BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 04 de noviembre de 2016.- 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 28 de octubre y el 03 de noviembre de 2016.

Importante vulnerabilidad 0-Day en Microsoft Windows

Google ha divulgado una vulnerabilidad crítica 0-Day que afecta a dispositivos con sistema operativo Windows. Aunque no está completamente descrita, indican que es una vulnerabilidad mediante la cual, sería posible que una aplicación que se estuviera ejecutando en la "Zona controlada" o SandBox, podría saltarse esas restricciones de seguridad y ejecutarse fuera de esa zona de control y acceder a sitios e información a los que no debería poder hacerlo.

Varias fuentes han confirmado que este problema se puede mitigar usando Windows 10 junto con los navegadores Microsoft Edge o Google Chrome. También han indicado desde Microsoft que los usuarios de Windows 10 que usen Windows Defender Advanced Threat Detection también están protegidos.

Detectados correos de phishing que suplantan al Banco Popular

Se han detectado correos electrónicos de una campaña de phishing que simulan proceder del Banco Popular. En esta ocasión, la excusa utilizada para engañar al usuario para que éste introduzca sus datos en la web fraudulenta, es la supuesta reactivación de la cuenta, tras haber sido bloqueada por haberse detectado actividad inusual en ella.

Si has recibido un correo de estas características y has accedido al enlace que facilita y completado y enviado la información solicitada, modifica lo antes posible tu contraseña de acceso a tu servicio de banca online del Banco Popular. Además, contacta con tu oficina

bancaria lo antes posible para informarles de lo sucedido con la tarjeta de crédito.

Tu router, tu castillo. Medidas básicas para su protección

Configurar correctamente el router es una de las tareas más importantes para salvaguardar la seguridad de nuestros dispositivos y de nuestra información personal por lo que ponte manos a la obra y ¡protege tu router!

El router es la puerta de entrada desde Internet hacia nuestra red privada por lo que configurarlo de manera correcta evitará, en la mayoría de las ocasiones, que alguien sin permiso se pueda “colar” e invada nuestra privacidad y seguridad.

Todos los router, lo que nos proporcionan las proveedores y los denominados “neutros”, cuentan con una configuración de parámetros por defecto que en la mayoría de los casos no son las más apropiadas

Una tutoría diferente: hablemos con los alumnos de sexting, ciberbullying y grooming

«Los chavales ya lo saben todo». Esa es la respuesta habitual cuando planteamos la idea de tratar temas como ciberbullying, sexting, grooming o cualquier otro riesgo de Internet.

Pero no, no lo saben todo, aunque muchas veces sí están saturados de recibir la misma información teórica sobre qué hay en Internet y qué deben hacer para prevenir determinados riesgos.

Por supuesto, es necesario que reciban esa información, pero para que ésta sea efectiva y cale en los alumnos debe complementarse con actividades prácticas y una dosis de realidad.

Octubre en un clic, #familiaCibersegura

¿Has visto el videoclip musical hecho por adolescentes para luchar contra el sexting y el acoso escolar? ¿Conoces las iniciativas más originales para prevenir problemas de convivencia en el aula? Consulta “en un clic” las noticias más destacadas de este mes.

¿Qué seguridad le pides a tu proveedor cloud?

Los servicios cloud ponen al alcance de la pyme las ventajas y funcionalidades de la tecnología que de otra forma no podrían permitirse. Los proveedores de estos servicios ofrecen escalabilidad

y flexibilidad para adaptarse sobre la marcha (pay as you go) a nuestras necesidades en cuanto a capacidad de procesamiento y de almacenamiento.

También nos permiten tener siempre disponibles y accesibles desde cualquier lugar nuestras aplicaciones. Todo esto con la posibilidad de contratar no solo la infraestructura o el software, sino también su mantenimiento. Pero, ¿cumplen también nuestros requisitos de seguridad?

Ransomware: «Truco o trato»

Existe un malware al que también le gusta jugar a «truco o trato». Un malware que también está de moda, siendo uno de los ataques más dañinos actualmente para nuestras empresas. Es un malware que se disfraza para que le dejemos entrar y pide un «trato» (un rescate) a cambio de un «truco» (te secuestra la información). Este malware, se llama ransomware, y da miedo de verdad, porque es real.

Para evitar que entren en nuestras empresas y consigan hacerse con un gran botín, debemos aplicar una serie de medidas de precaución:

- Hacer copias de seguridad periódicas y comprobar que funcionan.
- Proporcionar a los empleados medios para navegar seguros, cifrando las comunicaciones.
- Actualizar los sistemas de manera automatizada y centralizada.

Para más información en materia de Ciberseguridad visite INCIBE www.incibe.es, Protege tu Empresa https://www.incibe.es/protege-tu-empresa y OSI http://www.osi.es/.