Presentacion

Nombre: Bradigson

Matricula: 2018-6114

Profesor: Huascar Frias Vilorio

Trabajo: TAREA DE LA UNIDAD NO. 2

Crear una política de seguridad para evitar los VIRUS INFORMATICOS?

Además de las vulnerabilidades técnicas, a menudo el empleado representa la vía más fácil para que un atacante acceda a los datos de una empresa. La razón: incertidumbre, ignorancia o conveniencias en el trabajo cotidiano.

Pero esta desventaja puede convertirse en una oportunidad para ti. Puedes reducir significativamente el riesgo de ataques a tu empresa con una formación regular para empleados.

No te preocupes, tus empleados no tienen que ser especialistas en computación. Nosotros les enseñaremos las reglas básicas que deben de utilizar para hacer que tu empresa sea mucho más segura.

1. Actualizaciones regulares
En primer lugar, debes mantener el software de tu equipo lo más actualizado posible y las actualizaciones periódicas te ayudarán. Se recomienda activar la función automática de actualización del software. Las actualizaciones ayudan a eliminar posibles agujeros de seguridad. Ten en cuenta las actualizaciones regulares de tus navegadores y programas de correo electrónico.

2. Proteje tu equipo con programas antivirus
Recomendamos un programa antivirus actualizado que ayude a proteger el equipo de virus y troyanos. Los programas de este tipo escanean el ordenador, manual o automáticamente, e informan de cualquier problema que se produzca. Existen tres tipos diferentes de análisis: el análisis en tiempo real, el análisis manual y el análisis en línea:

- **Escáner en tiempo real:** Se ejecuta en segundo plano como un servicio del sistema y controla todos los archivos, aplicaciones y servicios. Si la protección antivirus ha encontrado algo sospechoso, normalmente se pregunta primero al usuario cómo debería ser el siguiente procedimiento, para que el usuario tenga el poder de decisión.
- **Analizadores de virus en línea:** Los analizadores en línea comprueban los archivos o todo el equipo a través de Internet. Esto funciona sin instalación y normalmente sin registro. Sin embargo, el software no protege el equipo de nuevas infecciones, sino que sólo detecta las amenazas existentes durante el análisis.
- **Escáneres manuales:** La característica especial es la configuración manual del escáner. El usuario debe iniciar cada escaneo por sí mismo. Si se encuentra un programa peligroso, el programa muestra posibles soluciones para neutralizarlo.

Debe determinarse de antemano que el escáner antivirus se ejecute de forma permanente para que los programas maliciosos puedan detectarse en una fase temprana. También se recomiendan los llamados escaneos completos, que escanean completamente el ordenador.

Los programas antivirus deberían ser obligatorios para todos, ya que esto aumenta drásticamente la seguridad general del ordenador.

3. ¡Atención a fuentes de datos desconocidas!
Las fuentes de datos desconocidas incluyen, por ejemplo, memorias USB o discos duros externos. Estos parecen ser seguros a primera vista, pero pueden contener malware o archivos contaminados con virus. Conectar un dispositivo USB puede ser suficiente para infectar el equipo sin ningún signo.

Sugerencia: No conectes ningún dispositivo extraño a tu equipo, ya que nunca se sabe lo que puede haber en él. Tampoco deberías prestar tus dispositivos a extraños, ya que una transmisión de virus es posible.

4. Precaución con archivos desconocidos en Internet
Como medio de comunicación más importante, el correo electrónico presenta un riesgo especialmente elevado en lo que se refiere a la suplantación de identidad (phishing): por lo tanto, deberías comprobar los mensajes de correo electrónico con archivos adjuntos en particular, ya que el malware podría esconderse ahí.

¡No debes abrir archivos adjuntos de correo electrónico de remitentes desconocidos!
Puedes utilizar un programa antivirus para comprobar los archivos adjuntos del correo electrónico, de modo que esté seguro. Además, puede optar por varios tipos de cifrado de correo electrónico para evitar posibles ataques de virus por parte de malware. Para protegerse eficazmente, los mensajes de correo electrónico deben encriptar los registros de correspondencia almacenados y la conexión con tu proveedor de correo electrónico.

5. Cuidado al instalar un software nuevo
Es muy probable que todos los que navegan por Internet ya hayan instalado algún software. También en este caso debe comprobarse de antemano si la fuente tiene buena reputación y en qué medida. Porque al descargar software en el ordenador, el malware puede ser un invitado no deseado.

6. Copias de seguridad regulares
A pesar de todas las precauciones de seguridad, es posible que el equipo se haya infectado con troyanos u otros programas malintencionados. Como resultado, ya no se puede acceder a los datos en el peor de los casos.
En resumen: Todo se borra o ya no se puede recuperar. Por lo tanto, recomendamos realizar copias de seguridad periódicas en medios de almacenamiento externos para que las fotos, los vídeos y los documentos se puedan almacenar independientemente del ordenador.

7. Seguridad del Navegador: ¡Utilice actualizaciones!
Los navegadores obsoletos son el objetivo número uno para los ataques de hackers maliciosos. También puede utilizar diferentes navegadores para diferentes servicios. Esto tiene la ventaja de que todos los plug-ins, extensiones y cookies pueden ser desactivados en un navegador, ya que son particularmente vulnerables.
Como resultado, ya no podrá realizar operaciones bancarias o compras en línea ahí, pero estará más seguro en sitios web supuestamente inseguros. Además, deberías borrar regularmente tus pistas en Internet, como por ejemplo el caché. Esto los hace más difíciles de detectar para los atacantes cibernéticos.

8. Descarga de drive-by: ¡Abre los ojos!
Los ataques de hackers son cada vez más frecuentes e imaginativos. Un ejemplo de esto son las descargas desde el disco duro. Sin embargo, el enfoque de los atacantes es bastante simple:
Un usuario de Internet visita un sitio web que ha sido previamente editado por hackers. Ahora esta manipulación del sitio web desencadena una descarga. En algunos casos esto ni siquiera es notado por el usuario, porque no hay demanda adicional si la descarga debe ser iniciada. Una vez que el programa malicioso está en el PC, el efecto real puede desplegarse y, por lo tanto, dañar el dispositivo del usuario.
Ahora surge la pregunta de cómo protegerse óptimamente contra tales ataques. Aquí también recomendamos un programa antivirus actualizado. De lo contrario, debes estar atento a sitios web sospechosos o descargas dudosas, ya que el malware es muy difícil de detectar.

9. Usa contraseñas seguras
En este punto, los usuarios y las empresas deben tener cuidado de utilizar contraseñas seguras y, sobre todo, complejas. Por ejemplo, los administradores de contraseñas se pueden utilizar para almacenar contraseñas de forma segura y para generar nuevas contraseñas compuestas de diferentes letras, números y caracteres especiales.

10. La protección de datos y la seguridad informática puede garantizar una empresa más resistente
Instrúyete e instruye a tus empleados con nuestros cursos de formación Seguridad Informática para Empleados y Protección de datos para empleados.
Una vez completado el curso con éxito, recibirás como prueba un certificado.