VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Noviembre 2012

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- El problema
- La solución
- El ejemplo

Autenticación de dos factores

EDITOR INVITADO

El editor invitado para esta edición es Fred Kerby, ex director de Seguridad de la Información en el Naval Surface Warfare Center, (Centro de Guerra Naval) en la división Dahlgren. Además, es Instructor Senior en el SANS Institute e imparte los cursos de Introducción a la Seguridad de la Información (SEC301), Liderazgo en Seguridad de la Información (MGT512) y Fundamentos de Seguridad (SEC401).

EL PROBLEMA

Hoy en día, el uso de muchos de los servicios en Internet tales como envío de correo electrónico, banca en línea o compras a través de Internet, requiere demostrar primero que somos quien decimos ser. A este proceso de probar nuestra identidad se le conoce como autenticación. La autenticación se realiza mediante el uso de algo que conoces (como tu contraseña), algo que tienes (como tu teléfono inteligente), o alguna característica única de ti (como un escáner de retina o un lector de huellas dactilares). Tradicionalmente una de las formas más comunes de autenticación se lleva a cabo haciendo uso de un usuario y una contraseña. El problema de utilizar solo una contraseña para realizar la autenticación es simple: todo lo que necesita un atacante es adivinar o poner en peligro tu contraseña y obtener acceso instantáneo a tu cuenta e información en línea. Si utilizas el mismo nombre de usuario y contraseña para varias cuentas el daño puede ser aún mayor. Para proteger mejor tus cuentas en línea, los sitios web están utilizando métodos de autenticación más robustos que requieren el uso de más de un factor de autenticación. A continuación, se explica que es este método, como funciona y por qué debemos usarlo.

LA SOLUCIÓN

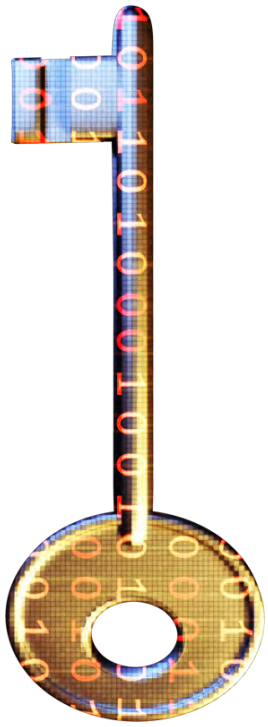
El proceso de autenticación robusto utiliza más de un factor; no basta conocer tu contraseña, además es necesario tener algo (como un teléfono inteligente) o algo que te caracterice (como tu huella digital). La autenticación de dos factores, tal como su nombre lo indica, utiliza dos factores para comprobar tu identidad en lugar de uno solo. Un ejemplo común de una autenticación de dos factores es el proceso empleado para usar tu tarjeta de cajero automático. Para hacer uso del cajero automático es necesario tener algo como (tu tarjeta), pero además necesitas saber algo (tu PIN). Si un atacante roba tu tarjeta, de nada le servirá a menos que conozca tu PIN (es por esta razón que no se

Autenticación de dos factores

recomienda escribir el PIN en la tarjeta). Al requerir dos factores de autenticación te encontrarás más protegido que si solo usaras uno de ellos. Los dos factores de autenticación trabajan en línea de una manera similar a la combinación entre tu tarjeta de cajero automático y el PIN. Utiliza tu nombre de usuario y contraseña cuando quieras ingresar a tu cuenta en línea. Sin embargo, después de introducir correctamente la contraseña, en lugar de ingresar a tus cuentas el sitio requerirá un segundo factor de autenticación, como un código de verificación o tu huella dactilar. Si no tienes el segundo factor, entonces no tendrás acceso a tu cuenta. Este segundo paso te protege. Si un atacante ha comprometido tu contraseña, tú y tu cuenta están a salvo ya que el atacante no puede completar el segundo paso sin tener el segundo factor.

EJEMPLOS

Veamos un ejemplo de cómo la autenticación de dos factores funciona. Uno de los servicios más utilizados en línea es Gmail. Muchas personas se autentican a su cuenta de Gmail u otros servicios de Google con su nombre de usuario y contraseña. Ahora, Google ofrece una mayor seguridad con la autenticación de dos factores o lo que Google denomina "verificación de dos pasos". El proceso de verificación de dos pasos que emplea Google requiere de dos elementos para la autenticación: tu contraseña (algo que conoces) y tu teléfono inteligente (algo que tienes). Para corroborar que tienes tu teléfono inteligente, Google te enviará vía SMS un código de verificación único (toma en cuenta que se pueden aplicar gastos de mensajería, revisa tu plan de servicios para obtener más información).



Utiliza autenticación de dos factores siempre que sea posible, es una de las maneras más robustas de proteger el acceso a tus cuentas e información

Posteriormente tendrás que ingresar el código, si lo prefieres, en lugar de que Google te envié el código de seguridad a través de un SMS, puedes instalar una aplicación para que te genere el código. De esta manera no necesitas hacer uso de tu proveedor de servicios, solo de tu teléfono inteligente. Este proceso de autenticación es tan fuerte que incluso si un atacante ha comprometido tu contraseña de Google, no podrá acceder a tus cuentas de Google a menos que también tenga acceso físico a tu teléfono inteligente. Tú y tu valiosa información están protegidos.

Autenticación de dos factores

Toma en cuenta, que estos códigos de verificación enviados a tu teléfono inteligente son únicos; son diferentes cada vez que te autenticas. Como tal, tendrás que pasar por este proceso de dos pasos cada vez que tengas que autenticarte en tu cuenta de Google. Es importante mencionar que esta función no está habilitada de forma predeterminada. Para activar esta función, ingresa a tu cuenta de Google, entra a configuración de la cuenta, selecciona seguridad y sigue las opciones para la verificación de autenticación de dos pasos.

Otros sitios en línea también ofrecen autenticación de dos factores, tales como Dropbox, PayPal o incluso tu banco. Algunos de estos servicios pueden ser compatibles con tu teléfono inteligente, mientras que otros, como PayPal, pueden enviar una señal especial para la generación de códigos de verificación únicos. Otros sitios pueden utilizar dispositivos especiales que se conectan al puerto USB de tu computadora, como Yubikey. Si alguno de los servicios que usas te ofrece la autenticación de dos factores, es muy recomendable activarla y utilizarla.

RECURSOS

Algunos de los enlaces mostrados se han acortado para mejorar la legibilidad a través del servicio TinyURL. Para mitigar los problemas de seguridad, OUCH! siempre utiliza estas características de vista previa de TinyURL, que muestra el enlace destino, solicitando permisos antes de abrirlo.

Google Two-Step Verification
http://preview.tinyurl.com/ajdf7a3

PayPal (and EBay) Security Key
http://preview.tinyurl.com/838dpds

Facebook
http://preview.tinyurl.com/amm2cjm

Common Security Terms
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day
http://preview.tinyurl.com/6s2wrkp

Consejo del día de UNAM-CERT
http://www.seguridad.unam.mx/usuario-casero/consejos/

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti.
Visítanos en http://www.securingthehuman.org

VERSIÓN EN ESPAÑOL

UNAM-CERT, Equipo de Respuesta a Incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.

Sitio web http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: Abraham Cueto, Carlos Colio, Célica Martínez, Jazmín López