ANEXO N°4

NIVEL DE PELIGROSIDAD Y DESCRIPCIÓN DE TIPO DE INCIDENTE

Clase de incidente	Tipo de Incidente	Descripción	Nivel de peligrosidad
Otros	Amenaza Avanzada Persistente	Una amenaza persistente avanzada (Advanced Persistent Threat o APT) es un ataque cibernético prolongado y dirigido en el que un intruso obtiene acceso a una red y permanece sin ser detectado por un período indeterminado de tiempo. Es realizado a través de distintas técnicas, tácticas y procedimientos como, por ejemplo: webshells, software de comando y control, software de acceso remoto (RAT), malware[1], spam o phishing[2], entre otros. El objetivo de un ataque APT puede ser variado, pero en general lo que se busca es obtener inteligencia y control sobre un grupo de individuos, una nación, gobiernos, instituciones privadas o públicas.	*Crítico*
Contenido abusivo	Pornografía Infantil – Sexual – Violencia	Pornografía infantil, glorificación de la violencia, otros.	*Alto*
	Spam	«Correo masivo no solicitado», lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de un grupo masivo de mensajes, todos teniendo un contenido similar	*Bajo*
	Difamación	Desacreditación o discriminación de alguien	*Medio*
Código malicioso	Malware, Virus, Gusanos, Troyanos, spyware, Dialler, rootkit	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.	*Muy Alto*
Recopilación de Información	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd[3], consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.	*Bajo*
	Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).	*Bajo*
	Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).	*Medio*

[1] Malware es un programa o código malicioso diseñado intencionalmente para causar daño a cualquier clase de dispositivos como computadoras, teléfonos móviles, dispositivos IoT o una infraestructura de red.

[2] Corresponde a una forma de engaño mediante un correo electrónico u otra forma de comunicación, como SMS y apps de mensajería, en la que delincuentes invitan o presionan a las personas a ingresar a un enlace adjunto en el correo o bajar un archivo, con el objetivo de dirigir a una página web fraudulenta, donde la persona se expone a perder información personal, bancaria o comercial, o a descargar un programa malicioso (o malware) en el equipo.

[3] Corresponde a un tipo de recolección de datos que requiere de la interacción con el sistema analizado.

Clase de incidente	Tipo de Incidente	Descripción	Nivel de peligrosidad
Intentos de Intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).	*Medio*
	Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el búfer desbordamiento, puerta trasera, secuencias de comandos cruzadas, etc.).	*Medio*
	Nueva Firma de Ataque	Un intento de usar un exploit[4] desconocido.	*Medio*
Intrusión	Compromiso de Cuenta Privilegiada	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede haber sido causado de forma remota por una vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet[5].	*Alto*
	Compromiso de Cuenta sin privilegios		*Medio*
	Compromiso de Aplicación, Bot		*Alto*
Disponibilidad	Ataque de denegación de servicio (DoS / DDoS)	Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla. Algunos ejemplos de DoS son ICMP e inundaciones SYN, ataques de teardrop[6] y bombardeos de correos electrónicos. Un DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como Ataques de amplificación de DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.	*Alto*
	Sabotaje		*Alto*
	Intercepción de información		*Muy Alto*
Información de seguridad de contenidos	Acceso no autorizado a la información	Además de un abuso local de datos y sistemas, la seguridad de la información puede ser en peligro por una cuenta exitosa o compromiso de la aplicación. Además, son posibles los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro). El error humano / de configuración / software también puede ser la causa.	*Alto*
	Modificación no autorizada de la información		*Alto*
Fraude	Phishing	Enmascarado como otra entidad para persuadir al usuario a revelar una credencial privada.	*Alto*
	Derechos de Autor	Ofrecer o instalar copias de software comercial sin licencia u otros materiales protegidos por derechos de autor (Warez).	*Medio*

[4] Un exploit es un software, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto. Su nombre deriva del verbo inglés to exploit, que significa *"usar algo en beneficio propio"*.

[5] Botnet o botnets es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática.

[6] Teardrop o ataque de goteo, es un tipo de ataque de denegación de servicio (DoS). Los DoS son ataques que intentan poner fuera de servicio un recurso informático inundando la red o el servidor con solicitudes y datos. El atacante envía paquetes fragmentados (por goteo) al servidor meta, y, en algunos casos en los que hay una vulnerabilidad de TCP/IP, el servidor no puede volver a instalar el paquete, lo cual provoca una sobrecarga.

Clase de incidente	Tipo de Incidente	Descripción	Nivel de peligrosidad
	Uso no autorizado de recursos	Usar recursos para fines no autorizados, incluida la obtención de beneficios empresas (por ejemplo, el uso del correo electrónico para participar en cartas de cadena de ganancias ilegales) o esquemas piramidales).	*Medio*
	Falsificación de registros o identidad	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.	*Medio*
Vulnerable	Sistemas y/o softwares Abiertos	Sistemas «Open Resolvers», impresoras abiertas a todo el mundo, vulnerabilidades aparentes detectadas con nessus[7] u otros aplicativos, firmas de virus no actualizadas, etc.	*Medio*
Otros	Todos los incidentes que no encajan en alguna de las otras categorías dadas	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.	*Bajo*
Test	Para pruebas	Producto de pruebas de seguridad controladas e informadas	*Bajo*

[7] Nessus es un programa de escaneo de vulnerabilidades para diversos sistemas operativos.