



IT Consultores

Septiembre, 2010

10 Tecnologías que el cibercrimen goza en utilizar (La felicidad del Cibercrimen) (Documento condensado.)

Las nuevas tecnologías en teleinformática y acceso al Internet nos hacen la vida mas fácil... también se la hace mas fácil al Cibercrimen. **Dato:** Sabías que: En Latinoamérica, alrededor de 40 de cada 100 ejecutivos en IT reportaron haber sufrido un ataque a la seguridad informática en el 2007?... este dato para Brasil y México sube a 46 y 42% respectivamente. (Fuente: Keegan Research & Associates)

1. Conectividad de banda ancha.

Hoy en nuestro País es común que tanto a nivel residencial como corporativo contemos con un canal dedicado (always on). 512/1 mbps, etc.... Un sistema activo 24/7 significa que si somos objetivo del cibercrimen, este tendrá una ventana en el tiempo mucho mas amplia para intentar penetrar en nuestra red e incluso de tener éxito, podrá depositar mas rápidamente archivos con código malicioso.

2. Redes Inalámbricas (WIFI Networking)

.... Con el WIFI, muy convenientemente nos movemos en nuestros entornos sin dejar de contar con ese acceso tan apreciado que es Internet.... Sin embargo....también un cibercriminal, dentro del rango de cobertura de un AP, podrá sin duda interceptar y aprovechar nuestra señal irrumpiendo en nuestra red de área local.

3. Dispositivos removibles (Almacenamiento)

Con un dispositivo de estos fácilmente alguien puede sustraer información confidencial de cualquier empresa además que pueden transportar amenazas como virus y otros.

4. El Web o navegación en la web.

... Anteriormente la vulnerabilidad en la web era mínima sin embargo, hoy todos los sitios web hacen mucho más que publicar información estática y muchos corren o ejecutan programas como JavaScripts y código active-x para una mejor experiencia multimedia; Lo malo es que un Cibercriminal también es capaz de correr o ejecutar su propios programas con código malicioso ... en nuestras computadoras!!.

5. Email y Mensajería Instantanea (IM).

...el Email es altamente atractivo al cibercrimen ya que sirve de medio de transporte de cualquier tipo de amenaza sin dejar rastro del remitente. Correspondencia ilegal como pornografía, entrada de spam, robo de identidades y otros entran por este medio al igual que por el IM el cual ya cuenta con capacidad de descarga de archivos lo cual hace a nuestro sistema mas vulnerable al recibir código malicioso.

6. Comunicaciones unificadas (convergencia de Tecnologías)

... Con la VOIP ganando terreno y reemplazando el servicio telefónico tradicional, ya todas estas tecnologías pueden correr sobre la misma Red de Area Local.

Ahora bien, Eso significa que todas sus llamadas de voz, están sujetas a las mismas amenazas que afectan a los datos. Un paquete de VoIP puede ser interceptado y mas aún modificado en tránsito al igual que un paquete de datos..

7. Programas Peer to Peer (P2P)

... Su uso esta extendido en el compartir música y películas... El P2P es un medio de amplio uso por el cibercrimen pues con facilidad pueden desplegar malware con código malicioso... con el mínimo de riesgo para ellos pues por lo general estas redes favorecen el anonimato de sus usuarios.

8. Comercio Electrónico y banca en línea (E-Commerce & Bank online)

... Es conveniente comprar lo que necesitamos en casa sin salir de ella y recogerlo en nuestra puerta; pagar cuentas y transferir dinero entre cuentas sin ir al banco... el cibercrimen sin duda adora esta tendencia... Ellos pueden interceptar información que circula en la red, romper una base de datos... o, mas aún, publicar un sitio falso de e-comercio en sustitución de uno legal (Previo lo han bloqueado), al cual uno accesa confiado, procediendo a realizar transacciones mediante tarjeta de crédito, transferencias u otro medio <sin saber que NO es el sitio original>.

9. Computación Móvil

Los sistemas informáticos se vuelven cada día mas móviles; Los dispositivos, desde una PDA o Cell/Smartphone... se están usando cada vez mas para guardar y transportar datos de importancia y poder conectarnos... Pero, por su “movilidad” estos equipo fácilmente se nos pueden perder o ser robados... Usted estará poniendo incluso a esos clientes en riesgo y hasta ser sujeto de requerimientos legales.

10. Conectividad Universal.

...no solo estamos poniendo “en línea” nuestras computadoras, nuestras centrales telefónicas; estamos conectando <todo>... exponamos un caso: muchos de nosotros tenemos o pensamos instalar cámaras de vigilancia remota (IP), así podemos monitorear una o mas áreas vía Internet desde cualquier parte del mundo... esto es excelente!! pero para el Cibercrimen también...!! De hecho podemos estar abriendo avenidas o rutas mediante las cuales el cibercriminal puede observar lo que sucede en nuestras casas o empresas sin poner un pié adentro.

En Conclusión: ... Debemos borrar toda presencia en la web, desconectarnos de Internet y encerrarnos en la empresa o en casa?? NO!! Hoy en día funcionar sin la ventaja de la tecnología es impensable; lo importante es tal, como lo hacemos en nuestro medio o vida real, **invertir en seguridad; establecer reglas o políticas correctas y ser proactivo** ante estas amenazas que hoy en día <no> vigilan la puerta de entrada de la empresa o la casa, **sino una entrada mucho mas pequeña, posiblemente del grosor de un alfiler que es su puerto de conexión a Internet donde entra y sale su información.**

Dato: ...Sabías que: Las empresas en Centro América no tienen un sistema de seguridad informática confiable?...más aún... en muchos casos NO TIENEN NINGUNO?? En nuestro País, exceptuando las grandes empresas por lo general transnacionales, la inversión en seguridad informática (IT) es mínima y hasta nula?.. y encima de ello, la poca que hay es manejada de manera poco formal?? (Fuente: ITNow)



Para mas información no dude en consultarnos.

La Seguridad no es solo un proceso tecnológico.... es un proceso organizacional!