proactive
Information security.

Ayudamos a Proteger sus Activos de Información

ProActive News Vol.5

Octubre 2017

VPNs & Redes Wi-Fi

VPNs

Virtual Private Network (VPN – Red Privada Vitual) es una tecnología que permite conectar computadoras o redes de computadoras de forma segura, ya sea sobre una plataforma de red pública (Internet) o un proveedor privado de servicios. Sus usos van desde asegurar las comunicaciones de redes privadas, conectar de forma segura trabajadores remotos o simplemente garantizar el anonimato en la navegación en Internet. Sobre este último punto es en lo que vamos a concentrarnos en este espacio informativo.

Uno podría llegar a contratar un proveedor VPN, (existen cientos en Internet) para asegurar el anonimato en la navegación o simplemente saltarse una validación de geo-localización de nuestra dirección IP para acceder a servicios bloqueados en algunos países, como la censura digital en China, por ejemplo.

Un caso acontecido en Massachussets-Estados Unidos estos días, en el cual un cyberstalker (ciberacosador) ha sido arrestado por el FBI saca a la luz el tema del anonimato en este tipo de conexiones.

Esta persona ha sido arrestada por acosar a su compañera de trabajo, utilizando conexiones VPN y servicios anónimos relacionados, para ocultar su identidad en la red, pero no tenía en cuenta que su proveedor de VPN guardaba información de su conexión real, con lo cual pudieron seguir su rastro, hasta dar con su arresto final.

Desde el punto de vista de la seguridad, la polémica va en que supuestamente estos proveedores de servicios o la mayoría de ellos, no guardan registros de sus usuarios, por lo que si estás pensando hacer algo malo, piénsalo dos veces.

Referencias:

- https://www.genbeta.com/seguridad/arrestan-a-un-acosador-que-usaba-una-vpn-para-ocultarse
- https://thehackernews.com/2017/10/no-logs-vpn-service-security_8.html

Redes Wi-Fi

Recientemente salió a la luz una vulnerabilidad que afecta al protocolo de conexión Wi-Fi utilizado actualmente WPA2/WPA (Personal & Enterprise), cuya denominación es KRACK (Key Reinstallation Attacks).

Como toda vulnerabilidad que se precie actualmente, posee logo y dominio propios ☺

Mediante esta nueva técnica, los impactos pueden ser bastante peligrosos, dado que se consigue modificar la comunicación segura e incluso se puede inyectar código para, por ejemplo, modificar el tráfico y descargar aplicaciones maliciosas en el cliente (como un troyano o ransomware).

Recomendación de seguridad: esperar a que se publiquen los parches de actualizaciones correspondientes y aplicarlos en nuestros sistemas ni bien estén disponibles. Otros tips de seguridad disponibles en el segundo enlace de referencia.

Referencias:

- https://www.krackattacks.com/
- https://www.linux.com/blog/2017/10/tips-secure-your-network-wake-krack
- http://www.seguridadpy.info/2017/10/krack-asi-es-como-han-conseguido-romper-wpa2/

Con objeto de mantenerlo actualizado y protegido, quedamos a vuestra disposición para asesorarlo en cuanto a la detección de vulnerabilidades en su plataforma que puedan ser explotadas.

Obtenga mayor información sobre nuestros servicios y productos, póngase en contacto con nosotros:

Web: www.proactive.consulting

Mail: contacto@proactive.consulting

Tel: +595 (981) 478-921

Twitter: @ProActive_py