Práctica de laboratorio: explorando el mundo de los profesionales en el área de ciberseguridad

Objetivos

Explorar las características de seguridad que utilizan las organizaciones como Google y Cisco para mantener los datos a salvo.

Parte 1: cómo proteger sus datos

Parte 2: cómo mejorar la seguridad en las cuentas de Google

Aspectos básicos/situación

En este capítulo se presenta el mundo cibernético a los estudiantes. Este mundo cibernético está lleno de áreas de datos que manejan cantidades inimaginables de información personal y de la organización. Como profesionales de la ciberseguridad, es importante comprender los tipos de mecanismos de ciberseguridad que una organización debe implementar para proteger los datos que almacenan, administran y protegen. En esta práctica de laboratorio, explorará una de las organizaciones de manejo de datos más grandes del mundo, Google. Verá dos videos y luego responderá una serie de preguntas. Cada video presenta un aspecto diferente de la defensa de ciberseguridad en Google. Al finalizar, tendrán una mejor comprensión de las medidas de seguridad y los servicios que las organizaciones como Google adoptan para proteger la información y los sistemas de información.

Videos:

Cómo Google protege sus datos

Clave de seguridad

Recursos necesarios

- Equipo de escritorio o dispositivo móvil con acceso a Internet

Parte 1: Protección de sus datos

Como uno de los depósitos de datos personales más grandes del mundo, Google almacena cantidades masivas de datos. Google representa alrededor del 50 % de toda la actividad de búsqueda en Internet. Para complicar aún más las cosas, Google posee y opera YouTube, el sistema operativo Android y muchas otra fuentes importantes de recopilación de datos. En esta actividad, verá un breve video e intentará identificar varias de las medidas que toman los profesionales de la ciberseguridad en Google para proteger sus datos.

Paso 1: Abra un navegador y vea el siguiente video:

Cómo Google protege sus datos

a. ¿Cómo garantiza Google que los servidores que instalan en sus centros de datos no estén infectados con malware por los fabricantes de equipos?

b. ¿Cómo se protege Google del acceso físico a los servidores ubicados en los centros de datos de Google?

c. ¿Cómo protege Google los datos de clientes en un sistema de servidor?

Paso 2: Identifique las vulnerabilidades de los datos.

a. Como podrá ver en el video, los datos de los centros de datos de Google están bien protegidos; sin embargo, al usar Google, no todos sus datos se encuentran en el centro de datos de Google. ¿En qué otro lugar puede encontrar sus datos al utilizar el motor de búsqueda de Google?

b. ¿Puede tomar medidas para proteger los datos al utilizar el motor de búsqueda de Google? ¿Cuáles son algunas de las medidas que puede usar para proteger sus datos?

Parte 2: Mejora de la seguridad en las cuentas de Google

La mayor amenaza al utilizar servicios en línea como Google es proteger la información de la cuenta personal (nombre de usuario y contraseña). Como agravante, estas cuentas se comparten y utilizan comúnmente para autenticarle a otros servicios en línea, como Facebook, Amazon o LinkedIn. Cuenta con varias opciones para mejorar el manejo de sus credenciales de inicio de sesión de Google. Estas medidas incluyen crear una verificación de dos etapas o un código de acceso con su nombre de usuario y contraseña. Google también admite el uso de claves de seguridad. En esta actividad, verá un video corto e intentará identificar las medidas que se pueden tomar para proteger sus credenciales al utilizar las cuentas en línea.

Paso 1: Abra un navegador y vea el siguiente video:

La clave para trabajar de manera más inteligente, rápida y segura

a. ¿Qué es la verificación de dos etapas? ¿Cómo puede proteger esta su cuenta de Google?

b. ¿Qué es una clave de seguridad y qué hace? ¿Puede utilizar la clave de seguridad en varios sistemas?

c. Haga clic aquí si tiene preguntas comunes sobre la clave de seguridad. Si configura su cuenta para utilizar una clave de seguridad, ¿aún se puede ingresar sin tener una clave física?

Paso 2: Protección del acceso a la cuenta de Gmail.

a. Se ha vuelto muy popular el uso de una cuenta de Gmail. Actualmente, Google tiene más de 1 mil millones de cuentas activas de Gmail. Una de las características convenientes de las cuentas de Gmail es la capacidad para otorgar acceso a otros usuarios. Esta característica de acceso compartido crea una cuenta de correo electrónico compartida. Los piratas informáticos pueden utilizar esta característica para acceder a su cuenta de Gmail. Para controlar la cuenta, inicie sesión en su cuenta de Gmail y haga clic en el icono de engranaje en la esquina superior derecha (Configuraciones). Cuando la pantalla de configuración se abre, se muestra una barra de menú debajo del título de la pantalla Configuración. (General – Etiquetas – Recibidos – Cuentas e importación – Filtros y direcciones bloqueadas...)

b. Haga clic en el elemento del menú **Cuentas e importación**. Marque la opción **Otorgar acceso a su cuenta**. Elimine los usuarios compartidos no autorizados de su cuenta.

Paso 3: Verifique su actividad en la cuenta de Gmail.

a. Los usuarios de Gmail también pueden verificar la actividad de la cuenta para asegurarse de que ningún otro usuario haya accedido a su cuenta personal de Gmail. Esta característica puede identificar quién accedió a la cuenta y desde qué ubicaciones. Utilice la opción **Última actividad de la cuenta** para determinar si alguien más accedió a su cuenta. Para acceder a la **Última actividad de la cuenta** siga estos pasos:

   1) Inicie sesión en la cuenta de Gmail.

   2) Seleccione **Última actividad de la cuenta:** que se encuentra en la parte inferior de la página. Mostrará la última vez que el usuario no autorizado ingresó a la cuenta y desde dónde.

   3) Debajo de este mensaje encontrará un hipervínculo de detalles. Haga clic en el hipervínculo de detalles.

b. Vea la actividad de la cuenta. Si encuentra un usuario no autorizado, puede desconectar el usuario no autorizado haciendo clic en el botón de la parte superior izquierda, en la opción **Cerrar todas las demás sesiones web**. Ahora cambie su contraseña para evitar que el usuario no autorizado acceda a la cuenta.

