Certified Tech Developer
The Ultimate Degree

DigitalHouse>

Certified Tech Developer
The Ultimate Degree

Infraestructura I

La criptografía en los sistemas

Cuando se habla de seguridad informática, los distintos conceptos, estrategias y técnicas para proteger un sistema o una red se construyen sobre tres pilares que se conocen por su sigla en inglés CIA:

- **Confidentiality** (confidencialidad): se refiere a la protección de los datos, recursos y sistemas de accesos no autorizados.
- **Integrity** (integridad): se refiere a la protección de los datos, recursos y sistemas de cambios no autorizados y así asegurar su confiabilidad.
- **Availability** (disponibilidad): se refiere a garantizar que aquellos usuarios autorizados tengan acceso a los datos, recursos y sistemas que necesitan.

Cuando hablamos de criptografía —una práctica que es parte de cualquier estrategia de seguridad informática—, la letra "A" en la sigla cobra un nuevo significado: **Authentication** (autenticación), que se refiere a verificar la identidad de un sujeto.

Es decir que la criptografía en el ámbito de la informática puede ser utilizada para tres propósitos distintos:

1. Implementar confidencialidad para proteger los datos y sistemas.
2. Proteger la integridad de los datos.
3. Verificar la identidad de una persona o sistema.

En las próximas secciones nos vamos a enfocar en los puntos 1 y 3, y cómo podemos utilizar la criptografía para lograr estos objetivos.

La criptografía como vector de ataque

Hasta aquí vimos que la criptografía es utilizada para proteger información de los ojos de terceros, asegurando que los mensajes intercambiados puedan ser leídos solo por aquellas partes que fueron autorizadas para tal fin. Sin embargo, desde mediados de la década del 2010, la criptografía se comenzó a popularizar como un vector de ataque informático a través de lo que se conoce como ***ransomware***.

Un ransomware es un **software que encripta la información de un individuo u organización con propósitos extorsivos**. Es decir, mediante el uso de la criptografía, los archivos en cuestión son cifrados utilizando un algoritmo complejo y una clave conocida únicamente por el autor del ataque. Finalmente, se indica al usuario qué operación financiera deberá realizar para el pago del rescate. El ámbito de ataque puede limitarse a una computadora en particular o a toda una red.

Los ataques de este tipo comienzan por vulnerar el perímetro por medio de la acción de un usuario que permite la ejecución del software programado con fines maliciosos. Esto puede suceder tentando al usuario a descargar un archivo desde Internet y luego

ejecutarlo, ya sea mediante un correo electrónico con enlaces que lleven al usuario a descargar el ransomware o con un dispositivo USB infectado.

Una vez que el ransomware comienza a ejecutarse en el dispositivo, localizará los archivos que está programado para encriptar. Para cumplir con los propósitos extorsivos, el software encripta archivos con extensiones conocidas y que pueden ser de valor para el usuario (imágenes, documentos, planillas de cálculo, etc.), pero deja intactos los archivos del sistema operativo. De esta manera, garantiza el correcto funcionamiento del mismo, así permite al usuario descubrir los efectos del ransomware y acceder a la información necesaria para realizar el pago (si así lo deseara).

Alternativamente, el ransomware podría estar programado para iniciar un escaneo de la red en busca de otras computadoras y de potenciales vulnerabilidades en ellas que le permitan reproducir la mecánica de encriptación y extender el ataque más allá del ámbito de la computadora en la que el ataque comenzó.

Cómo defenderse de un ramsonware

Defenderse de un ransomware es sencillo. El administrador de sistemas —o incluso nosotros mismos que como usuarios hogareños podemos ser vulnerables a estos ataques— podemos prepararnos para prevenir o recuperarnos de un ataque de estas características.

Para ello **es fundamental que tomemos acciones antes del ataque**. De no hacerlo, una vez sucedido, no hay mucho que se pueda hacer más que cumplir con la demanda del atacante y confiar ciegamente de su buena fe, o resignarnos y aceptar la pérdida de información. Pero si nos preparamos, podemos reducir y prevenir el daño:

- Como toda estrategia de ciberseguridad la base es educar al usuario a:
    - No abrir correos sospechosos.
    - Identificar y reportar correos sospechosos al departamento de sistemas.
    - No insertar dispositivos USB de los que se desconoce su procedencia.
- Tener una red debidamente segmentada, en donde los usuarios no compartan el mismo espacio de la red que los servidores. Esto permite tener puntos de control para el tráfico entre el tráfico de usuario y los servidores de la compañía.
- Mantener todos los sistemas operativos actualizados, protocolos deprecados desactivados y vulnerabilidades remediadas.
- Finalmente, pero no por eso menos importante, mantener una buena estrategia de backup, que permita recuperar de nuestros respaldos cualquier archivo que haya podido ser cifrado con propósitos extorsivos.