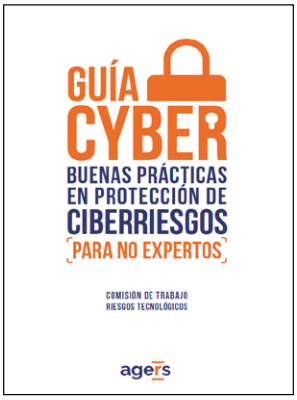
GUÍA CYBER BUENAS PRÁCTICAS EN PROTECCIÓN DE CIBERRIESGOS (PARA NO EXPERTOS)



Autores: Comisión de trabajo riesgos tecnológicos de AGERS
Editorial: Agers
Año: 2023 – 70 páginas
ISBN: 978-8409486854
https://agers.es/libreria

La **Asociación Española de Gerencia de Riesgos y Seguros (Agers)** ha presentado una ilustrativa guía con la que pretende "trasladar, fundamentalmente, al colectivo de gerentes de riesgos y seguros, pero también a todo el personal no técnico implicado en estos riesgos, qué medidas de diversa índole son recomendables para gestionar la prevención de los incidentes cibernéticos".

Para ello, a lo largo de sus 70 páginas propone un modelo que seguir a través de buenas prácticas, planteando un enfoque dividido en cinco fases: conocimiento de la empresa, identificación, protección, detección, respuesta y recuperación. En definitiva, con esta guía, sus participantes, más de dos decenas de profesionales de reconocido prestigio en este ámbito, aportan "luz sobre lo que es una adecuada gestión de la ciberseguridad según la normativa NIST y sobre aquellas medidas a las cuales el mercado de seguros cibernéticos da mayor importancia". Eso sí, "no pretendemos que con este documento nos convirtamos en expertos, pero sí entender qué tipo de medidas se pueden aplicar y los requisitos que una aseguradora exige para contratar estos seguros", indican. Así pues, se trata de un documento de lectura obligada que se puede conseguir desde la web de la asociación.

WHATSAPP INT: OSINT EN WHATSAPP

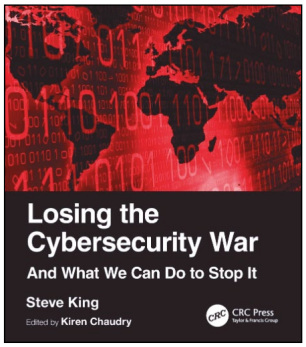
Autor: Luis Márquez
Editorial: 0xword
Año: 2023 – 210 páginas
ISBN: 978-8409485550
https://0xword.com

WhatsApp una de las aplicaciones de mensajería instantánea más utilizada, con más de 1.000 millones de mensajes al día, pero ¿qué pasaría si toda esta información cayera en las manos equivocadas, sobre todo, si fuera de carácter corporativo? Enviar audios, recibir imágenes e, incluso, activar la verificación en dos pasos son solo algunas de sus principales características que no están libres de ser vulneradas por los ciberdelincuentes que aprovechan estos puntos flacos para obtener datos tan sensibles de la víctima como su ubicación, fotografías, leer los mensajes o eliminar su cuenta.

Sorprendentemente, casi siempre, con interfaces de usuario se puede lograr vulnerar la intimidad de un usuario. Por ello, este libro trata, de forma rigurosa, cómo se realizan este tipo de ataques y cómo se pueden evitar.

¿Qué sabe Facebook de nosotros? ¿Puedo conocer desde donde chatea una persona? ¿Cómo hacer mi perfil de WhatsApp inquebrantable? Son solo algunas de las preguntas a las que este libro da respuesta. Una obra eminentemente generalista pero que también incumbe al profesional especializado que, posiblemente, use en el ámbito corporativo esta conocida plataforma de mensajería.

LOSING THE CYBERSECURITY WAR: AND WHAT WE CAN DO TO STOP IT

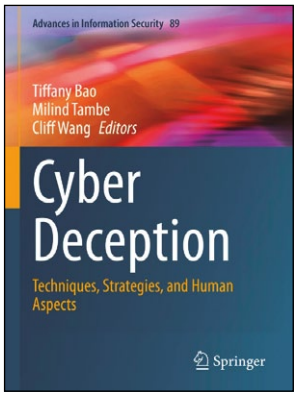


Autor: Steve King
Editorial: CRC Press
Año: 2022 – 172 páginas
ISBN: 978-1032364087
www.routledge.com

Interesante aproximación a cómo un enfoque de confianza cero puede equilibrar la 'batalla' ante cibercriminales, hacktivistas y, también, ataques de estado nación. Con una prosa de fácil lectura, rica en datos y ejemplos, **Steve King**, uno de los profesionales de ciberseguridad más reconocidos de EE.UU., explica su apuesta por una defensa basada en 'cinco pilares o campos de batalla': Economía, Tecnología, Información, Educación y Liderazgo. "Nos hemos sumergido profundamente en cada uno de ellos, pero tenemos una clara desventaja debido a la estructura constitucional y las pautas morales de comportamiento", recuerda, a la vez que ofrece su visión de cómo llegamos aquí, qué podemos hacer al respecto y cómo evitar los riesgos aún no conocidos en el futuro.

Para ello, analiza en profundidad el concepto de confianza cero y muestra cómo puede 'cambiar el juego', aplicándolo a cada uno de los cinco campos propuestos. Así, al 'entretejer' los principios de Zero Trust a lo largo de estos conceptos, el autor demuestra cómo su aplicación permitirá que los "atacantes ya no sean dueños del terreno elevado. "Como defensores y protectores, podemos aprovechar la tecnología moderna de Zero Trust para mantener nuestros datos y activos a salvo de la infiltración y la explotación", resalta.

CYBER DECEPTION

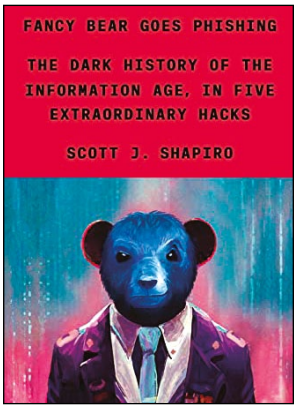


Editores: Tiffany Bao, Miling Tambe, Cliff Wang
Editorial: Springer
Año: 2023 – 250 páginas
ISBN: 978-3031166136
https://link.springer.com

Este libro presenta los diversos resultados de investigaciones recientes sobre el engaño cibernético, un campo prometedor para la ciberdefensa proactiva que tantas compañías están aplicando, algunas con tecnologías de origen español como la de CounterCraft. "Su belleza y su desafío residen en que es un campo interdisciplinario que requiere estudiar desde técnicas y estrategias, hasta aspectos humanos", destacan sus coordinadores, que han intentado cubrir en esta obra una amplia variedad de investigaciones, incluida la teoría de juegos, la inteligencia artificial, la ciencia cognitiva y la tecnología relacionada con el engaño. Además, prestan especial atención a lo que consideran tres elementos centrales del ciberengaño; comprender los comportamientos cognitivos humanos en escenarios de red señuelo; cómo desarrollar estrategias engañosas efectivas, basadas en los comportamientos humanos; y cómo diseñar técnicas que apoyen la aplicación de estrategias engañosas.

La obra es, sin duda, recomendable para quien se acerque a este campo o quiera mejorar sus conocimientos. Además, tanto el capítulo 'Uso de Amnesia para detectar infracciones de la base de datos de credenciales', como 'Engañar la identificación de amigo o enemigo basada en ML para ejecutables', se ofrecen a modo de contribución, de forma gratuita a través de la web de la editorial, bajo una licencia internacional Creative Commons Attribution 4.0.

FANCY BEAR GOES PHISHING: THE DARK HISTORY OF THE INFORMATION AGE, IN FIVE EXTRAORDINARY HACKS



Autor: Scott J Shapiro
Editorial: Farrar, Straus and Giroux
Año: 2023 – 432 páginas
ISBN: 978-0374601171
https://us.macmillan.com

Esta novedad editorial, perfecta para los meses de verano, muestra de forma perturbadora, fascinante e hipnótica, cómo actúan los grandes grupos criminales, en ocasiones patrocinados por estados, tomando como ejemplo cinco casos muy conocidos como el grupo APT, Fancy Bear o el del autor del primer virus informático de la historia, Robert Morris, entre otros.

Con una prosa desenfada, amena y mezclando información y filosofía, su autor muestra la 'trastienda' en la que se mueven y actúan estos grupos robando información, datos, traficando con ellos y realizando ataques dirigidos gracias, en muchas ocasiones, a nuestros propios fallos o falta de preparación.

"Una de las grandes paradojas de nuestro tiempo es, precisamente, la conciencia de que vivimos en una sociedad de la información... frente al desconocimiento de cómo funciona", destaca el autor, que muestra las principales herramientas que usan estos piratas informáticos dando respuesta a preguntas vitales como: ¿Por qué Internet es tan vulnerable? y, ¿cómo podemos reaccionar? con un relato trepidante, rico en referencias sobre el cibercrimen, el espionaje cibernético y la guerra que se vive más allá del ámbito físico.

CYBERSECURITY THREATS, MALWARE TRENDS, AND STRATEGIES: DISCOVER RISK MITIGATION STRATEGIES FOR MODERN THREATS TO YOUR ORGANIZATION

Autor: Tim Rains, Prólogo de Timothy Youngblood
Editorial: Packt Publishing
Año: 2023 – 584 páginas
ISBN: 978-1804613672
www.packtpub.com

Segunda edición actualizada y ampliada de esta conocida obra, escrita para un público profesional, sobre todo CISOs, con el objetivo de ayudar a "comprender y desarrollar estrategias efectivas de ciberseguridad basadas en datos para sus organizaciones".

En sus casi 600 páginas, se ofrece una amplia información sobre las tendencias a largo plazo en la divulgación y explotación de vulnerabilidades, las diferencias regionales en las infecciones de *malware* y los factores socioeconómicos que las sustentan, además de analizar cómo el *ransomware* ha evolucionado de una amenaza oscura a la amenaza más temida en ciberseguridad.

También, se ofrece información sobre los roles que desempeñan los gobiernos en la ciberseguridad, incluido su papel como actor de amenazas y cómo mitigar el acceso a los datos más críticos. Dedica su último y amplio capítulo a ofrecer una "inmersión profunda" en los enfoques modernos de ciberprotección que utilizan la nube, con un enfoque riguroso por parte del autor, que ha sido asesor jefe de seguridad global de Microsoft y CISO Global para el sector público mundial de Amazon Web Services.

CYBERSECURITY BLUE TEAM STRATEGIES: UNCOVER THE SECRETS OF BLUE TEAMS TO COMBAT CYBER THREATS IN YOUR ORGANIZATION

Autores: Kunal Sehgal y Nikolaos Thymianis
Editorial: Packt Publishing
Año: 2023 – 208 páginas
ISBN: 978-1801072472
www.packtpub.com

En el panorama editorial son muchos y de calidad los libros dedicados al concepto de Red Team, pero muy escasos los que tratan del Blue Team. Por eso, es bienvenido este 'Cybersecurity Blue Team Strategies', que se ofrece a modo de guía para ampliar los conocimientos de cualquier especialista en la materia o del que quiera aprender de ella. En él se muestran desde cómo implementar en este tipo de ejercicios medidas defensivas de ciberprotección, siempre pensando en la mente del atacante, hasta cómo probar y evaluar la eficacia de la postura de ciberseguridad de la empresa que los pone en práctica.

"Independientemente del medio que haya elegido su organización: nube, local o híbrido, este libro le proporcionará una comprensión profunda de cómo los atacantes cibernéticos pueden penetrar sus sistemas y obtener acceso a información confidencial", recuerdan sus autores, que comienzan la obra con una breve descripción general de la importancia de un equipo azul, para mostrar en profundidad las principales técnicas y mejores prácticas que un operador de ciberseguridad o un profesional del equipo azul deben conocer. Sin duda, una obra de referencia para los que quieran implementar los equipos azules (la obra va dirigida, sobre todo a CISOs) acordes a un buen programa de gobierno, para reforzar los controles preventivos y de detección.

INGENIERÍA SOCIAL. LA CIENCIA DE LA PIRATERÍA HUMANA

Autor: Christopher Hadnagy
Editorial: Anaya Multimedia
Año: 2023 – 288 páginas
ISBN: 978-8441547926
anayamultimedia.es

"En la fortaleza de defensa que construimos en torno a nuestros datos, el elemento humano siempre es el eslabón más débil", comienza destacando el autor de esta obra que muestra los principales trucos que usa el cibercrimen para acceder a información sensible, a través de técnicas de "piratería humana" para convencer a la gente de que revele contraseñas, envíe archivos sensibles, transfiera grandes cantidades de dinero y haga voluntariamente otros actos contrarios a sus intereses. Frente a ello, **Christopher Hadnagy** detalla cómo se puede ayudar a los responsables de ciberseguridad a identificar y remediar los puntos débiles de sus propios sistemas, en este ámbito. Para ello explora el actual modelo de comunicación, la mentalidad tribal, las habilidades de observación, la manipulación y otros aspectos que permiten identificar, combatir y evitar las últimas técnicas de este tipo de ataques a nuestras organizaciones. Es de agradecer la abundancia de casos prácticos extraídos de la prensa diaria y el gran número de consejos sobre elicitación, pretextos, recopilación de información, *tailgating, shoulder surfing* y *phishing*. En definitiva, destaca el autor, "este libro profundiza en cómo se puede influir en los seres humanos para que tomen decisiones comprometedoras".