Asegurar las tecnologías: Hardening

En general, si examinamos cómo operan las tecnologías que usamos a diario, podemos notar que muchas han sido diseñadas teniendo en cuenta la experiencia del usuario; con el propósito de crear soluciones que sean fáciles de usar, prácticas e intuitivas. Es comprensible que estas se centren en la funcionalidad, ya que se busca llegar al mayor número de usuarios posible, y esto se logra, en parte, con un producto/servicio fácil de utilizar. Sin embargo, dado que no todos tienen la destreza para utilizar un sistema o dispositivo, "si no se le brinda apoyo en ese aspecto, es poco probable que el producto desarrollado tenga éxito. Sin embargo, al mismo tiempo, cuando el enfoque principal recae en la funcionalidad, suele descuidarse la seguridad. Esto sucede porque en la mayoría de los casos, al implementar medidas para proteger una tecnología, se tiende a complicar una tarea que anteriormente se realizaba de manera más sencilla.

Veamos un ejemplo:

Cuando una persona adquiere un teléfono móvil, este no le obliga a utilizar un mecanismo de autenticación para acceder. Es el usuario quien, opcionalmente, debe configurar un patrón, una contraseña, un PIN o algún dato biométrico. Como se puede observar, se prioriza la funcionalidad sobre la seguridad. A pesar de saber que como usuarios tendremos mucha información confidencial almacenada en el dispositivo, y si no tiene una clave, al menos, cualquiera que tenga dicho dispositivo en sus manos podría ver los datos allí almacenados.

El proceso de Hardening

Es fundamental considerar que todo dispositivo o software que vayamos a utilizar debe estar sujeto a un proceso de endurecimiento para modificar la configuración de fábrica o por defecto hacia una orientación orientada a la seguridad que permita protegerse de cambios inesperados o posibles ataques.

Ahora bien, ¿cómo podemos saber qué cambios deberíamos implementar en la configuración para asegurar el dispositivo o software que vamos a utilizar? Para llevar a cabo un proceso de endurecimiento, podemos basarnos en las guías desarrolladas por el mismo fabricante, por organismos de seguridad reconocidos o por expertos en materia de seguridad. Estas guías explican cuál es la forma más segura de configuración a aplicar, pero es importante entender que a veces estos cambios pueden ser tan radicales que podrían hacer que el uso no sea

sencillo. Recordemos que la seguridad, a veces, complica un proceso. Si aplicamos demasiada seguridad, es posible que descuidemos la facilidad. Por lo tanto, tomaremos esas guías como referencia, pensando en equilibrar seguridad y funcionalidad.

¿Qué guías podemos utilizar?

Entre las recomendables, encontramos las guías de endurecimiento desarrolladas por el CIS - Center of Internet Security. Este organismo desarrolla buenas prácticas de seguridad, controles y herramientas para que cualquiera las pueda utilizar.
Existen guías de endurecimiento denominadas CIS Benchmarks para servidores, servicios en la nube, equipos de escritorio, dispositivos móviles, impresoras, equipos de red, etc. Están en inglés pero tienen una lectura fácil: CIS Benchmarks.
Por otro lado, están las guías del organismo español CCN CERT, que también desarrolla buenas prácticas y herramientas para que el público las utilice. Están en español y abarcan una gran variedad de plataformas y productos: CCN CERT.

Consideraciones al llevar a cabo un hardening

Si vamos a realizar modificaciones en la configuración de uno o más equipos, siempre debemos recordar probar estos cambios primero en un entorno de pruebas para verificar cómo responde el dispositivo o el software en cuestión. Nunca debemos aplicar cambios directamente en el entorno de producción, ya que podríamos afectar el funcionamiento y esto podría acarrear problemas de los que no tenemos dimensión.
De la misma manera que mencionamos que para aplicar parches de actualización es necesario realizar primero una prueba en un entorno de pruebas para controlar su respuesta, estos cambios de configuración de seguridad que realizaremos también deberían pasar inicialmente por una prueba. Si no se presentan conflictos, podemos estar seguros de implementarlos en producción.