arte de la legislación y de la ciberseguridad de la IoT, así como las propuestas legislativas que están encima de la mesa sobre la seguridad de las cosas conectadas y la responsabilidad por los daños que causen. Absolutamente recomendable.

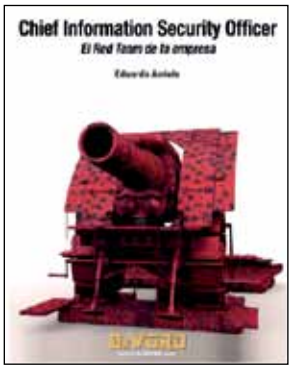
PRIVACY'S BLUEPRINT. THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES

Autor: Woodrow Hartzog
Editorial: Harvard University Press Año: 2018 – 364 páginas
ISBN: 9780674976009 http://www.hup.harvard.edu

Cada día, los usuarios de internet interactúan con numerosas tecnologías diseñadas para quebrantar su privacidad. Las redes sociales y la Internet de las Cosas, entre otras, han sido desarrolladas sin tener en cuenta la protección de la información personal e, incluso, existen leyes que no castigan tal hecho porque depende de los usuarios protegerse a sí mismos, inclusive cuando los riesgos se tornan deliberadamente contra ellos.

En **Privacy's Blueprint**, su autor, **Woodrow Hartzog,** rechaza este *status quo* argumentando que la ley debería exigir que los fabricantes de software y hardware velen por la privacidad de los datos personales en el diseño de sus productos. La doctrina legal actual trata la tecnología como si fuera neutral en cuanto a los valores del usuario: solo éste decide si funciona para bien o para mal. Pero esto no debería ser así. Según Hartzog, muchas herramientas digitales, entre ellas, las más populares, están diseñadas para exponer a las personas y manipular a los usuarios para que revelen información personal. Asimismo, sostiene que las ganancias devenidas de la privacidad provendrán de mejores reglas para los productos, no para los usuarios.

En este sentido, **Privacy's Blueprint** pretende corregir esto mediante el desarrollo de las bases teóricas de un nuevo tipo de ley de privacidad que responda a la forma en que las personas realmente perciben y usan las tecnologías digitales. En el libro se explica que la ley puede exigir cifrar, puede prohibir las interfaces maliciosas que engañan a los usuarios y los dejan vulnerables, puede prevenir ante los abusos de la vigilancia biométrica y puede hacer que la tecnología sea digna de nuestra confianza.



CHIEF INFORMATION SECURITY OFFICER: EL RED TEAM DE LA EMPRESA

Autor: Eduardo Arriols
Editorial: 0xWord Año: 2018 – 248 páginas
ISBN: 9788409014972 https://0xword.com/es/

Si bien el origen de los equipos de Red Team es militar y se englobaba dentro de los conocidos juegos de guerra o *war gamming*, cada vez son más las organizaciones que optan por este enfoque para identificar el nivel de exposición y riesgo, e incrementar las capacidades de detección y respuesta a potenciales incidentes. Su desarrollo plantea la necesidad de hacer uso de una metodología diferente a lo habitual, donde podrán ser utilizados de forma conjunta vectores de ataque dentro del ámbito digital, físico y humano para lograr la intrusión.

Eduardo Arriols, Responsable del servicio Red Team de **InnoTec** –Grupo Entelgy– es el autor de este interesante libro –cuyo título induce al equivoco por incluir innecesariamente el término "Chief Information Security Officer"– que sumergirá al lector en la ejecución de estos ejercicios, exponiendo técnicas utilizadas para identificar vectores de acceso en cualquier ámbito de actuación, el uso de una metodología que permita lograr una intrusión real y simular de forma correcta a un adversario real, así como aquellos aspectos más relevantes adquiridos durante la experiencia del desarrollo de ejercicios Red Team en grandes organizaciones.

La obra comienza así con una introducción a los Red Team explicando su definición; las diferencias entre auditoria, *test* de intrusión y ejercicio de Red Team; el pensamiento crítico; el uso de los ejercicios para la toma de decisiones; y la metodología, entre otros aspectos. Tras ello, el lector se sumergirá en capítulos que desarrollan temas tan importantes como los vectores de acceso digitales, físicos y de ingeniería social, intrusiones internas y elevación de privilegios, los movimientos laterales, despliegues de persistencia, así como el análisis interno de la organización y acceso a activos críticos. Una estructura que permitirá al lector utilizar este libro de forma puntual o como guía para el desarrollo de ejercicios de intrusión desde su inicio hasta la finalización de los mismos.