MATERIAS TÉCNICO-CIENTÍFICAS

TEMA 41

Ciberdelincuencia y agentes de la Amenaza: Botnet; Business E-mail Compromise; Cartas nigerianas; Cryptojacking; Denegación de servicio; Ingeniería social; Inyección SQL; Malware; Pharming; Phishing; Spear phishing; Ransomware; Skimming; Spoofing; Spyware, Troyano; XSS; Zero-day. Cibercriminales. Crimen as Service. Hacktivistas. Insider threat. APTs. Cyber Kill Chain.

1. Ciberseguridad

El prefijo «ciber» alude a todo lo relacionado con la **informática**, no solo con internet, requiriendo una **visión más amplia** de la seguridad informática. Aunque las amenazas a menudo provienen de internet, no es la única vía de ataque a los sistemas informáticos.

La **ciberseguridad** es un conjunto de medios, acciones y normas implementadas en el entorno de un sistema informático para garantizar la **seguridad de todos sus activos**. Estos activos incluyen elementos tangibles (hardware, infraestructuras) e intangibles (información, capital humano, tecnología), siendo estos últimos los más relevantes para instituciones como la **Policía Nacional.**

Para preservar la seguridad de los sistemas informáticos, es necesario conocer las f**laquezas** (**vulnerabilidades**) y las posibles **amenazas**.

Vulnerabilidades de un sistema

- Manejar **gran cantidad de datos.**
- Trabajar en **entornos virtuales.**
- El **uso corporativo de terminales privados** (dispositivos propiedad de la empresa usados por trabajadores para fines personales y corporativos, mezclando contenido y aumentando la exposición a amenazas).
- El **uso indebido de redes sociales.**
- El uso inadecuado del **internet de las cosas** (dispositivos conectados como altavoces con asistente virtual o termostatos inteligentes controlados por smartphone).

Amenazas

Las amenazas son **ataques con fines delictivos**, pero también pueden ser **accidentes naturales o tecnológicos**. Estos últimos preocupan especialmente a empresas o instituciones que deben proteger sus datos y equipos para continuar operando, ya que la pérdida de servidores por un huracán sin un «plan B» supondría un **caos**.

2. Agentes de la amenaza

Las **amenazas** provienen de diversos ámbitos y con fines distintos; la vida en internet ha propiciado que el mundo delincuencial también llegue a estos lugares.

Los diferentes agentes de la amenaza, de dónde proviene el peligro, se clasifican en cinco grupos:

- **Amenaza aislada:** Proviene de individuos muy poco organizados o una única persona, buscando satisfacción personal más que beneficio económico real.
- **Cibercriminales**: Grupos u organizaciones criminales que basan su actividad en internet para cometer delitos o facilitan el aprovechamiento del beneficio de otros delitos, como hackers que envían e-mails falsos haciéndose pasar por bancos para robar claves y vaciar cuentas.
- **Ciberterroristas**: Organizaciones terroristas que usan internet como medio para realizar acciones contra infraestructuras o estados, o como medio de financiación, propaganda o reclutamiento.
- **Ciberactivistas o Hacktivistas**: Grupos organizados que usan internet para difundir ideologías, generalmente contra otro grupo o gobierno; son cibercriminales con un perfil muy concreto.
- **Estados**: Ciertos estados pueden usar internet para desestabilizar a otros.

3. Conceptos

3.1. MALWARE

Un **programa malicioso** (malware), **programa maligno, programa malintencionado o código maligno** es cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Tipos de malware

- **Ransomware**: Forma de ciberextorsión donde el malware se instala en un terminal sin consentimiento, permitiendo al delincuente bloquear o encriptar datos remotamente. La víctima debe pagar para obtener un código de recuperación.
- **Spyware**: Software espía que se instala sin conocimiento del usuario para captar y recopilar información a la que accede un ordenador, enviándola a una entidad externa.

- **APTs** (**Amenazas Persistentes Avanzadas**)**:** Tipo de ataque que penetra en un sistema y permanece oculto, buscando obtener objetivos de manera progresiva y aumentar conocimientos sobre la entidad atacada, sin buscar beneficio a corto plazo.
- **Troyano**: Malware que se presenta como un programa legítimo e inofensivo, pero que, al ejecutarse, brinda a un atacante acceso remoto al equipo infectado.
- **Botnet**: Red compuesta por dispositivos infectados (zombis) controlados remotamente por atacantes, cuyo objetivo principal es controlar el mayor número de dispositivos para llevar a cabo actividades ilícitas.

3.2. Ataques dirigidos a empresas

- **Business Email Compromise:** Ataque dirigido contra las cuentas de correo de una organización o alguno de sus empleados, con el fin de penetrar en ella, conocer su funcionamiento interno y llevar a cabo otro tipo de ataques como el Spear Phishing.
- **Spear Phishing:** Phishing dirigido contra un usuario u organización concreta, simulando ser un contacto conocido para ganar su confianza.
- **Insider Threat:** Amenaza proveniente de una persona de la organización o empresa que divulga información sensible sobre dicha empresa de forma intencionada.

3.3. Ataques relacionados con tarjetas bancarias

- **Carding**: Técnica para robar datos financieros mediante malware, phishing/smishing, vishing, shoulder surfing, webs fraudulentas o lectores de tarjetas.
- **Phishing**: Ataque en el que alguien suplanta una entidad o servicio, remitiendo un correo o mensaje instantáneo para conseguir credenciales o información de tarjeta de crédito.
- **Vishing**: Llamadas telefónicas fraudulentas que se hacen pasar por entidades para recopilar datos de posibles víctimas.
- **Shoulder surfing:** Técnica en la que el ciberdelincuente anota los números de la tarjeta si la tiene físicamente o está en su campo de visión.
- **Skimming**: Extracción de datos de la tarjeta de crédito en el punto de venta para fabricar tarjetas falsas o comprar artículos; suele requerir un dispositivo físico deshonesto en el lugar de pago.

3.4. Ataques a páginas web

- **DDoS** (**Denegación de servicio**)**:** Ataque distribuido que ataca a un servidor web simultáneamente desde muchos equipos diferentes para bloquear su funcionamiento al no poder administrar tantas solicitudes de información.
- **Inyección SQL:** Ataque que permite insertar códigos en las bases de datos de páginas web (basadas en el lenguaje de programación SQL) para obtener acceso a los datos de esa página.
- **Pharming**: Ataque que aprovecha una vulnerabilidad del software de los servidores DNS, modificando o sustituyendo el archivo del servidor de nombres de dominio y cambiando la dirección IP legítima por otra que da acceso a una web falsa.
- **XSS**: Vulnerabilidad en páginas web generadas dinámicamente (en función de los datos de entrada) que el atacante aprovecha para cambiar la configuración del servidor y conseguir los datos de la página.

3.5. Otros ataques informáticos

- **Spoofing**: Técnica de suplantación de identidad, especialmente por correo electrónico, donde el atacante cambia la dirección del remitente y el asunto para simular una comunicación real. El email spoofing se usa para estafas y obtener datos personales (contraseñas, números de tarjeta de crédito, cuentas bancarias, DNI, correos) con fines económicos. El atacante enmascara su correo por el de una víctima indirecta (usuario, entidad, servicio), suplantando a alguien de confianza para obtener dinero o información personal mediante un segundo fraude.
- **Zero day:** Vulnerabilidades en sistemas o programas desconocidas por fabricantes y usuarios, pero conocidas por atacantes, que aún no pueden ser corregidas y son explotadas.
- **Crime as service:** Especialización delictiva donde expertos en tecnología ofrecen servicios a terceros, permitiendo a personas menos técnicas cometer delitos tecnológicos.
- **Cryptojacking**: Ataque a dispositivos para usar sus recursos sin permiso del propietario y generar criptoactivos.
- **Cartas Nigerianas**: Comunicación inesperada (correo electrónico, carta, mensajería instantánea) prometiendo negocios rentables, que solicita dinero por adelantado para obtener el beneficio prometido.

- **Técnicas de ingeniería social:** Conjunto de técnicas de engaño a usuarios legítimos para obtener información privada sobre su entorno, permitiendo ataques más sofisticados como acceso a sistemas, fraude o robo de información.

4. CYBER KILL CHAIN

Es la cadena de secuencias que sigue cualquier tipo de ciberataque, incluyendo las fases de reconocimiento, preparación, distribución, explotación, instalación, comando y control y acciones sobre los objetivos.

Reconocimiento
Primer paso de la Cyber Kill Chain, donde se recopila toda la información de los objetivos.

Preparación
Una vez recopilada suficiente información de su objetivo, se elegirán uno o varios vectores de ataque para iniciar la intrusión a su espacio.

Distribución
Una vez que el ciberdelincuente ha conseguido acceder a sus sistemas, tendrá la libertad que necesita para distribuir la carga de lo que tenga reservado para ese ataque (malware, ransomware, spyware, etc.).

Explotación
Con la carga ya distribuida, comienza el proceso de explotar el sistema, lo que dependerá del tipo de ataque.

Instalación
Si un ciberdelincuente ve la oportunidad de realizar ataques en el futuro, su siguiente movimiento es instalar una puerta trasera para acceder de forma constante a los sistemas del objetivo.

Comando y control
Una vez que los programas y las puertas traseras están instalados, el atacante tomará el control de los sistemas y ejecutará cualquier ataque que tenga pensado.

Acciones sobre los objetivos

Esta es la fase de ejecución continua en la que un atacante emprende acciones sobre su objetivo. Las posibles consecuencias incluyen:

- **Cifrar datos** para pedir un rescate.
- **Filtrar datos** al exterior para obtener un beneficio económico.
- Hacer que **caiga su red** mediante un ataque por denegación de servicio.
- **Otras posibles** consecuencias.