Técnico en

DESARROLLO DE SOFTWARE

Seguridad Informática

Instituto Von Neumann

Ataques que comprometen la seguridad informática

Unidad II

1. Sensibilidad de la información

Cuando se habla de sensibilidad de la información podría referirse a la vida misma de cada una de las personas que se exponen en un solo fragmento digital. Existen muchas definiciones, pero en el entorno empresarial una de las más completas, es la siguiente: “Aquella información, cuya revelación, alteración, pérdida o destrucción puede producir daños importantes al propietario de esta”.

Teniendo en cuenta que cada vez más cantidad de información está en formato digital, como profesionales del sector de las TI y, en concreto, desarrolladores de software nuestra misión fundamental es protegerla.

La pérdida de información sensible puede producirse accidental o malintencionadamente y suele acarrear un daño económico y de prestigio, afectando al propietario. Pero ¿qué sucedería si la información enviada en ese correo electrónico fuese confidencial para la empresa?, ¿y si la transmisión de esa información sin el consentimiento del propietario de esta estuviera incumpliendo alguna ley? Pues probablemente tendríamos un serio problema, bien porque dicha información confidencial pudiera caer en manos de nuestra competencia o en las de posibles ciberdelincuentes.

2. Ciberataques

Es un asalto al sistema en cuestión utilizando una vulnerabilidad deliberadamente por un actor, para evadir los servicios de seguridad y violar las políticas de seguridad del sistema.

Tipos de ataques:

- **Pasivos**: son los ataques que pretenden aprender y recopilar información de los sistemas perpetrados, pero sin causar ningún daño que afecte el funcionamiento del sistema.
- **Activos**: es un ataque que busca afectar el funcionamiento del sistema.

Algunos conceptos importantes para entender los ciberataques son:

- **Superficie de ataque**: se define como toda vulnerabilidad disponible para atacar.
- **Virus**: es un fragmento de software que se adhiere a un ejecutable para infectar un sistema.

Ciberataques de mayor impacto en la historia

Durante la historia moderna de la computación se han perpetrado grandes y significativos ataques informáticos distribuidos en todo el mundo y a veces enfocados en una localidad. Dichos acontecimientos han supuesto grandes perdidas monetarias para corporaciones, instituciones, gobiernos y en general para la población.

1. MafiaBoy
    a. Aconteció durante el año 2000.

   b. Fue un ataque **DDoS**
   c. Los principales afectados fueron CNN, Dell, E-Trade, eBay y Yahoo!
   d. Gracias a este ataque, las leyes ante delitos cibernéticos fueron promovidas.

2. ILoveYOU
   a. Aconteció en mayo del 2000.
   b. Fue un ataque de **Phishing** y **Worm**, utilizando una doble extensión.
   c. Las perdidas se calculan cerca de $10 mil millones

3. Conficker
   a. Aconteció durante noviembre del 2008.
   b. Fue un ataque de **Botnet** y **Worm**.
   c. Los principales afectados fueron computadoras Microsoft domesticas, corporativas y gubernamentales en 190 países.
   d. Las perdidas se calculan cerca de $9 mil millones.

4. WannaCry
   a. Aconteció durante mayo del 2017.
   b. Fue un ataque **Ransomware** con $300 por desencriptar la información.
   c. Aproximadamente 230,000 computadoras sin los parches de seguridad en 150 países fueron afectadas.
   d. Cerca de $4 mil millones fueron perdidos.

5. Pegasus
   a. Aconteció durante el año 2021.
   b. Fue un ataque utilizando **Spyware** en dispositivos IOS y Android.

c. Entre las aplicaciones afectadas WhatsApp, SMS y IMessage.

d. Los objetivos de este ataque fueron personajes públicos de diferentes países, tales como presidentes y servidores públicos.

Tipos de malware

Un malware es un programa que tiene un objetivo malicioso contra el sistema que infecta utilizando diferentes técnicas y tácticas.

Existen distintos tipos de malware en la actualidad y cada uno de ellos tiene sus peculiaridades y una estrategia específica de infección, así también como un objetivo. Para cada uno de estos malware existe ciertas defesas que se pueden utilizar para prevenirlo, mitigarlo o para recuperar el sistema, si es el caso.

- **Ransomware:** es un tipo de malware que encripta la información de todo el sistema (host) al que infecta y pide una recompensa (ransom) para dar la llave para desencriptarla o en su defecto la eliminación de toda la información.
- **Keylogger**: su principal función es capturar escritura realizada con el teclado, el siguiente nivel de vigilancia se denomina **Spyware**.
- **Spyware**: este malware que infecta un sistema con el propósito es espiar la actividad del usuario mediante cámara, micrófono, periféricos tal como teclado, mouse. Incluso, el sonido generado al utilizar el teclado puede ser traducido a texto mediante el uso de Machine Learning.
- **Adware**: su principal objetivo es mostrar insistentemente anuncios publicitarios al usuario para generar ganancias.

- **Trojans horse**: es un programa que se enmascara mostrándose como útil, pero contiene un virus.
- **Worms**: su característica principal es infectar un equipo y luego, mediante escaneos de red, replicarse a otros sistemas e infectarlos.
- **Botnet**: este malware infecta una computadora sigilosamente y la hace un zombi, para luego ser utilizado en ataques DDoS activando toda la red de bots.

Ataques más comunes

1. **Ingeniería social:** es el uso de técnicas psicológicas para engañar a los usuarios para infectar dispositivos con malware. Usualmente es utilizado como el punto de partida de los ataques, luego de realizar la recolección de datos. La única manera prevenirlo es educando a los usuarios y aplicando lineamientos y estándares.
2. **Man-in-the-middle:** técnica en la cual el atacante finge ser la puerta de salida (Gateway) por donde se realizan las conexiones a internet o a otro sistema. Y redirige todo el trafico al destinatario real. En tal posición le es posible analizar todo el tráfico que surge de dicha comunicación en ambas vías.
3. **Phishing:** es un de los ataques mas comunes y extendidos, involucra engañar a los usuarios, fingiendo ser una empresa legítima y solicitar acciones. Algunas de estas acciones suelen ser, enviar datos sensibles por correo, ingresando a un enlace o descargando y abriendo un archivo (Word, Excel, PDF, etc.) con una carga maliciosa.

4. **Spam:** esta técnica involucra enviar promociones o anuncios no deseados a usuario. En el caso mas grave, puede ser la vía para realizar un ataque de **Phishing**.
5. **Brute force:** técnica para obtener la llave para descifrar un contenido que involucra probar cada combinación posible.
6. **Denial of service (DoS):** ataque que utiliza una gran cantidad de solicitudes a un servidor para saturarlo y hacer que este sea inaccesible.
7. **Distributed denial of service (DDoS)**: el objetivo es el mismo que el ataque **DoS**, únicamente que en este se utiliza computadoras zombis de una **Botnet** para que el ataque tenga múltiples orígenes y se mas complicado detenerlo mediante bloqueos de IP.

3. Defensas ante ataques informáticos

Existen diversos tipos de defensas que se pueden utilizar para prevenir, mitigar y recuperar los sistemas ante la variedad de amenazas anteriormente descritas. Entre las mas importantes se encuentran:

- **Certificados HTTPS**: son certificados brindados por una entidad certificadora autorizada y con la confianza de los usuarios. Su función es asegurar que la pagina web mostrada es la página web solicitada.
- **Parches de seguridad**: son actualizaciones publicadas por los desarrolladores de los programas o sistemas operativos. Usualmente son descubiertas por actores benignos mediante programas de recompensas y otras veces son malignos

buscando obtener un beneficio. La responsabilidad de aplicar dichas actualizaciones recae siempre en los usuarios.

- **Encriptación de datos**: cifrar los datos utilizando algunos de los algoritmos disponibles. Aun cuando un actor no autorizado consiga acceso a los datos, existe una capa de seguridad extra para proteger la confidencialidad.
- **Copias de seguridad**: ante ataques tipo Ransomware, una vez ejecutados, la única salida que no implica un pago es cuando se tiene una copia de seguridad. De esta manera podemos estar seguros de que los datos están respaldados.
- **Web application firewall (WAF)**: usualmente los sistemas de Software as a Service, tal como Google Cloud o Amazon Web Services, poseen la capacidad de proteger las aplicaciones mediante un firewall dedicado a la comunicación Web. Se utilizan para proteger de ataques DDoS.
- **Listas blancas (Whitelist)**: es un listado de opciones que aceptamos. Es decir, todo lo que este en la lista blanca se acepta el **resto se rechaza**.
- **Listas negras (Balcklist)**: es un listado de las opciones que rechazamos. Es decir, todo lo que esta en la lista negra se rechaza, el **resto se acepta**.
- **Extensiones de archivos visibles**: se debe tener siempre visibles las extensiones de los archivos, para asegura que un archivo sea lo que dice ser y no un ejecutable con doble extensión (texto.txt.vbs).
- **Antivirus**: es un programa destinado para proteger el sistema de diferentes tipos de virus, mediante escaneos frecuentes y utilizando una base de datos compartida y actualizada mundialmente con la firma de los virus encontrados.

Referencias y contenido adicional para revisar

- https://technet.microsoft.com/es-es/library/dd897007.aspx
- https://technet.microsoft.com/es-es/library/dd897033.aspx
- https://technet.microsoft.com/es-es/library/dd897047.aspx
- “Network Security Essentials,” 6/e, by William Stallings, Chapter 1 – “Introduction”