BOLETÍN INFORMATIVO

INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 16 de junio de 2023.- El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y empresas. Además, es un instrumento para la trasformación social y oportunidad para la innovación, fomentando la I+D+i y el talento.

INCIBE centra sus esfuerzos en la prestación de servicios públicos de prevención, concienciación, detección y respuesta ante incidentes de seguridad, adaptándose a cada público específico (menores, ciudadanía y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

Honeypot: una trampa para los ciberdelincuentes

Un *honeypot* es una herramienta de seguridad que actúa como equipo o sistema altamente atractivo para un ciberdelincuente, es decir, un señuelo, con el fin de monitorizar o detectar posibles ciberataques en la empresa o entorno, antes de que puedan afectar a sistemas críticos, y así aprender de ellos para poder evitarlos en el futuro.

Pero, ¿cómo se consigue engañar a los ciberdelincuentes? El *honeypot* crea servicios falsos que suelen ser objetivos de ataque, como un servidor web o una base de datos, para que cuando atenten contra ellos se recojan los datos del ciberataque. Posteriormente, estos se utilizarán para preparar a los sistemas reales ante posibles amenazas similares.

Más información: https://www.incibe.es/empresas/blog

Campaña de correos electrónicos fraudulentos suplantando a Correos

Esta semana INCIBE ha detectado una campaña de *phishing* a la empresa de mensajería y paquetería Correos, cuyo objetivo es robar información personal de la víctima. En el correo electrónico se hacen pasar por la entidad y solicitan que se modifique la fecha de entrega de un paquete para proceder a su reenvío.

En caso de ser víctima de este engaño, se recomienda practicar *egosurfing* para asegurarse de que los datos no han quedado expuestos en la Red y realizar capturas de pantalla de los emails o notificaciones recibidas relacionadas con el fraude para presentar una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.

Más información: https://www.incibe.es/ciudadania/avisos

Caso real del 017: un hotel es suplantado mediante la técnica de *spoofing* para estafar a sus clientes

Un usuario se pone en contacto con el servicio Tu Ayuda en Ciberseguridad porque su hotel ha sido víctima de una suplantación de identidad. Uno de los clientes aseguraba haber recibido un correo electrónico suyo con un enlace para que pagara la factura y quiso comprobar la veracidad del mismo, puesto que habían acordado hacerlo a través de la plataforma.

Este caso real relata un fraude conocido como *email spoofing*, con dos tipos de víctimas y consecuencias. Por una parte, el hotel, que ve su imagen dañada al ser suplantado, y por otra, los clientes, que tras reservar sus vacaciones, reciben un correo fraudulento para realizar el pago. ¿Cómo pudo ocurrir esta situación y qué pautas de ciberseguridad le proporcionó INCIBE?

Más información: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales

Más información: https://www.incibe.es/