



UNIDAD 2

AUDITORÍA DE INCIDENTES DE CIBERSEGURIDAD

Las amenazas más importantes relacionadas con el ciberespacio se pueden clasificar en dos grupos: amenazas contra la información, y amenazas contra la infraestructura. Las amenazas contra la información son aquellas que provocan una pérdida o un uso indebido de la información, el espionaje, el fraude, el robo de identidad, entre otras muchas. Por otro lado, las amenazas contra la infraestructura son aquellas que pueden provocar la interrupción parcial o total de los sistemas, como la infección de malware, ataques contra redes, sistemas, etc. En esta unidad vemos a realizar una taxonomía de estos incidentes, de como detectarlos, monitorizarlos y notificar a los responsables de responder a ellos.

TAXONOMÍA DE INCIDENTES DE CIBERSEGURIDAD.

La taxonomía que aquí se propone está tomada de la propuesta por la ENISA¹ la cual es básicamente la utilizada por el INCIBE² y que es necesario utilizar en la guía de nacional de gestión y notificación de ciberincidentes³ A continuación se detallan los tipos de incidentes según su categoría:

¹ https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

² <https://www.incibe-cert.es/taxonomia>

³ https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Contenido abusivo

SPAM: correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.

Delito de odio: contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.

Pornografía infantil, contenido sexual o violento inadecuado: material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.

Contenido dañino:

Sistema infectado: sistema infectado con malware. Ejemplo: sistema, computadora o teléfono móvil infectado con un rootkit.

Servidor C&C (Mando y Control): conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.

Distribución de malware: recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.

Configuración de malware: recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de webinjects para troyano.

Malware dominio DGA: nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).

Obtención de información

Escaneo de redes (scanning): envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.

Análisis de paquetes (sniffing): observación y grabación del tráfico de redes.

Ingeniería social: recopilación de información personal sin el uso de la tecnología. Ejemplos: mentiras, trucos, sobornos, amenazas.

Intento de intrusión

Explotación de vulnerabilidades conocidas: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ejemplos: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).

Intento de acceso con vulneración de credenciales: múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.

Ataque desconocido: ataque empleando exploit desconocido.

Intrusión

Compromiso de cuenta con privilegios: compromiso de un sistema en el que el atacante ha adquirido privilegios.

Compromiso de cuenta sin privilegios: compromiso de un sistema empleando cuentas sin privilegios.

Compromiso de aplicaciones: compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.

Robo: intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.

Disponibilidad

DoS (Denegación de Servicio): ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.

DDoS (Denegación Distribuida de Servicio): ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

Sabotaje: sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.

Interrupciones: interrupciones por causas externas. Ejemplo: desastre natural.

Compromiso de la información

Acceso no autorizado a información: acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.

Modificación no autorizada de información: modificación no autorizada de información.

Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.

Pérdida de datos: pérdida de información. Ejemplos: pérdida por fallo de disco duro o robo físico.

Fraude

Uso no autorizado de recursos: uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales.

Derechos de autor: ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplos: Warez.

Suplantación: tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

Phishing: suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

Vulnerable

Criptografía débil: servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.

Amplificador DDoS: servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist.

Servicios con acceso potencial no deseado: servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.

Revelación de información: acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos: SNMP o Redis.

Sistema vulnerable: sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Otros

Otros: todo aquel incidente que no tenga cabida en ninguna categoría anterior.

APT: ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Ciberterrorismo: uso de redes o sistemas de información con fines de carácter terrorista.

Daños informáticos PIC: borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

CONTROLES, HERRAMIENTAS Y MECANISMOS DE MONITORIZACIÓN, IDENTIFICACIÓN, DETECCIÓN Y ALERTA DE INCIDENTES: TIPOS Y FUENTES

IDENTIFICACIÓN

No es fácil en todos los casos determinar con precisión si se ha producido o no un ciberincidente y, si es así, identificar su tipo y evaluar a priori su peligrosidad. Básicamente, los indicios de que nos encontramos ante un ciberincidente pueden provenir de dos tipos de fuentes: los precursores y los indicadores. Un precursor es un indicio de que puede ocurrir un incidente en el futuro. Un indicador es un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.

Algunos ejemplos de precursores podrían ser: Las entradas de log del servidor Web, con los resultados de un escáner de vulnerabilidades; El anuncio de un nuevo exploit, dirigido a una atacar una vulnerabilidad que podría estar presente en los sistemas de la organización; Amenazas explícitas provenientes de grupos o entidades concretos, anunciado ataques a organizaciones objetivo.

Para identificar un incidente de seguridad, determinar su alcance y los sistemas afectados por el mismo, se pueden obtener indicios de múltiples maneras en función de la naturaleza y tipo de incidente. Uno de los principales mecanismos es el análisis de logs, registros y

fuentes de información para detectar anomalías. Sin ánimo de exhaustividad, fuentes de información a considerar en este punto son:

- Consolas de antivirus.
- Sistemas de Detección / Prevención de Intrusión (IDS/IPS).
- Alertas de sistemas de correlación de eventos de seguridad o SIEM.
- Registros de auditoría para detectar intentos de acceso no autorizados.
- Registro de conexiones bloqueadas en los cortafuegos.
- Registro de conexiones realizadas a través de proxys corporativos.
- Registros en herramientas DLP (Data Loss Prevention).
- Bloqueo de cuentas de usuario u otras anomalías reportadas en masa al CAU o que impliquen algún riesgo como pérdidas de USBs o equipos portátiles.
- Consumos excesivos y repentinos de memoria o disco en servidores.
- Anomalías de tráfico como picos de consumo a horas no habituales.
- Volcados de red, mediante port mirroring por ejemplo, que permitan confirmar alguna sospecha de incidente.

La detección de este tipo de anomalías permite identificar un posible incidente de seguridad, así como la naturaleza o el alcance del mismo. En el caso de que alguno de estos registros presentase alguna anomalía, sería necesario su análisis detallado para determinar si realmente existe un incidente.

Este análisis se puede realizar, por ejemplo, mediante la detección de tráfico de red malicioso, identificando la infraestructura afectada, las direcciones de origen y destino, valores de puertos utilizados, TTL, protocolos, etc.

Estas acciones ayudarán a determinar si realmente hay un incidente de seguridad y su naturaleza.

A nivel de sistema, algunos ejemplos para conocer si está siendo afectado por un incidente son:

- Cuentas de usuario inusuales en el sistema o especialmente privilegiadas.

- Ficheros ocultos o con tamaños, nombres o ubicaciones sospechosas, pudiendo indicar los mismos algún tipo de fuga de información o registro por parte de algún malware.
- Ficheros con permisos inusuales, con SUID o GUID en rutas no habituales, ficheros huérfanos y que pudieran determinar algún tipo de intrusión o rootkit.
- Entradas sospechosas en el registro, principalmente en el caso de infecciones por malware en sistemas Windows, donde ésta es una de las principales técnicas que el malware utiliza para asegurar su persistencia en el sistema infectado.
- Procesos y servicios inusuales, no sólo servicios a la escucha, si no con conexiones establecidas a puertos o host extraños, poco habituales o incluidos en algún tipo de lista negra de servidores de Comando y Control (C&C) utilizados por las botnets.
- Cargas excesivas de disco o memoria pueden estar producidas por un incidente de seguridad como malware, denegaciones de servicio o intrusiones.
- Sesiones abiertas en la máquina desde otros equipos, anomalías en las tablas de la base de datos, carpetas compartidas inusuales, o un elevado número de conexiones con algún flag TCP activado de manera anómala y que pudiera evidenciar un ataque de denegación de servicio.
- En el caso de equipos de usuario o terminales móviles, pueden indicar algún tipo de infección en el sistema, entre otros: comportamiento anómalo de alguna aplicación, ventanas emergentes del navegador, conexiones muy lentas, reinicios o aplicaciones que se cierran sin motivo.
- Tareas programadas o actividad sospechosa en los registros de auditoría y logs que indique un funcionamiento anormal del sistema o intentos de intrusión en algún servicio mediante por ejemplo fuerza bruta.
- Reporte del antivirus corporativo o de alguna herramienta habitualmente instalada en el sistema de identificación de rootkits, de control de integridad de ficheros, firma de los binarios, etc. No es recomendable instalar ad hoc estas herramientas en un sistema sospechoso ya que pueden alterar las fechas de acceso de los sistemas y suponer una pérdida de evidencias.

Aunque en la organización se contemplen todas estas medidas para identificar un incidente de seguridad y el equipo o equipos afectados, no es descartable que la identificación del

incidente se produzca a través de una fuente de información externa, un reporte de un CERT o de otro organismo, de un usuario externo a la organización, etc.

