Formación sobre ciberseguridad

Creado por https://security-companion.net/

Versión 1.6

Acerca de esta formación

- Publicado bajo licencia de código abierto (Creative Commons Zero v1.0 Universal)
  -> La formación es de libre acceso
  -> se permite el uso, los cambios y la duplicación
- La versión actual se puede descargar aquí

Visión de conjunto

- Motivación
- Ingeniería social
- Seguridad en Internet
- Correo electrónico
- Contraseñas
- Autenticación de dos factores
- Copias de seguridad
- Información general

Motivación

- Los ataques de hackers (por ejemplo, ransomware) hacia empresas y organizaciones han aumentado considerablemente en los últimos tiempos
- Todas las medidas técnicas son inútiles si las personas que las manejan se saltan las medidas de seguridad consciente o inconscientemente
- En muchas ocaciones los empleados de una organización son el punto más débil de la cadena
- Esta presentación quiere equipar a los empleados para el futuro y aumentar la conciencia sobre la ciberseguridad

Datos que valen la pena proteger

- Direcciones de contactos externos o internos
- Datos de cuentas bancarias
- Nombres de usuario/contraseñas
- Informes financieros
- Hardware y software utilizado en la organización

- Número de la seguridad social
- Fecha de nacimiento, lugar de nacimiento, nombre de la madre (a menudo se utilizan como autentificadores para recuperar una contraseña)
- Direcciones de correo electrónico (a menudo se utilizan para la autenticación, por ejemplo, en las redes de la empresa)
- etc.

Ingeniería social

- Definición: Métodos que los atacantes utilizan para obtener confianza y así recibir información sensible de los empleados/usuarios, a menudo utilizando presión y tratando de provocar la simpatía (Phishing)
- Especialmente los recepcionistas deben tener cuidado al recibir llamadas o recibir a un supuesto "técnico de reparación de impresoras" en el campus

- Ejemplos:
  - si no se realiza inmediatamente una transferencia bancaria ordenada por el supuesto jefe, se amenaza con elevados costes de recordatorio
  - un atacante se hace pasar por un nuevo colega y pide durante una llamada telefónica con un empleado que le pase contraseñas
  - un atacante manda un correo electrónico pidiendo al recipiente de contactar urgentemente al contacto técnico de una compañía. Pero el teléfono proporcionado en el correo no es el de la compañía sino uno que es controlado por el atacante (Callback Phishing)

- Ejemplos:
  - Los atacantes se hacen pasar por el servicio técnico, por ejemplo de Microsoft, y afirman que necesitan resolver un problema en un ordenador
  - el atacante se hace pasar por un nieto y afirma tener una necesidad (económica)

Seguridad en Internet

- Los navegadores y programas de correo electrónico están directamente expuestos al Internet
  -> mantenerlos siempre actualizados para estar lo mejor protegido posible contra nuevos ataques
- Antes de hacer clic en un enlace de correo electrónico, aplicación de chat, SMS, etc., comprueba siempre lo siguiente

- ¿Esperaba este enlace?
  - Enlace de un servicio de entrega de paquetes aunque no se espera ningún paquete
  - Enlace de un banco, pero no tiene ninguna cuenta en ese banco

- ¿Conozco la URL (= dirección del enlace)?
- ¿Es mala la traducción de la página o del correo electrónico? ¿Las imágenes son de mala calidad?
- ¿Realmente no hay ninguna letra cambiada en la URL? https://amazon.com y https://amaz0n.com son completamente diferentes
- ¿Estoy en el sitio oficial o pertenece la última parte del dominio a otro país? .ru, .uk, .cn, etc.?
  - Ejemplo: https://company.com.uk o https://company.de en lugar de https://company.com
  - Ejemplo: https://facebk.com en lugar de https://facebook.com

- Antes de hacer clic en un enlace, señálelo con el ratón (en las tabletas haga una pulsación larga sobre él) y compruebe en la barra de estado que es correcto
  - ¿Es visible una dirección IP (93.235.136.159) en lugar de una URL?
- Comprueba los enlaces acortados con servicios como https://urlex.org/ o https://unshorten.me/ (muestran el enlace completo)

- Al visitar páginas desconocidas, compruébalas críticamente y, en caso de duda, cancele la visita
- ¿Tiene el diseño un aspecto extraño o falta por completo?
- Con https://virustotal.com es posible revisar y comprobar la falta de virus de sitios webs cuestionables(y archivos adjuntos inesperados de los correos electrónicos)
- Es más seguro introducir la dirección de un sitio web directamente en el navegador en lugar de hacer clic en el enlace de un correo electrónico

- Cuando utiliza plataformas de venta, sólo comuníquese con otros usuarios a través de la aplicación de contacto oficial de la plataforma
  - Si un comprador potencial se pone en contacto consigo a través de messenger, sea precavido
  - No permitas que otros lo presionen, sino que cancele el contacto en caso de duda

- Al recibir un correo electrónico con un archivo adjunto sospechoso de un amigo/colega, llamar al remitente antes de abrir el archivo adjunto para comprobar si el correo es legítimo
- Buscar el candado en la barra del navegador 
  - Atención: El candado sólo significa que la conexión entre el navegador y el cliente está cifrada
  - Un candado no significa automáticamente que el sitio sea seguro o que no sea operado por un atacante

- No instalar un software que se anuncia en una ventana emergente del navegador
- No iniciar sesión en cuentas de correo electrónico o banca en línea en ordenadores públicos (hotel, biblioteca, etc.) ya que atacantes pueden ver y analizar posiblemente sus datos
- No activar macros en Microsoft Word, Excel, etc. con archivos adjuntos sospechosos

Correo electrónico

- Muchos programas de correo electrónico sólo muestran el nombre del remitente, pero no la dirección de correo electrónico completa
- Correos electrónicos falsos: Los atacantes hacen que un correo electrónico parezca válido aunque sea falso/estafa
- Verificar el dominio: sólo service@paypal.com es válido, servicioalconsomidorpaypal@gmail.com no
  - Tener en cuenta que la segunda dirección de correo electrónico no es filtrada por los servidores de correo y los filtros de spam y, por lo tanto a los atacantes les gusta usar correos de este tipo

- No utilizar la misma cuenta de correo electrónico para todas sus actividades en línea, separe la del trabajo de la personal
- Utilizar una cuenta separada cuando compres en línea
  - Muchos vendedores añaden automáticamente a los compradores a sus listas de correo, por lo que la cuenta recibirá muchos correos con el tiempo
  - Si la cuenta recibe demasiado spam, se puede cerrar y crear una nueva
    -> La cuenta personal se mantiene limpia de correos no deseados

Contraseñas

- Los atacantes tienen largas listas de contraseñas con millones de contraseñas a su disposición. Las prueban en las páginas de inicio de sesión hasta que tienen éxito
- Ejemplos de malas contraseñas:
  - C0ntr@seña
  - verano2021
  - secreto1
  - abc123

- Requisitos mínimos para las contraseñas:
  - Evitar el Leetspeak (sustitución de caracteres por símbolos y números de aspecto similar, por ejemplo, @ por "a" o 3 por "e")
  - Utilizar al menos 12 caracteres con una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
  - Cuanto más larga sea la contraseña, más difícil será descifrarla.
  - No reutilizar las contraseñas
  - Tener en cuenta que las contraseñas que son fáciles de recordar para usted también son fáciles de adivinar por un atacante

- Evitar las siguientes palabras en las contraseñas, ya que los atacantes pueden investigarlas fácilmente
  - Nombres de familiares o mascotas
  - Cumpleaños, dirección
  - Palabras relacionadas con la compañía donde trabaja (nombre del edificio, etc.)
  - Año actual
  - Palabras que puedan encontrarse en un diccionario o citas de libros famosos, películas, etc.

- Mejor utilizar las primeras letras de una frase
  - Ejemplo: MgcpcS55: Me gusta comer pizza con Salami 55
- Evitar guardas contraseñas directamente en texto plano en el disco duro o pegarlas a la pantalla con un pedazo de papel
- Utilizar haveibeenpwned.com o HPI Identity Leak Checker para comprobar si su combinación de dirección de correo electrónico y contraseña ha formado parte de una fuga de datos

Gestor de contraseñas

- Caja fuerte digital para todas las combinaciones usuario-contraseña
  - las contraseñas se almacenan encriptadas en el disco duro y están protegidas por una contraseña maestra
- Posibilidad de sincronización entre varios dispositivos
- Ofrecen la posibilidad de generar contraseñas al azar

- Variantes gratuitas de código abierto: KeepassXC y Bitwarden
  - Las extensiones del navegador aumentan la comodidad al rellenar automáticamente los campos de inicio de sesión
- Muchos proveedores comerciales también ofrecen variantes gratuitas
  - Sin embargo, si un atacante hackea los servidores del proveedor, sus propias contraseñas también podrían ser robadas y eventualmente publicadas en la red oscura

Autenticación de dos factores

- Asegurar los inicios de sesión con un segundo factor a parte de la combinación nombre de usuario/contraseña.
  - Ejemplo: secuencia cronológica de dígitos en el teléfono móvil (token que cambia cada pocos segundos)
  - Sólo con el token es posible un inicio de sesión y, por lo tanto, protege eficazmente contra los abusos
- Activar cuando sea posible

- Evitar los tokens que se envían por SMS/mensaje de texto al teléfono, mejor utilizar tokens que cambian cada minuto y que son generados por una app
- Si es posible, almacene el código QR/código de configuración en el gestor de contraseñas para no quedar bloqueado de los servicios si se pierde el teléfono móvil

Wi-Fi

- Los piratas informáticos pueden configurar fácilmente su propio Wi-Fi con el mismo nombre que el original (por ejemplo, Wi-Fi de la biblioteca o del tren)
  - Evitar las Wi-Fis públicas no cifradas
  - Utilizar sólo Wi-Fi encriptado y/o VPN
  - Utilizar preferentemente conexiones por cable en lugar de Wi-Fi

VPN

- Las VPN no hacen que una conexión sea "más segura", ya que hoy en día la mayoría de las conexiones ya están cifradas mediante SSL/TLS
- La VPN es útil
  - si quiere ocultar a tu proveedor de Internet qué sitios visitas
  - si quiere ocultar a una página web de qué país vienes (y si por ejemplo quieres activar contenidos que no estarían disponibles sin VPN)

- Los proveedores de VPN comerciales prometen encriptar los datos del usuario y, por lo tanto, no poder acceder a ellos ni desencriptarlos, aunque esto es difícil de verificar
- Evitar los proveedores de VPN "gratuitos"

Protección de datos

- Pensar cuales tipo de datos tiene en su trabajo o en su lugar privado y considerar como protegerlos si se pierden, se los roban o si están en manos de alguien extraño
- Ordenadores: Aunque es necesario iniciar sesión para usarlos, los datos pueden ser leídos aún si su disco está conectado a otro ordenador o si se conecta a él una memoria USB con un segundo sistema operativo.

- Mejor encriptarlos con herramientas como BitLocker, VeraCrypt en Windows, FileVault en Mac y LUKS en Linux
- Lo mismo ocurre con los discos duros y las memorias USB: Una vez conectados a un ordenador, los datos pueden ser leídos desde ellos si no están encriptados

Almacenamiento en la nube/en línea:

- Muchos proveedores de la nube encriptan sus datos en sus servidores - pero tienen la llave maestra y por lo tanto pueden encriptar y leer sus datos
- Es mejor buscar proveedores que ofrezcan almacenamiento de conocimiento cero
  - Esto significa que los datos se encriptan localmente en su máquina antes de ser transmitidos a un proveedor de la nube
  - Nadie más que usted puede leer los datos
- También puede cifrar los archivos localmente con programas como Cryptomator y BoxCryptor antes de enviarlos p. ej. a Dropbox

Copias de seguridad

- Hacer copias de seguridad periódicas de los datos importantes, por ejemplo, utilizando un NAS o una memoria USB (cifrada)
- Mantener varias versiones, por ejemplo, según el esquema abuelo, padre, hijo
- Sólo las copias de seguridad que no estén conectadas a un ordenador o a la red (copias de seguridad sin conexión) protegan contra el cifrado por troyanos o ataques similares
- Practicar regularmente la restauración de datos para estar preparado en caso de emergencia

Información general

- Uno Nunca puede estar 100% "seguro" de los ataques, sólo puede gestionar y mitigar los riesgos a los que se enfrenta uno
- Revisar regularmente si lo que se ha estado haciendo ayer sigue siendo útil y seguro hoy y mañana

- Con los productos que se pueden utilizar de forma gratuita, a menudo el usuario mismo es el producto
  - Los proveedores utilizan los datos de los clientes y los venden a otras compañías
  - El freeware puede ser un programa espía que envía información sensible de su ordenador a los servidores del desarrollador
  - A veces es mejor pagar por un producto y así limitar la recogida de datos
- Instalar solamente el software necesario y descárguelo únicamente de fuentes confiables

- Mantener siempre actualizado el sistema operativo y el software
- Mantener actualizado el antivirus
- Tener en cuenta que las suites que prometen hacer "todo" lo relacionado con la seguridad por el usuario tienen sus límites
- No conectar al ordenador memorias USB desconocidas que haya encontrado, por ejemplo, en el estacionamiento
  - Los programas pueden iniciarse de forma independiente, sin que se note y sin que el usuario actúe
  - Los atacantes pueden utilizar estos métodos específicamente para penetrar (entrar) una red