5 julio, 2019

Matriz de clasificación de incidentes

Matriz de clasificación de Incidentes			
N°	**Clase de Incidente**	**Tipo de Incidente**	**Descripción**
1	Contenido Abusivo	Pornografía Infantil – Sexual – Violencia	Pornografía infantil, glorificación de la violencia, otros.
		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 una grupo masivo de mensajes, todos teniendo un contenido similar
		Difamación	Desacreditación o discriminación de alguien
2	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.
3	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, consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.
		Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
		Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
4	Intentos de Intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
		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.).
		Nueva Firma de Ataque	Un intento de usar un exploit desconocido.
5	Intrusión	Compromiso de Cuenta Privilegiada	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede han 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.
		Compromiso de Cuenta sin privilegios	
		Compromiso de Aplicación, Bot	
6	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 DoS son ICMP e inundaciones SYN, ataques de teardrop y bombardeos de mail’s. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como Ataques de amplificación 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.
		Sabotaje	
		Intercepción de información	
7	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.
		Modificación no autorizada de la información	

8	Fraude	Derechos de Autor	Ofrecer o instalar copias de software comercial sin licencia u otro materiales protegidos por derechos de autor (Warez).
		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).
		Falsificación de registros o identidad	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.
9	Vulnerable	Sistemas y/o softwares Abiertos	Sistemas «Open Resolvers», impresoras abiertas a todo el mundo, vulnerabilidades aparentes detectadas con nessus u otros aplicativos, firmas de virus no actualizadas, etc.
10	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.
11	Test	Para pruebas	Producto de pruebas de seguridad controladas e informadas

Referencia: ENISA

Teatinos 92 piso 6.
Santiago, Chile
csirt.gob.cl