BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 30 de abril de 2015.- El Instituto Nacional de Ciberseguridad (INCIBE) tiene como misión reforzar la ciberseguridad, la confianza y la protección de la privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, red académica, Administración, al sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general. INCIBE elabora para los medios informativos un boletín semanal de Seguridad, con el fin de colaborar conjuntamente en la difusión de la Seguridad de la Información.

Principales informaciones de INCIBE entre el 24 y el 30 de abril de 2015.

Nueva oleada de fraude masivo que cifra equipos mediante email suplantando a "CORREOS"

INCIBE advierte de una nueva campaña masiva de fraude mediante envío de spam simulando ser Correos. En el correo electrónico se indica que no se ha podido entregar un envío y se debe seguir un proceso para poder recogerlo bajo pena de pago de una cantidad económica por cada día de retraso.

Al final del proceso, se proporciona un archivo PDF (que en realidad es un archivo con extensión .exe) que, al ejecutar, se encarga de cifrar todos los datos del equipo. Para más información sobre esta campaña de Correos, visita el aviso publicado por la Oficina de Seguridad del Internauta (OSI).

Cómo eliminar los datos de navegación

Los navegadores web son herramientas muy potentes que nos permiten acceder a todo lo que nos ofrece Internet. Desde leer las noticias hasta ponernos en contacto con amigos y familiares utilizando el correo electrónico o las redes sociales, pasando por realizar algunas compras.

Los pasos que se dan en Internet dejan un rastro en el navegador que se conoce como historial, un listado que recoge las páginas que se han visitado, y cuándo se ha hecho.

Esta información puede ser útil para posibles ciberatacantes, por lo que hay que tener presente la importancia de reforzar la privacidad

mediante el borrado periódico de estos datos. En el siguiente vídeo de la OSI se muestra lo más relevante sobre el borrado periódico de datos en el historial de navegación.

Aprende a identificar estafas en la mensajería instantánea

Tal como sucede con cualquier tecnología que cuente con muchos usuarios, las principales amenazas y estafas tradicionales se han adaptado a estas nuevas plataformas, de manera que hay que ser igual de cautos con la mensajería instantánea que lo seríamos con nuestro correo electrónico o cuando vamos por la calle.

Mensajes extraños de remitentes conocidos, enlaces a fotos en conversaciones que no se corresponden con lo hablado previamente o cadenas de bulos pueden ser excusas que lleven implícitos intentos de estafa online. En este vídeo de la OSI se detallan todos los aspectos relativos a esta realidad.

Decálogo de ciberseguridad en la información de tu empresa

¿Dónde comienza la ciberseguridad de la empresa? Por norma general, las organizaciones abordan en primer lugar la adaptación a la LOPD, ya que se trata de un requisito de carácter obligatorio si las empresas tratan datos de carácter personal (situación habitual en la mayor parte de las empresas).

Para llevar a cabo el análisis sobre la criticidad de la información que maneja cualquier organización, puede ser útil abordar las primeras fases de un Plan Director de Seguridad. Aun así, INCIBE ha elaborado un decálogo con las diez prácticas y consejos más recomendables para proteger la ciberseguridad de cualquier empresa.

Historias reales: ¡Me convertí en un spammer sin saberlo!

David es un joven empresario que tras mandar varios correos a un mismo remitente, se enteró que muchos de sus mails entraban como spam a sus remitentes más habituales. Según su proveedor de informática, la dirección IP de su servidor de correo (lo que identifica a su servidor de correo en Internet) está incluida en varias listas negras de spammers.

Además, el tráfico SMTP (Simple Mail Transfer Protocol) de su red, es decir el volumen de correo que se está gestionando desde su servidor de correo, es extrañamente elevado. Por este motivo, sus correos no llegan a los destinatarios.

¿Qué hacer cuando a un usuario le ocurra lo mismo que a David? En este caso, se debe contactar con el proveedor de servicios informáticos o de Internet. En este sentido, INCIBE ofrece a través del centro de respuesta a incidentes de seguridad (CERT) de Seguridad e Industria (CERTSI), un servicio público y gratuito de asistencia y soporte desde el cual puedes solicitar asistencia ante un incidente de seguridad.

Si tiene cualquier problema de seguridad, INCIBE y la Oficina de seguridad del Internauta OSI le ofrecen los siguientes servicios gratuitos: boletines gratuitos de seguridad, el asistente de seguridad y el servicio de atención telefónica (901 111 121). Para más información en materia de ciberseguridad visite: INCIBE www.incibe.es y OSI http://www.osi.es/

comunicacion@incibe.es
www.incibe.es
Av. José Aguado 41 / 24005 León
T. (+34) 987 877 189 / F. (+34) 987 261 016