BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 11 de septiembre de 2020.- 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, ciudadanos y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

Campaña de distribución de malware a través de email que suplanta a la AEAT y Vodafone

Esta semana, INCIBE, a través de Protege tu Empresa, ha detectado dos casos diferentes de suplantación a la Agencia Estatal de Administración Tributaria (AEAT), organismo perteneciente al Ministerio de Hacienda. Por un lado, una campaña de envío de correos electrónicos fraudulentos que tratan de suplantar a la entidad con la intención de distribuir *malware*.

El correo electrónico distribuye un tipo de troyano diseñado para robar datos personales del usuario o realizar tareas encubiertas para preparar el equipo para posteriores ataques.

Por otro lado, se detectó una campaña masiva de envío de correos electrónicos fraudulentos que también tratan de suplantar a la AEAT con el propósito de difundir *malware*. Sin embargo, en esta ocasión, en el cuerpo del mensaje se solicita al usuario verificar si el «monto de la factura fiscal es correcto» y se le indica que el plazo de pago ha finalizado.

Además, desde INCIBE se ha detectado una campaña de envío de correos electrónicos fraudulentos que tratan de suplantar a Vodafone, con el fin de difundir *malware*.

Más información en: https://www.incibe.es/protege-tu-empresa/avisos-seguridad, https://www.incibe.es/protege-tu-empresa/avisos-seguridad y https://www.incibe.es/protege-tu-empresa/avisos-seguridad.

CSIRT Telefónica, uno de los 7 equipos españoles participantes, gana los International CyberEx 2020

El equipo español CSIRT Telefónica se proclamó campeón de la sexta edición de los International CyberEx, con 4.300 puntos, tras conseguir la máxima puntuación en tres de las pruebas propuestas del ejercicio en formato CTF (Capture The Flag): análisis forense, ingeniería inversa y criptografía.

Durante 8 horas, han participado 80 equipos procedentes de 39 países, entre los que se encontraba España, con 7 equipos; junto a otros 10 países europeos, 16 de Latinoamérica, 5 de África, 6 de Asia y Estados Unidos.

Más información en: https://www.incibe.es/sala-prensa/notas-prensa.

Shoulder surfing: mirando por encima del hombro

En el mundo de la ciberseguridad, cualquier medio utilizado para obtener información personal se considera un tipo de ciberataque, desde intentar acceder a un equipo personal o mirar por encima del hombro mientras un usuario escribe un correo o utiliza su dispositivo personal. Esto último es lo que se conoce como *shoulder surfing*. ¿Qué es y para qué sirve? Se trata de una técnica de ingeniería social empleada por los atacantes con el objetivo de conseguir información de un usuario en concreto. ¿Cómo se puede prevenir el *shoulder surfing*?

Más información en: https://www.osi.es/es/actualidad/historias-reales.

Asegura tus cuentas de usuario con la autenticación de doble factor

Actualmente, según diversos estudios, casi el 80% de los ciberataques se centran en el uso de contraseñas inseguras. De hecho, se estima que una gran parte de las contraseñas que circulan por la Red podrían ser descifradas por un atacante en un tiempo máximo de dos horas.

¿En qué consiste la autenticación de doble factor? Se puede definir como el proceso de seguridad por el cual un usuario debe confirmar su identidad de, al menos, dos maneras diferentes.

Más información en: https://www.incibe.es/protege-tu-empresa/blog.

Puertos del router: qué son y cómo afectan a nuestra seguridad

La correcta configuración de los puertos es vital para conseguir un rúter seguro. ¿Qué son? Los puertos son un concepto informático utilizado en el ámbito de las redes de comunicaciones que sirve para establecer los intercambios de información con éxito. El rúter es el encargado de transmitir

la información que entra o sale de los dispositivos conectados a la Red y la transporta, a través de rúter intermedios, hasta su destino.

En este artículo se explica cuál es su función y cómo afectan a la seguridad. Es importante identificar el papel que juegan los puertos cuando los usuarios se conectan a Internet para descargar contenidos, hablar por videoconferencia o jugar, y conocer cuáles son los pasos que deben seguir para abrirlos y cerrarlos con toda seguridad.

Más información en: https://www.osi.es/es/actualidad/blog.

Tecnologías disruptivas para la empresa segura

En los últimos años, se han ido sucediendo, de forma vertiginosa, una serie de cambios en las tecnologías que se usan en los entornos empresariales y que han ido transformando la manera de hacer negocios o de realizar las tareas por parte de los empleados.

Se considera una tecnología disruptiva cuando deja obsoletas las tecnologías imperantes hasta ese momento, al producirse un abaratamiento de los costes de producción, una mejora de las tareas realizadas para la obtención final del producto o servicio, así como una mejora de la calidad de los mismos y el tiempo empleado en producirlos. ¿Cuáles son?

Más información en: https://www.incibe.es/protege-tu-empresa/blog.

Para más información en materia de ciberseguridad visite INCIBE www.incibe.es, Protege tu Empresa https://www.incibe.es/protege-tu-empresa, OSI www.osi.es e IS4K www.is4k.es.