educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 2

educación IT
CODE YOUR FUTURE

Hardening: Asegurar las tecnologías

Asegurar las tecnologías: *Hardening*

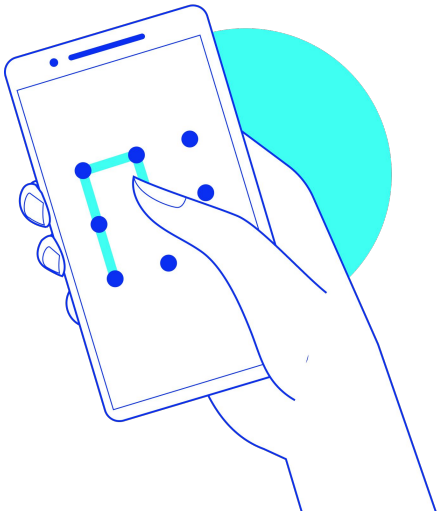
Por lo general, si analizamos cómo funcionan las tecnologías que utilizamos a diario, podremos notar que muchas de ellas han sido diseñadas teniendo en cuenta la ***experiencia del usuario***; con el objetivo de crear soluciones que sean intuitivas, de fácil uso y prácticas. Es razonable que estas tengan el foco puesto en la **funcionalidad**, ya que se pretende alcanzar a la mayor cantidad de usuarios posibles, y eso se logra, en parte, con un producto/servicio fácil de usar.

Ahora bien, dado que no todo el mundo tiene la facilidad para utilizar un sistema o un dispositivo, si no se le ayuda en ese sentido, difícilmente el producto que se desarrolló, tendrá éxito. Sin embargo, al mismo tiempo, **cuando lo que se ha creado tiene el centro de atención en la funcionalidad, se suele dejar de lado la seguridad**. Esto es así, ya que en la gran mayoría de los casos, al incorporar medidas para proteger una tecnología, **se suele complejizar una tarea que antes se hacía de forma más sencilla**.

Veámoslo con un ejemplo:

Cuando una persona compra un celular, éste no lo obliga a utilizar un mecanismo de autenticación para acceder. **Es el usuario quien debe, a elección, configurar un patrón, una contraseña, un pin o algún dato biométrico**. Como se ve, **se pone por delante la funcionalidad a la seguridad**.

Pese a saber que como usuarios, tendremos mucha información confidencial almacenada en el aparato y si no tiene una clave, al menos, cualquiera que tenga ese dispositivo en sus manos podría ver los datos allí almacenados.



Veamos otros ejemplos: comparemos una tecnología desarrollada pensando en la funcionalidad y otra en la seguridad.

WhatsApp - Funcionalidad

Esta aplicación de mensajería es muy sencilla de utilizar, es intuitiva y no tiene publicidad, lo que todo usuario quiere. Podríamos decir, entonces, que fue desarrollada teniendo en cuenta la **funcionalidad** y al día de hoy sigue siendo la número uno a nivel mundial.

No obstante, durante varios años WhatsApp **tuvo una grave falla de seguridad**, porque los **mensajes intercambiados con otros dispositivos no se realizaban de forma *cifrada***, esto implicaba un gran riesgo, ya que estos podían ser interceptados y leídos sin problemas.

Seguramente, las personas no estaban cómodas con la idea de que sus mensajes podían ser vistos por terceros. Luego de unos años **este problema fue resuelto porque se implementó el *cifrado punto a punto***.

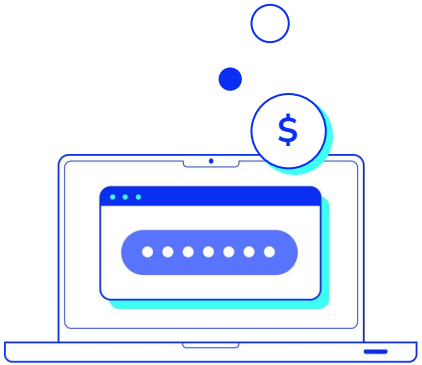
Homebanking - Seguridad

Los sistemas bancarios siempre han puesto la **seguridad sobre la funcionalidad**.

Por ejemplo, podemos nombrar que piden cambio de contraseña cada cierto tiempo, no es posible usar las últimas claves utilizadas, si se ingresa mal más de tres veces las credenciales se bloquea el usuario y solicita ir a un ATM para desbloquear, lo que requiere contar con la tarjeta y el PIN para ingresar a la terminal para sacar un nuevo usuario y clave.

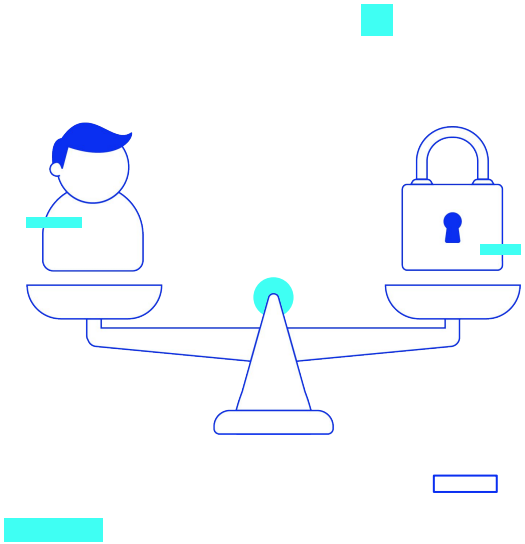
Adicionalmente, ahora se ha implementado el ***segundo factor de autenticación*** (***2FA***), que como vimos, es un mecanismo de autenticación adicional a la hora de realizar ciertas operaciones que revisten importancia como transferencias, cargas de CBU, etc.

Si analizamos su **funcionamiento desde el punto de vista del usuario**, notaremos que **no es cómodo** cambiar claves, tener que usar *2FA* o ir a un ATM a desbloquear un usuario, **pero son medidas necesarias con el objetivo de evitar que surjan problemas o delitos informáticos**.



Por suerte hoy se está buscando mezclar ambos mundos para **crear tecnologías funcionales y seguras**, lo que convierte en un escenario mucho más favorable para los usuarios al contar con sistemas o dispositivos que integran lo mejor de los dos mundos y no uno solo.

De todas formas, no todo es color de rosa, ya que siempre debemos tener presente que al momento de adquirir o utilizar un software o dispositivo, tenemos que revisar las configuraciones de seguridad que tiene y considerar que si no cambiamos la que viene por defecto, es probable que esa tecnología sea vulnerable. **Al proceso de asegurar una tecnología se le denomina *Hardening***.



El proceso de *Hardening*

Como se mencionó antes, es necesario contemplar que todo dispositivo o software que vayamos a usar tiene que ser sujeto a un **proceso de *hardening*** para modificar la configuración de fábrica o por defecto que trae, hacia una orientada a la seguridad que permita proteger de cambios no esperados o de posibles ataques.

Ahora bien, ¿cómo podemos saber qué cambios deberíamos implementar en la configuración, para asegurar ese dispositivo o software que vamos a utilizar? Para llevar a cabo un proceso de hardening, podemos apoyarnos en las guías desarrolladas por el mismo fabricante, por organismos de seguridad reconocidos o por expertos en materia de seguridad. En esas **guías** se explica cuál es la forma más segura de configuración a aplicar, pero es necesario entender que a veces estos cambios pueden ser tan radicales que podría generar que el uso no sea sencillo. Recordemos que **la seguridad, a veces, complejiza un proceso.** Si aplicamos mucha seguridad es factible que dejemos de lado la facilidad. Así que tomaremos esas guías como referencia, **pensando en equilibrar seguridad y funcionalidad**.

¿Qué guías podemos utilizar?

Entre las recomendables, encontramos **las guías de *hardening*** 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 hardening denominadas ***CIS Bechmarks*** para servidores, servicios *cloud*, *desktops*, 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 castellano y tienen para una gran variedad de plataformas y productos: CNN CERT.

CIS Center for Internet Security®

CCN-CERT centro criptológico nacional

Consideraciones al llevar a cabo un *Hardening*

Si vamos a realizar cambios en la configuración de uno o más equipos, siempre tenemos que tener presente **probar estos cambios primero en un ambiente de pruebas** para verificar cómo responde el dispositivo o el software en cuestión. **Nunca tenemos que aplicar cambios directamente en el ambiente de producción** porque podríamos afectar el funcionamiento y esto traería consigo problemas que no tenemos dimensión.

De la misma manera que mencionamos que para aplicar parches de actualización primero se haga en un ambiente de prueba para controlar su respuesta, estos cambios de configuración de seguridad que realizaremos también deberían **pasar de forma inicial por una prueba**. Si no se presentan conflictos, podemos estar seguros de implementarlos en producción.

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!