Edición No. 4 – marzo 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

Ataques a las Conexiones

Los ataques a las conexiones inalámbricas **son muy comunes, y los ciberdelincuentes se sirven de diversos software y herramientas con las que saltarse las medidas de seguridad** e infectar o tomar control de nuestros dispositivos.

Generalmente, este tipo de ataques se utiliza para monitorizar y robar datos personales, bancarios, contraseñas, etc.

Redes trampa

Consiste en la creación de una red wifi gemela a otra legítima y segura, con un nombre igual o muy similar a la original, que crean utilizando software y hardware. Luego, la configuran con los mismos parámetros que la original, esperando que nos conectemos a esta.

¿Cómo se propaga o infecta? Este tipo de ataques suelen darse en lugares con una red **wifi pública**, con gran afluencia de usuarios. De modo que su red falsa pueda pasar desapercibida y engañe al mayor número de víctimas posible.

Spoofing

Consiste en el **empleo de técnicas de hacking de forma maliciosa para suplantar nuestra identidad, la de una web o una entidad.** Se basa en tres partes: el atacante, la víctima y el sistema o entidad virtual que va a ser falsificado..

IP Spoofing

El ciberdelincuente **consigue falsear su dirección IP y hacerla pasar por una dirección distinta**. De este modo, consigue saltarse las restricciones del router, y hacer llegar un paquete con malware.

Web Spoofing

Consiste en la **suplantación de una página web real por otra falsa.** La web falsa es una copia del diseño de la original, llegando incluso a utilizar una URL muy similar. El atacante trata de hacernos creer que la web falsa es la original.

¿Cómo se propaga o infecta? El atacante se sirve de otro tipo de ataques, como la ingeniería social o anuncios maliciosos, para intentar que accedamos al enlace de la web falsa pensando que se trata de la página web legítima.

Mail Spoofing

Consiste en suplantar la dirección de correo de una persona o entidad de confianza. También suele ser usado para enviar de forma masiva correos de Spam o cadenas de bulos u otros fraudes.

Edición No. 4 – marzo 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

¿Cómo se propaga o infecta? El atacante ha podido obtener el Email suplantado a partir de otro tipo de ataques, como la ingeniería social

Objetivo de ataques las conexiones:

Robar nuestros datos cuando accedamos a nuestra cuenta bancaria, redes sociales o correo electrónico, pensando que estamos llevando a cabo una conexión segura. Además, el ciberdelincuente puede llegar a tomar control sobre la navegación, accediendo a determinadas webs fraudulentas o muy similares a la original preparadas para el engaño o para la infección por malware.

Definiciones

Hacking: Conjunto de técnicas a través de las cuales se accede a un sistema informático vulnerando las medidas de seguridad establecidas originariamente.

Dirección IP: es un conjunto de números que identifica, de manera lógica y jerárquica un equipo en la red.

Router: dispositivo de hardware que permite la interconexión de ordenadores en red.

URL: (Uniform Resource Locator) dirección específica que se asigna a cada uno de los recursos disponibles en la red con la finalidad de que estos puedan ser localizados o identificados (páginas web, documentos, etc).

Fuente: INCIBE y la Oficina de Seguridad del Internauta (OSI).

Te invitamos a tomar las siguientes medidas preventivas:

- **NO abrir archivos adjuntos** ni abrir enlaces que provengan de correos de destinatarios desconocidos, que alerten sobre cobros jurídicos, demandas o similares y en caso de recibirlo, se debe reportar de inmediato al correo de Seguridad de tu institución o al área de informática, adjuntando el correo sospechoso.
- No descargue contenido multimedia por redes de intercambio tales como Ares.
- Apagar el equipo de cómputo cuando termine su jornada laboral, no solo previene que sea blanco de un ataque, sino que mejora el rendimiento, ahorra energía y previene el desgaste innecesario de este.
- Evitar ingresar a páginas de orígenes desconocidos.