

} Aparentemente, todo es seguro |

Autor: Yago Cruz (Director Comercial de G2 Security)

Internet es una de las vías más importantes para una empresa de publicar información y si no se tiene cuidado a la hora de configurar y manejar una Web Site pública, se deja la organización a merced de serios problemas de seguridad, ¿Le gustaría verse en la situación de que unos intrusos hayan modificado el aspecto de su página, dañando su imagen y reputación? No es tan difícil que ocurra esto, a la página de mayor referencia en Internet para la seguridad, www.securityfocus.com, le cambiaron uno de sus banners de publicidad por la imagen de un conejito que decía "¿y vosotros decís que sabéis? No tenéis ni IDEA.

Por supuesto esto sería un mal menor, pues si se ha accedido al servidor web, a partir de ahí los hackers tienen la posibilidad (y muchos de ellos lo toman como obligación) de entrar aún más allá, a la red interna, donde el nuevo objetivo es robar claves, datos confidenciales, hacer pedidos, falsificar documentos... y añada el etcétera que más miedo le de.

Pero no todo es tan malo, si se preocupa por la seguridad y toma las medidas necesarias, nada tiene por qué ocurrir, al igual que cierra la puerta de su casa con llave al salir, simplemente utilice la llave que le brinda la tecnología y los expertos para cerrar su red a intrusos.

Debe elegir un servidor y/o host con la tecnología y la plataforma adecuada, aunque haya a veces que sacrificar un poco de facilidad de uso por ganar en seguridad. Se debe realizar la correcta configuración, y no solo cuando se instala, se debe estar pendiente a cualquier actualización del software o cualquier cambio en la política de seguridad de la empresa, pues por supuesto, se debe haber diseñado una y seguirla a rajatabla. Como en todas las áreas, la disciplina es una buena conducta para llevar toda empresa a un buen fin.

El servidor, debe estar adecuadamente aislado de la red interna de su organización, o estaría poniendo una ventana de cristal a su caja fuerte, y por supuesto, de nada le sirve una cámara oculta (los logs del sistema) si cuando llega por la mañana ni siquiera mira las cintas grabadas.

Los requerimientos básicos de seguridad para su negocio, entre los ya mencionados incluyen también:

- } Información sobre las vulnerabilidades y parches disponibles. Es extremadamente importante estar al día de los nuevos parches y versiones de programas.
- } Restringir las actividades administrativas. ¿De qué vale una clave de dominio público en su empresa? El conocimiento de las claves no puede estar supeditado a la comodidad, y, el 90% de las veces a no ser que se usen otros dispositivos (DIGIPASS, smartcards), TODA la información sensible que posea depende de algunas letras.

Pero esto no es todo ni mucho menos, se debe hacer todo un plan de seguridad de acuerdo a sus necesidades, evaluarlas, examinarlas, estudiarlas e implementarlas en la medida de lo posible. Existe una palabra devaluada en el uso cotidiano pero extremadamente útil en el mundo de la seguridad informática. Sólo a los realmente buenos se les puede calificar de "paranoicos". Ser un paranoico en la seguridad informática significa evaluar

}Aparentemente, todo es seguro|

todas las posibilidades, pensar como lo haría el atacante e incluso ir más allá, imaginando situaciones que por muy absurdas que sean, pudiesen llegar a ocurrir.

La seguridad, al fin y al cabo, y cuando un atacante se enfrenta a un sistema, se convierte en un juego, donde la imaginación es una potente arma, y el mejor de los hackers es el que más imaginación maneja, manipulando y combinando las herramientas que posee, yendo más allá de lo que nadie espera, y por supuesto, dedicándole más tiempo del que cualquiera esperaría emplear en muchos asuntos, simplemente por suponer un reto.

A la hora de montar su servidor, piense que lo más importante de su empresa es la información que posee en su disco y el tiempo que ha perdido en conseguirla más el tiempo que puede perder si se destruye. Piense que en cualquier tienda, por pequeña que sea, existen sistemas de alarma y posiblemente contraten a un guarda durante la noche. ¿No merece su información la misma vigilancia?