Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1216

(09/2020)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

Requisitos para la obtención y preservación de pruebas de incidentes de ciberseguridad

Recomendación UIT-T X.1216

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1216

Requisitos para la obtención y preservación de pruebas de incidentes de ciberseguridad

Resumen

En la Recomendación UIT-T X.1216 se describe un procedimiento general para la investigación e intervención en caso de incidente de ciberseguridad, se analizan las fuentes de las pruebas de incidentes de ciberseguridad y se especifican las capacidades que han de tener las herramientas empleadas para la obtención y preservación de esas pruebas durante la investigación. En esta Recomendación se especifican también requisitos de garantía de fiabilidad para esas herramientas, así como directrices para los diseñadores de herramientas para tal efecto.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1216	2020-09-03	17	11.1002/1000/14259

Palabras clave

Ciberseguridad, investigación e intervención en caso de incidente, pruebas de incidentes de ciberseguridad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1216

Requisitos para la obtención y preservación de pruebas de incidentes de ciberseguridad

1 Alcance

En esta Recomendación se describe un procedimiento general para la investigación e intervención en caso de incidente de ciberseguridad, se analizan también las fuentes de las pruebas de incidentes de ciberseguridad y se especifican las capacidades que han de tener las herramientas empleadas para la obtención y preservación de esas pruebas durante la investigación. En esta Recomendación se especifican también requisitos de garantía de fiabilidad para esas herramientas, así como directrices para los diseñadores de herramientas para tal efecto.

En esta Recomendación no se contemplan la privacidad ni la reglamentación relativa a la obtención de datos de incidentes de ciberseguridad, procedimientos jurídicos, procedimientos disciplinarios u otras medidas conexas en relación con el tratamiento de posibles pruebas de incidentes de ciberseguridad, pues se consideran fuera del alcance de la "obtención y preservación".

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 obtención [b-ISO/CEI 27037]: Proceso de reunión de los elementos físicos que pueden contener pruebas digitales

3.1.2 prueba [b-UIT-T X.813]: Información que, ya sea por sí misma o utilizada conjuntamente con otra información, puede utilizarse para resolver un litigio.

3.1.3 investigación [b-ISO/CEI 27042]: Realización de exámenes y análisis que ayudan a entender un incidente, y su interpretación.

3.1.4 preservación [b-UIT-R BR.1351]: Operaciones de mantenimiento que deben realizarse para asegurar una conservación adecuada de los materiales, tales como comprobación periódica del estado de deterioro de los medios y regeneración del contenido en nuevos medios cuando sea necesario.

3.1.5 incidente de seguridad [b-UIT-T E.409], [b-IETF RFC 2828]: Cualquier evento adverso que podría amenazar algún aspecto relacionado con la seguridad.

3.1.6 sello de tiempo [b-ISO/CEI 27037]: Parámetro de tiempo variable que indica un instante en el tiempo respecto de una referencia común.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 prueba de incidente de ciberseguridad: Información o datos, almacenados o transmitidos en formato binario, que mediante análisis se ha determinado pertinente para la investigación de un incidente de ciberseguridad.

NOTA – Esta definición se basa en la definición de "prueba digital" de [b-ISO/CEI 27037].

3.2.2 defensa de blanco móvil: Mecanismos que modifican automáticamente uno o más atributos para que la superficie de ataque de un sistema sea impredecible para los adversarios.

NOTA – Esta definición se basa en [b-Jajodia14].

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ARP Protocolo de resolución de direcciones (*address resolution protocol*)

BYOD Traiga su propio dispositivo (*bring your own device*)

DLL Biblioteca de enlaces dinámicos (*dynamic linked library*)

IIP Información de identificación personal

IP Protocolo Internet (*Internet protocol*)

MAC Control de acceso a medios (*media access control*)

MTD Defensa de blanco móvil (*moving target defence*)

PE File Archivo ejecutable portable (*portable executable file*)

WORM Escritura única lectura múltiple (*write once read many*)

5 Convenios

En esta Recomendación:

La utilización del verbo "requerir" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

La utilización del verbo "deber/recomendar" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

6 Aspectos generales de las pruebas de incidentes de ciberseguridad

6.1 Procedimiento general para la investigación e intervención en caso de incidente

Al analizar las causas de un incidente de ciberseguridad, la obtención y preservación de pruebas relacionadas con el incidente es un elemento fundamental de la investigación e intervención en caso de incidente, pues los datos del incidente de ciberseguridad analizados pueden convertirse en pruebas ante los tribunales. Además, las pruebas de incidentes de ciberseguridad reunidas pueden emplearse para examinar las vulnerabilidades y mejorar la ciberseguridad de una organización.

El procedimiento de investigación de incidentes ilustrado en la Figura 1 consta de las siguientes fases secuenciales:

– Preparación: durante esta fase se han de realizar los preparativos preliminares para la investigación del incidente.

– Detección: durante esta fase se observa un evento no autorizado, esto es, un incidente. En función de la gravedad del incidente se tomará una decisión sobre cómo responder al incidente además de obteniendo datos.

– Obtención: se deben recoger datos de las herramientas utilizadas para obtener los datos de tráfico. Esta fase es muy importante, pues los datos de tráfico se intercambian a gran velocidad y no es posible generar los mismos datos de tráfico de red con posterioridad.

– Preservación: los datos de tráfico de red originales se almacenan en un dispositivo de copia de seguridad. También se ha de preservar el generador (hash) de todos los datos.

– Investigación: a lo largo de esta fase se integran todas las pistas recogidas. Se buscan pruebas para identificar ataques. Los indicadores se clasifican y correlacionan para deducir observaciones importantes empleando los patrones de ataque existentes. Puede determinarse el trayecto de ataque, y se puede establecer la identidad del atacante, realizando iterativamente análisis durante esta fase para llegar a una conclusión.

– Información: las observaciones y explicaciones de la investigación se deben presentar en un lenguaje comprensible para el personal jurídico.

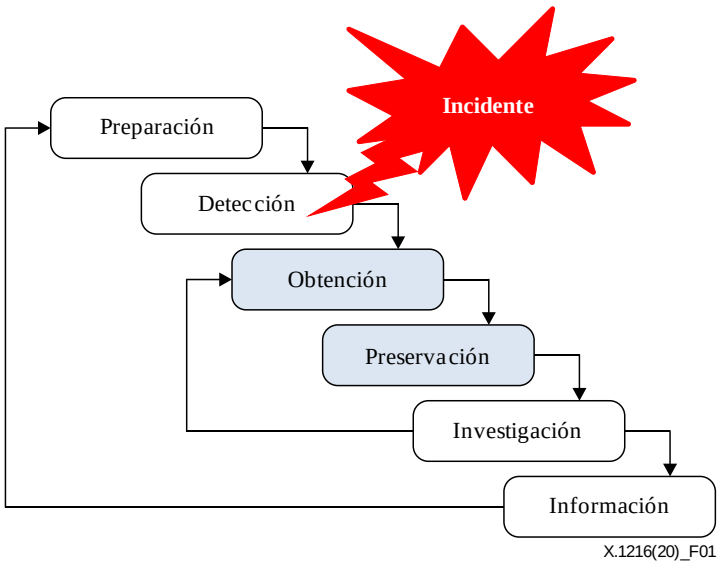

Figura 1 – Procedimiento general de investigación de incidentes

La ISO/CEI tiene directrices normativas sobre investigación digital e intervención en caso de incidente [b-ISO/CEI 27035-3], [b-ISO/CEI 27037], [b-ISO/CEI 27041], [b-ISO/CEI 27042] y [b-ISO/CEI 27043]. Estas directrices se centran sobre todo en las prácticas idóneas y el tratamiento de pruebas digitales a lo largo de todo el procedimiento de investigación. En [b-IETF RFC 3227] también se facilitan directrices para la obtención y el archivo de pruebas, como la preparación y elementos que hay que tener en cuenta durante la obtención; la selección de medios de archivo y la documentación de la cadena de custodia, y las herramientas necesarias para la obtención y el archivo de pruebas. Sin embargo, no se dan directrices claras para la selección o creación de herramientas de investigación.

6.2 Fuentes de datos de incidentes de ciberseguridad

Las fuentes de datos típicas en caso de incidente de ciberseguridad son los dispositivos anfitriones, los dispositivos de seguridad de red, los dispositivos de red y las redes. En la Figura 2 se muestran las categorías de información que se pueden obtener de las fuentes de datos.

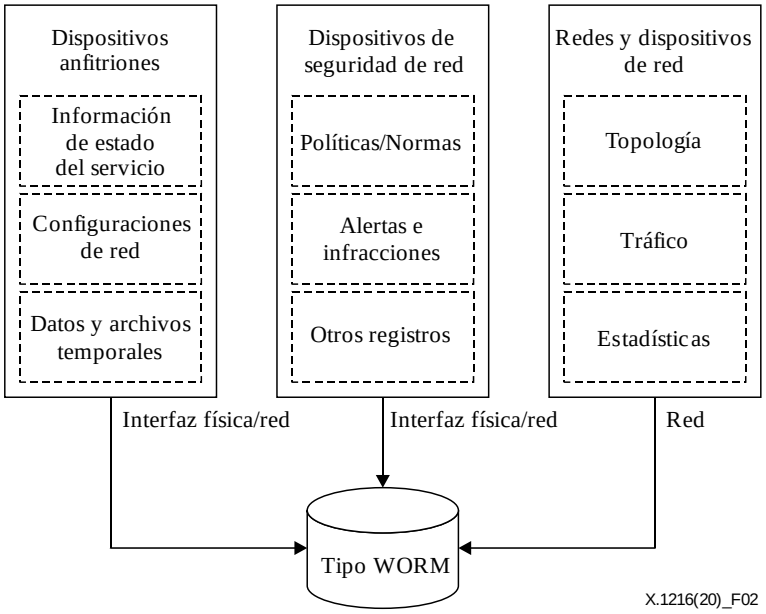

Figura 2 – Diversas fuentes para obtener datos sobre incidentes de ciberseguridad tipo WORM

6.2.1 Dispositivos anfitriones

Por norma general, un dispositivo anfitrión facilita distintos tipos de datos relacionados con incidentes de ciberseguridad. Las herramientas de obtención de datos deben reunir esos datos con cuidado, pues algunos de ellos son volátiles y pueden destruirse con facilidad. A continuación, se indican los tipos de datos que pueden obtenerse de los dispositivos anfitriones:

1) Relacionados con el estado del sistema:
   - Información general (nombre del anfitrión, información de cuenta de usuario, hora y fecha del sistema, hora del último arranque, zona horaria actual, dispositivo de arranque).
   - Información sobre el sistema operativo (fabricante, nombre, arquitectura, versión, número de serie, fecha de instalación).
   - Programas de aplicación (programas instalados, estados de los parches, variables de entorno).
   - Procesos (tabla de procesos, procesos de ejecución automática, servicios calendarizados).
   - Sesión iniciada.
   - Otros datos de registro.
2) Relacionados con los datos y el almacenamiento:
   - Datos de memoria.
   - Sistemas de archivo temporal (archivos recientemente utilizados o ejecutados, incluidos la biblioteca de enlaces dinámicos (DLL, *dynamic linked library*) y los identificadores jerárquicos).
   - Archivos ocultos, archivos ejecutables, archivos abiertos, archivos eliminados, zona no atribuida.

– Medios de almacenamiento.
– Datos compartidos (ficheros compartidos, dispositivos de red).

3) Relacionados con la conexión de red:
– Tabla de encaminamiento, cache del protocolo de resolución de dirección (ARP, *address resolution protocol*), estadísticas del núcleo.
– Configuración de red (direcciones IP, direcciones de control de acceso a medios (MAC, *media access control*), puertos abiertos, interfaces de red).
– Información relacionada con el navegador Internet (historial de navegación Internet, objetos Internet recientemente accedidos, cookies).

6.2.2 Dispositivos de seguridad de red

Los datos relacionados con los ataques deben obtenerse de los dispositivos de seguridad de red, como los sistemas de detección de intrusiones y los cortafuegos.

– políticas de seguridad (control de acceso, reglas de detección);
– eventos y registros de seguridad (alertas, alarmas, avisos, errores);
– información estadística.

6.2.3 Redes y dispositivos de red

Al investigar ciberataques es importante obtener datos de las redes. Concretamente, la información sobre la topología de la red puede ayudar a los investigadores de incidentes de ciberseguridad a entender los componentes y configuraciones de la red de una empresa, descubrir los trayectos de ataque y estimar el alcance de los daños, sobre todo cuando la configuración de red cambia dinámicamente, como ocurre con la computación en la nube, la máquina virtual y traiga su propio dispositivo (BYOD, *bring your own device*), y se emplean tecnologías de seguridad basadas en la defensa de blanco móvil (MTD, *moving target defence*). Como ejemplos típicos de datos de redes y dispositivos de red pueden citarse los siguientes:

– configuración de topología de red;
– registros del encaminador;
– servicios en red;
– información relacionada con el anfitrión de red (puertos abiertos, servicios operativos internos, estado);
– rastros de tráfico, incluidos la cabecera y los datos;
– datos de flujo de sesión (dirección IP/número de puerto fuente, dirección IP/número de puerto destino, protocolo, otra información del encabezamiento TCP);
– archivos transferidos por la red;
– estadísticas de tráfico de red.

7 Requisitos para la obtención de datos de incidentes de ciberseguridad

Cuando ocurre un incidente de ciberseguridad, tan importante como decidir qué datos se han de obtener es decidir cómo obtener, preservar y analizar esos datos. En esta cláusula se describen capacidades para obtener datos de incidentes de ciberseguridad de los tres tipos de fuentes de datos presentadas en la cláusula 6.

En los datos de registro cronológico y de otro tipo sobre el incidente obtenidos de las fuentes de datos puede haber información de identificación personal (IIP). Los implementadores deben limitar la recuperación de IIP al mínimo indispensable para la información e intervención en caso de incidente y proteger la IIP de conformidad con las leyes y reglamentos pertinentes y aplicables.

7.1 Obtención de datos de incidentes de ciberseguridad de dispositivos anfitriones

Los dispositivos anfitriones son normalmente la principal fuente de datos para los análisis de incidentes de ciberseguridad. Ofrecen datos relacionados con los registros, los registros cronológicos y los archivos cargados por el sistema. Cuando se necesite un análisis más detallado, se obtendrá del dispositivo anfitrión una descarga de memoria.

Para ello, las herramientas de obtención deben ser capaces de hacer lo siguiente:

– examinar procesos y obtener información sobre los procesos;
– conocer el estado del sistema;
– hacer copias bit a bit;
– generar imágenes del núcleo;
– automatizar el proceso de obtención;
– importar y exportar los datos obtenidos;
– soportar diversos sistemas operativos de dispositivos anfitrión;
– facilitar las bibliotecas necesarias para la obtención de datos y no utilizar las bibliotecas de los dispositivos anfitriones;
– obtener datos volátiles cuando el sistema está en funcionamiento, y
– conocer el estado de red de la conexión en curso y del conector abierto.

7.2 Obtención de datos de incidentes de ciberseguridad de dispositivos de seguridad de red

De los dispositivos de seguridad de red deben obtenerse numerosos datos útiles para el análisis de incidentes de ciberseguridad, como los sistemas de protección contra intrusiones, los sistemas de detección de intrusiones, los sistemas de prevención de intrusiones, los sistemas cortafuegos y los sistemas de información de seguridad y gestión de eventos.

Para ello, las herramientas de obtención deben ser capaces de hacer lo siguiente:

– obtener registros cronológicos de eventos de los dispositivos de seguridad de red;
– obtener registros cronológicos de alertas e infracciones de los dispositivos de seguridad de red;
– obtener registros cronológicos de autentificación de usuarios de los dispositivos de seguridad de red;
– reunir las políticas y reglas de seguridad de los dispositivos de seguridad de red.

7.3 Obtención de datos de incidentes de ciberseguridad de las redes y los dispositivos de red

La organización obtiene pruebas y supervisa la red para identificar puntos sospechosos de conspiración interna. Si la supervisión del anfitrión no es eficaz, la supervisión de la red puede aumentar la eficacia de las pruebas. El objetivo de la supervisión de la red no es prevenir los ataques, sino obtener información pertinente en caso de incidente y ofrecer muchas más pruebas para el análisis. Para obtener datos de incidentes de seguridad de las redes y los dispositivos de red, las herramientas de obtención de datos deben ser capaces de lo siguiente:

– obtener el tráfico de red sin pérdidas;
– extraer el flujo de sesión de los rastros de red y obtener información sobre ese flujo, como la dirección IP y el número de puerto fuente, la dirección IP y el número de puerto destino, el protocolo IP y la información de servicio, la hora de inicio y fin de la sesión, el número y tamaño de paquetes entrantes, y el número y tamaño de paquetes salientes;

– obtener los archivos ejecutables portables (PE, *portable executable*) transferidos por la red y extraer información de los archivos como el nombre del fichero, el tamaño del fichero, la hora de obtención del fichero, la dirección y el número de puerto fuente de la sesión con el archivo PE, la dirección IP y el número de puerto destino de la sesión con el archivo PE, y el protocolo IP, y
– obtener registros cronológicos de los dispositivos de red, como los encaminadores, los conmutadores y los sistemas de supervisión de la red.

8 Requisitos para la preservación de datos de incidentes de ciberseguridad

Para analizar las causas de un incidente de ciberseguridad es necesario preservar los datos originales obtenidos y evitar que se dañen. Concretamente, cuando haya implicaciones jurídicas, será necesario preservar los datos obtenidos a fin de mantener la integridad y legitimidad de las pruebas. Para ello, las herramientas de preservación deberán ser capaces de lo siguiente:

– generar comprobaciones y firmas digitales;
– validar que los datos obtenidos se preservan sin pérdidas;
– generar sellos de tiempo (en ms) de la hora de obtención y preservación de los datos;
– registrar los datos obtenidos en un dispositivo de escritura única lectura múltiple (WORM, *write once read many*);
– ofrecer el perfil de las políticas de retención de datos que se habrá de respetar;
– asegurar que los datos obtenidos se preservan mientras esté en vigor la política, y
– preservar los datos y metadatos obtenidos de forma formalizada (en [b-UIT-T X.1215] y [b-UIT-T X.1541] pueden encontrarse otras consideraciones sobre esta cuestión).

9 Requisitos de garantía de fiabilidad de las herramientas de obtención y preservación

Los datos obtenidos y preservados con herramientas de obtención y preservación pueden utilizarse para investigar las causas de los incidentes de ciberseguridad y como pruebas para identificar a los responsables del incidente.

Por consiguiente, las herramientas para obtener y preservar datos para analizar incidentes de ciberseguridad deben tener, para garantizar la fiabilidad, las siguientes capacidades de gestión de usuarios y gestión de datos:

– La herramienta debe ofrecer un medio para limitar y controlar el acceso de usuarios a la herramienta misma y a los datos almacenados.
– La herramienta no debe permitir la sobreescritura, la alteración o la supresión de datos conservados sin la adecuada autorización.
– La herramienta debe ofrecer funciones de gestión de seguridad que los administradores autorizados puedan configurar, además de gestionar las funciones de seguridad, las políticas de seguridad y los datos importantes.
– Al transmitir datos obtenidos entre dispositivos físicamente separados, los datos deben encriptarse para garantizar la confidencialidad y la integridad.
– Todos los medios de comunicación asociados con la herramienta deben utilizar un protocolo de comunicación encriptada seguro.
– La herramienta debe ofrecer una función de copia de seguridad de los datos preservados.
– La herramienta debe ofrecer capacidades de registro cronológico, información de errores y auditoría.
– La herramienta debe ofrecer capacidades de procesamiento de metadatos y contenido formalizado y compartirlos de acuerdo con las políticas existentes (como se especifica en [b-UIT-T X.1550] y [b-UIT-T X.1582]).

Bibliografía

[b-UIT-T E.409] Recomendación UIT-T E.409 (2004), *Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones*.

[b-UIT-T X.813] Recomendación UIT-T X.813 (1996), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo*.

[b-UIT-T X.1215] Recomendación UIT-T X.1215 (2019), *Casos de uso del intercambio de información estructurada sobre amenazas*.

[b-UIT-T X.1541] Recomendación UIT-T X.1541 (2017), *Formato para el intercambio de descripciones de objetos de incidentes* (Versión 2).

[b-UIT-T X.1550] Recomendación UIT-T X.1550 (2017), *Modelos de control de acceso para redes de intercambio de incidentes*.

[b-UIT-T X.1582] Recomendación UIT-T X.1582 (2014), *Protocolos de transporte para el intercambio de información de ciberseguridad*.

[b-UIT-R BR.1351] Recomendación UIT-R BR.1351 (1998), *Requisitos para la aplicación de la tecnología digital a los sistemas de archivado del audio en la radiodifusión*.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*.

[b-IETF RFC 3227] IETF RFC 3227 (2002), *Guidelines for Evidence Collection and Archiving*.

[b-ISO/CEI 27035-3] ISO/CEI 27035-3, *Information technology – Security techniques – Information security incident management – Part 3: Guidelines for incident response operations*.

[b-ISO/CEI 27037] ISO/CEI 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*.

[b-ISO/CEI 27041] ISO/CEI 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method*.

[b-ISO/CEI 27042] ISO/CEI 27042:2015, *Information technology — Security techniques – Guidelines for the analysis and interpretation of digital evidence*.

[b-ISO/CEI 27043] ISO/CEI 27043: 2015, *Information technology – Security techniques – Incident investigation principles and processes*.

[b-Jajodia14] Jajodia, Sushil, and Kun Sun. "*MTD 2014: First ACM workshop on moving target defense*." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021