3.8 Seguridad básica

CONTRASEÑAS

La seguridad de las contraseñas es fundamental en la era digital. Una contraseña segura actúa como la primera línea de defensa en el ámbito de la seguridad, protegiendo el acceso a la información o servicios que no deseamos que queden expuestos. Sin embargo, las contraseñas débiles o una mala política de establecimiento de contraseñas puede provocar que se vean comprometidas, lo que lleva a brechas de seguridad y pérdida de datos. Por lo tanto, es crucial seguir las mejores prácticas para crear y gestionar contraseñas seguras. De acuerdo al informe Verizon de 2024 aproximadamente el 50% de las brechas de seguridad se produjeron a través de la obtención de credenciales.

A continuación veremos una serie de medidas que se deben adoptar para prevenir estos problemas.

CONTRASEÑAS II

CÓMO CREAR CONTRASEÑAS FUERTES

- **Usar contraseñas únicas.** Utilizar diferentes contraseñas para diferentes servicios o cuentas. Esto reduce el impacto de que una fuga de seguridad impacte al resto de servicios o cuentas.
- **Hacerla aleatoria.** Que no sigan un patrón, que utilicen mayúsculas, minúsculas, letras, números o caracteres especiales. Que NO guarden relación con información personal.
- **Usar combinaciones largas.** A mayor longitud de una contraseña, mayor complejidad y tiempo necesario para averiguarla. De acuerdo al NIST se debe implementar un mínimo de 12 caracteres., aunque idealmente deberían ser 16. Ej. Calculadora seguridad.
- **Evitar contraseñas usadas comúnmente o demasiado sencillas.** “12345678”, “Admin”,”quewty”,”asdf”

CONTRASEÑAS III

BUENAS PRÁCTICAS

- **Actualizarlas regularmente.** Es importante para minimizar el riesgo de accesos no autorizados. Una práctica aconsejables es cambiarlas cada 6 meses.
- **Implementar políticas de caducidad.** Obligar a los usuarios a actualizar la contraseña pasado un período de tiempo. Sin embargo debe existir un equilibrio entre esto y la “fatiga” de los usuarios.
- **Estar atento a fugas de contraseñas.** No solo a nivel interno de una empresa, si no a publicaciones a fugas publicadas en internet. Ejemplo.
- **Añadir capas extra cuando sea posible.** Añadir funcionalidades como 2FA, biometría o tokens. Algo que sé, algo que soy, algo que tengo.

CONTRASEÑAS IV

- **Modificar siempre las contraseñas por defecto.** Es común que por ejemplo los routers u otros dispositivos tengan contraseñas de acceso o de red predefinidas, muy sencillas o genéricas. Ejemplo1, Ejemplo2
- **Implementar almacenamiento seguro de contraseñas.** Utilizar algún tipo de algoritmo de encriptación para almacenar las contraseñas. NUNCA EN TEXTO PLANO.
- **Utilizar gestores de contraseñas.** Existen servicios que se encargarán de guardar, generar, almacenar y custodiar las contraseñas por nosotros.
- **Utilizar protocolos seguros "en tránsito".** El uso de protocolos de comunicación seguros como por ejemplo HTTPS cuando navegamos por internet, disminuye el riesgo de que una contraseña se vea comprometida.

ACTUALIZACIONES I

Los sistemas operativos, navegadores web, programas, aplicaciones e incluso el firmware son susceptibles de tener fallos de seguridad. Por este motivo, pueden necesitar ser actualizados, independientemente del dispositivo en el que se encuentren instalados. Esto incluye los programas y sistemas operativos de ordenadores, tablets, smartphones, consolas de videojuegos u otro tipo de dispositivos.

Una actualización es un añadido o modificación realizada sobre los sistemas operativos o aplicaciones que tenemos instaladas en nuestros dispositivos, cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

IMPORTANTE: No confundir tener una aplicación actualizada con tener la última versión.

ACTUALIZACIONES II

SUBSANAN VULNERABILIDADES

Es la razón número 1 para actualizar el software o el firmware de un equipo. Una vez se hace público un fallo de seguridad, cualquiera con los conocimientos adecuados puede utilizarlo para causar daño u obtener información sensible.

Habitualmente “fabricantes” u organizaciones que mantienen y publican el software, mantienen canales donde informan de las actualizaciones o “parches” que publican y los “problemas” que vienen a subsanar. Ejemplo1, Ejemplo2 , Ejemplo3, Ejemplo4, Ejemplo5

ACTUALIZACIONES III

CVSS

Para medir el impacto de una vulnerabilidad existe el Common Vulnerability Scoring System (CVSS), que es un estándar global para evaluar y gestionar vulnerabilidades IT. Permite puntuar las vulnerabilidades de 0 a 10, basándose en su probabilidad de explotación y su impacto en las organizaciones. Esta puntuación ayuda a las empresas a priorizar y mitigar las vulnerabilidades, teniendo en cuenta sus recursos y objetivos empresariales. Los niveles de severidad se clasifican como bajo (0,1-3,9), medio (4-6,9), alto (7-8,9) y crítico (9-10).

ACTUALIZACIONES IV

EPSS

El Exploit Prediction Scoring System (EPSS) estima la probabilidad de que una vulnerabilidad de software sea explotada. Proporciona una puntuación de 0 a 100% basada en información de amenazas de CVE y datos de explotación. EPSS recopila información sobre la vulnerabilidad, como el proveedor, la antigüedad, referencias, debilidades (CWE), métricas CVSS y más. Proporciona una estimación diaria de la probabilidad de actividad de explotación en los próximos 30 días. EPSS es un estándar en desarrollo y se proporciona libremente al público.

ACTUALIZACIONES IV

ZERO-DAY

Es un “exploit” que aprovecha un fallo de seguridad desconocido en software, hardware o firmware. “Día cero” se refiere al hecho de que el proveedor de software o dispositivo tiene cero días para solucionarlo porque podría ser utilizado para acceder a sistemas vulnerables. La vulnerabilidad puede permanecer sin detectar hasta que alguien la encuentra. En el mejor de los casos, los investigadores de seguridad o los desarrolladores de software, encuentran el problema antes que los atacantes.

Ejemplo

ANTIVIRUS

Por obvio que parezca, el uso de algún software antivirus es una medida básica de prevención y control para que los equipos no se infecten con algun tipo de malware, adware o similares.

Además de los antivirus de instalación tradicional se puede utilizar alternativas online como virustotal, que posiblemente sea el sandbox más conocido. Hace uso de más de 60 motores de detección para analizar archivos o urls.

Otra alternativa es crear una máquina virtual replicando lo más posible el entorno habitual y con recursos suficientes para su funcionamiento, además de herramientas de monitorización y análisis para poder examinar el comportamiento.

NOTA: Windows 10 Pro/Enterprise y Windows11 ofrecen la posibilidad de utilizar sandbox ya integrados.

FIREWALL

Un firewall es un sistema de seguridad que controla el tráfico de red basándose en políticas de seguridad. Se sitúa entre redes seguras y no seguras (generalmente Internet) para proteger contra amenazas, bloquear contenido malicioso y prevenir la fuga de información confidencial. Puede ser hardware, software o una combinación de ambos. Al monitorear el tráfico, puede bloquear aquel que podría explotar una vulnerabilidad de seguridad, previniendo así las vulnerabilidades de día cero. Es importante:

- **Bloquear puertos innecesarios.** Cerrar los puertos que no se utilizan reduce las posibles vías de ataque.
- **Actualizado.** Especialmente en el tipo software.
- **Deshabilitar servicios o protocolos inseguros.** Por ejemplo Telnet.

ORÍGENES CONOCIDOS

No menos importante, a la hora de instalar o utilizar software, es fundamental que este tenga un origen fiable o conocido. Una fuente de entrada habitual de malware o cualquier tipo de software malicioso es la instalación y/o utilización de software de un origen diferente a su origen.

El software de fuentes desconocidas o no confiables puede contener virus, spyware, ransomware u otros tipos de malware que pueden comprometer la seguridad de tu sistema. Estos programas maliciosos pueden robar información personal, dañar tus archivos, ralentizar tu equipo o incluso tomar el control de tu sistema.

Por lo tanto, es crucial verificar siempre la fuente del software antes de descargarlo e instalarlo. Esto puede implicar la comprobación de la reputación del desarrollador, la lectura de opiniones de otros usuarios, y la utilización de un software antivirus para escanear el archivo antes de la instalación.

ORÍGENES CONOCIDOS II

Incluso, en ocasiones la publicación en repositorios conocidos no garantiza que algo esté libre de malware.

- Paquetes maliciosos en Pypi.
- Paquetes maliciosos en RubyGems
- Paquetes maliciosos en NPM
- Malware distribuido a través de versiones pirateadas de MS Office
- Uso de errores de IA para distribuir malware.

CONTROL DE ACCESO FÍSICO

El control de acceso físico es un componente crucial en la ciberseguridad. Se refiere a las medidas preventivas implementadas para restringir el acceso no autorizado a recursos físicos, como edificios, sistemas y dispositivos de hardware.

Estas medidas pueden incluir tarjetas de acceso, cerraduras biométricas, sistemas de vigilancia y seguridad física. Estas medidas son esenciales para proteger contra amenazas físicas que pueden comprometer la seguridad de la información. Por ejemplo, un intruso podría obtener acceso a un servidor físico y extraer datos sensibles. Por lo tanto, el control de acceso físico es un componente esencial de un plan de seguridad integral, trabajando en conjunto con el control de acceso lógico para proporcionar una defensa en profundidad contra una variedad de amenazas de seguridad.