Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1333

(01/2022)

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

Aplicaciones y servicios con seguridad (2) – Seguridad de las redes eléctricas inteligentes

Directrices de seguridad para la utilización de herramientas de acceso remoto en sistemas de control conectados a Internet

Recomendación UIT-T X.1333

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 (1)	X.1140–X.1149
Seguridad de las aplicaciones (1)	
Protocolos de seguridad	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.1350–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.13979
Seguridad de tecnología de libro mayor distribuido (2)	X.1400–X.1429
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad de la web (2)	X.1470–X.1489
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
Ciberdefensa	X.1590– X.1599
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
COMUNICACIONES CUÁNTICAS	
Terminología	X.1700 –X.1701
Generador cuántico de números aleatorios cuánticos	X.1702 –X.1709
Marco de seguridad para QKDN	X.1710 –X.1711
Seguridad de diseño para OKBN	X.1712 –X.1719
Técnicas de seguridad para OKDN	X.1720 –X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de macrodatos	X.1750 –X.1759
Protección de datos	X.1770–X.1789
SEGURIDAD DE LAS IMT-2020	X.1800–X.1819

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

Recomendación UIT-T X.1333

Directrices de seguridad para la utilización de herramientas de acceso remoto en sistemas de control conectados a Internet

Resumen

Las herramientas de acceso remoto (HAR) se utilizan ampliamente en los sistemas de control a efectos de la supervisión, el control y el mantenimiento de dichos sistemas, con el fin de reducir los costes de mantenimiento y minimizar los tiempos de respuesta en caso de mal funcionamiento. Las HAR permiten manipular sistemas de control a distancia, no obstante, al mismo tiempo, una configuración poco segura de estas herramientas o la existencia de vulnerabilidades en las mismas pueden incrementar de manera significativa las posibilidades de que esos sistemas de control sufran ataques. El problema más grave es una interfaz de acceso al sistema de control desde la red externa que pueda permitir a los atacantes acceder al sistema de control desde Internet.

En la Recomendación UIT-T X.1333, se presenta una visión global para la utilización segura de las HAR a efectos de supervisión, control y mantenimiento. Además, se definen diversas amenazas a la configuración de la red inducidas por la utilización de las HAR y se facilitan directrices de seguridad para una configuración segura y una serie de medidas de seguridad con miras a la utilización de las HAR en los sistemas de control conectados a Internet.

El establecimiento de unos controles de seguridad bien organizados con miras a la utilización de las HAR puede resultar útil para los proveedores de servicios digitales que emplean sistemas de control a fin de reducir las posibilidades de ataque y las amenazas provenientes de redes externas. Además, convendría armonizar los niveles de seguridad entre los países desarrollados y en desarrollo, pues este problema no tiene un alcance local, sino mundial.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1333	2022-01-07	17	11.1002/1000/14798

Palabras clave

Directriz, herramienta de acceso remoto, seguridad, sistema de control.

* 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 la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en la presente Recomendación 1
4 Abreviaturas y acrónimos 1
5 Convenios 2
6 Resumen – HAR en sistemas de control conectados a Internet 3
7 Amenazas a la utilización de HAR en sistemas de control conectados a Internet 5
7.1 Amenazas para los clientes HAR 5
7.2 Amenazas a los servidores HAR 6
7.3 Amenazas al canal de comunicación entre el cliente y los servidores 6
8 Directrices para una utilización segura de HAR en sistemas de control conectados a Internet 6
8.1 Directrices de seguridad para los clientes HAR 6
8.2 Directrices de seguridad para los servidores HAR 10
8.3 Directrices de seguridad para las redes 12
8.4 Directrices de seguridad para los registros de auditoría 15
8.5 Relación entre las amenazas a la seguridad y los controles de seguridad 16
Apéndice I – Ejemplo de configuración segura de herramientas de acceso remoto en un sistema energético sostenible 17
I.1 Visión general del sistema 17
I.2 Configuración segura 17
Bibliografía 19

Recomendación UIT-T X.1333

Directrices de seguridad para la utilización de herramientas de acceso remoto en sistemas de control conectados a Internet

1 Alcance

En la presente Recomendación se facilitan directrices de seguridad para la utilización de herramientas de acceso remoto (HAR) en sistemas de control conectados a Internet a través de redes de telecomunicaciones. La Recomendación abarca lo siguiente:

- detección de amenazas a una configuración poco segura de las HAR y sus repercusiones en los sistemas de control conectados a Internet;
- controles de seguridad y su justificación para una configuración segura de las HAR;
- directrices de aplicación para cada control de seguridad; y
- un ejemplo de configuración segura de las HAR en el Apéndice.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utiliza el siguiente término definido en otro documento:

3.1.1 interfaz hombre-máquina (IHM) [b-IEC 61924-2]: Parte de un sistema con la que interactúa un operador. La interfaz es el conjunto de medios que permite a los usuarios interactuar con una máquina, un dispositivo o un sistema. La interfaz proporciona medios de entrada, que permiten a los usuarios controlar el sistema, y de salida, que permiten al sistema informar a los usuarios.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Abreviaturas y acrónimos

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

CAR control de acceso a la red

CCS capa de conexión segura

CLP controlador lógico programable

DDoS ataque de denegación de servicio distribuido (*distributed denial of service*)

DNS servidor de nombres de dominio (*Domain Name Service*)

DoS denegación de servicio (*denial of service*)

ETI estación de trabajo de ingeniería

GDM gestión de dispositivo móvil

GEIS sistema de gestión de eventos e información de seguridad

HAR herramienta de acceso remoto

ICS intérprete de comandos seguro

IHM interfaz hombre-máquina

IPsec seguridad del protocolo Internet (*Internet Protocol security*)

LAN red de área local (*local area network*)

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

MDMS sistema de gestión de datos de medición (*Meter Data Management System*)

MV máquina virtual

NFC comunicación de campo cercano (*near-field communication*)

PIN número de identificación personal (*personal identification number*)

PMCI protocolo de mensajes de control Internet

RFID identificación por radiofrecuencia (*Radio Frequency Identification*)

SCT seguridad de la capa de transporte

SDI sistema de detección de intrusiones

URL localizador uniforme de recursos (*uniform resource locator*)

VPN red privada virtual (*virtual private network*)

ZDM zona desmilitarizada

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

La expresión "**se recomienda**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "**se tiene la opción de**" u "**opcionalmente**" indica que el requisito se permite, sin que ello signifique que se recomiende.

En el cuerpo de la presente Recomendación, ocasionalmente pueden aparecer las palabras "**puede**" o "**pudo**", en cuyo caso deben interpretarse como "**es capaz de**" o "**fue capaz de**".

En el Apéndice I aparecen algunas veces verbos que expresan obligación que no deben interpretarse en sentido normativo.

6 Resumen – HAR en sistemas de control conectados a Internet

Los sistemas de control se emplean con fines industriales, por ejemplo, para producir y transportar materia o energía. Incumbe al sistema de control velar por la consecución del resultado deseado o del rendimiento del objetivo industrial. En aras de la calidad de funcionamiento del sistema de control, una serie de operadores supervisan la información y los datos obtenidos a partir de los sensores de las redes externas (véase la Figura 1). Basándose en los datos y la información antes mencionados, los operadores pueden tomar el control del sistema si es necesario. A efectos del mantenimiento del sistema de control o la resolución de problemas técnicos, los ingenieros de mantenimiento del proveedor del sistema de control pueden acceder al sistema de control.

Las herramientas de acceso remoto (HAR) se utilizan ampliamente en las redes industriales para actividades de supervisión, control y mantenimiento, con el fin de reducir los costes de mantenimiento y minimizar los tiempos de respuesta en caso de mal funcionamiento. Según un informe [b-Kruglov et al.], en el primer semestre de 2018, este tipo de herramientas se emplearon en el 31,6% de los sistemas de control informáticos, excluido el número de conexiones a escritorios remotos.

En la mayoría de los sistemas de control, las HAR suelen utilizarse a fin de:

- supervisar/controlar la interfaz hombre-máquina (IHM) desde un puesto de trabajo de operador;
- supervisar/controlar la IHM desde una estación de trabajo de ingeniería;
- conectar múltiples operadores a una única estación de trabajo de operador;
- conectar varios operadores remotos a una estación de trabajo de operador a través de una red externa; y
- garantizar el mantenimiento del sistema de control conectado a Internet desde la computadora de un ingeniero de mantenimiento del proveedor del sistema de control a través de una red externa.

Estos casos de uso muestran que la utilización de HAR para la supervisión, el control y el mantenimiento de los sistemas de control podría constituir un requisito indispensable para la explotación de dichos sistemas. Además, el empleo de HAR reduciría los costes de mantenimiento. Por ejemplo, en los 3 primeros puntos mencionados *supra*, cabría la posibilidad de reducir el número de licencias para el *software* de la IHM. Además, los dispositivos inteligentes de reciente creación también podrían utilizarse como clientes HAR. En ese sentido, los clientes finales podrían supervisar y controlar sus sistemas fotovoltaicos, por ejemplo, utilizando una HAR en sus teléfonos inteligentes.

La Figura 1 ilustra un tipo de configuración general para la utilización de HAR en sistemas de control conectados a Internet, basado en los citados casos de uso.

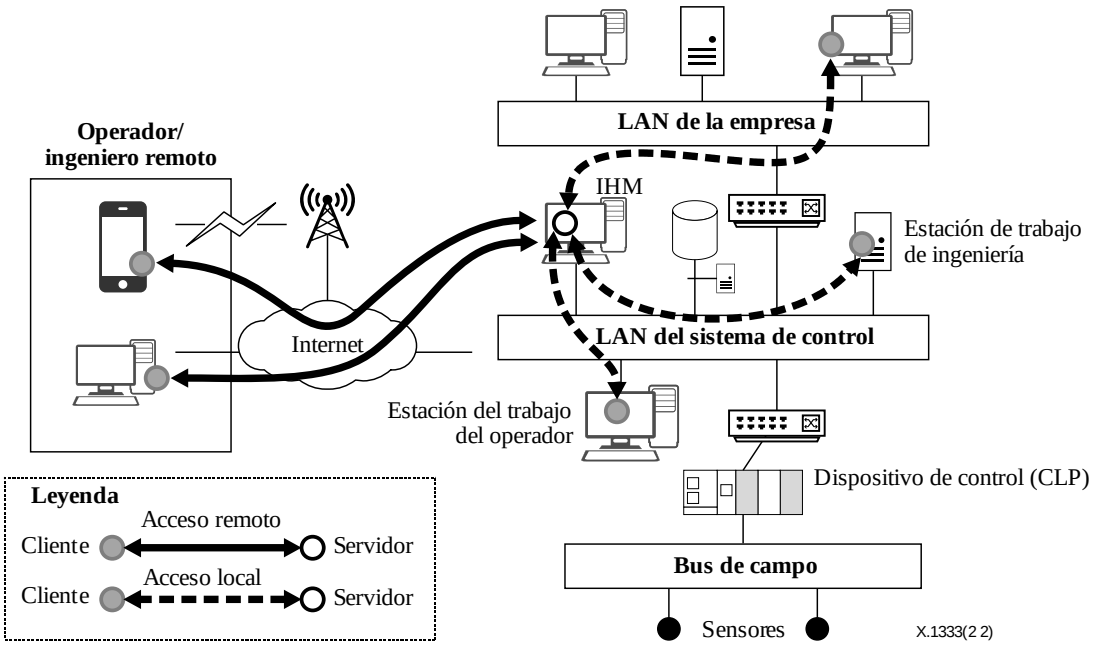

Figura 1 – Configuración de red para la utilización de HAR en sistemas de control conectados a Internet

En otros casos, la organización que explote el sistema de control podría agregar un sistema de control de pequeño tamaño a los sistemas de control legados. Por ejemplo, un centro que explote un generador de energía a gran escala podría emplear un nuevo sistema de pilas de combustible para aumentar su capacidad con energía no contaminante. Los sistemas de pilas de combustible incluyen computadoras dotadas de una IHM, dispositivos de control, sensores, baterías y otros sistemas. Así, en este ejemplo, la IHM y los dispositivos de control podrían conectarse a la misma subred situada en la parte exterior del sistema de pilas de combustible. La Figura 2 ilustra una configuración que permite utilizar las HAR para acceder a la IHM en el exterior.

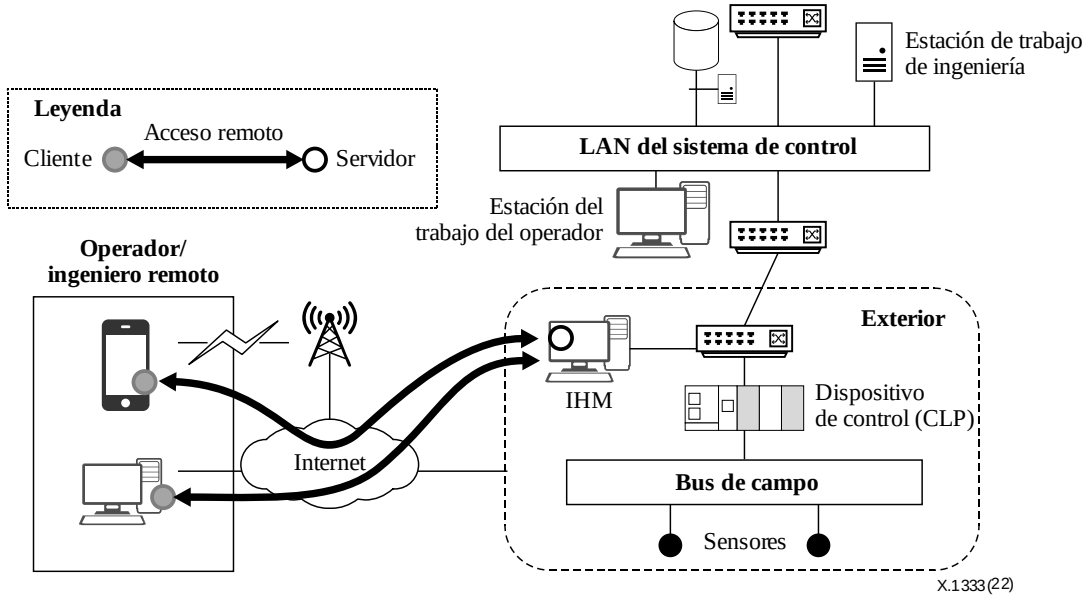

Figura 2 – Configuración de red para la utilización de HAR en una red externa de sistemas de control conectados a Internet

Las HAR permiten manipular sistemas de control a distancia y ayudan a reducir los costes de mantenimiento. Sin embargo, al mismo tiempo, una configuración poco segura de estas herramientas o la existencia de vulnerabilidades en las mismas pueden incrementar de manera significativa las posibilidades de que dichos sistemas sufran ataques. El problema más grave radica en que las HAR pueden utilizarse como interfaz para acceder a un sistema de control conectado a Internet desde las redes externas, a las que normalmente puede accederse desde Internet. De esta forma, una vez que los atacantes acceden a un cliente HAR del sistema de control conectado a Internet, pueden causar fallos en el funcionamiento del sistema en cuestión. Además, es difícil detectar sus actividades. Por consiguiente, esta Recomendación se centra en las conexiones de las HAR desde el exterior de los sistemas de control conectados a Internet.

7 Amenazas a la utilización de HAR en sistemas de control conectados a Internet

7.1 Amenazas para los clientes HAR

El cliente HAR puede instalarse en una computadora cliente en un lugar remoto o en un dispositivo móvil propiedad de un operador remoto o de un ingeniero de mantenimiento remoto. La ubicación remota podría hallarse fuera del radio de protección física de la organización y del radio de protección lógica de su cortafuego. Además, es posible que las computadoras cliente no se gestionen adecuadamente, mientras que las computadoras de las organizaciones se gestionan y blindan con sumo cuidado. Por tanto, muchas de las amenazas inherentes a la utilización de las HAR podrían provenir de las computadoras en las que se instalan los clientes HAR.

En este caso, conviene tener en cuenta las siguientes amenazas a las computadoras cliente y a los clientes HAR:

- (T1) Un atacante podría explotar las vulnerabilidades de las computadoras cliente o de los clientes HAR para causar daños a las computadoras o clientes en cuestión. Una vez que los atacantes se hacen con el control la computadora cliente o del cliente HAR, pueden conectarse al sistema de control a través de la HAR.
- (T2) Un atacante podría explotar la tunelización dividida de una computadora cliente. Las computadoras cliente suelen estar conectados no sólo a los servidores HAR, sino también a otros sistemas conectados a Internet. En consecuencia, si el atacante logra hacerse con el control total de la computadora cliente, puede transmitir información crucial del sistema de control a través de una conexión a Internet desprotegida.
- (T3) Un atacante podría instalar un programa malicioso en una computadora cliente, detectar la información sensible (por ejemplo, el identificador de acceso y la contraseña) y extraerla. Una vez que los atacantes obtienen dicha información, pueden acceder al servidor HAR utilizando un cliente HAR instalado en cualquier otra máquina en lugar de la computadora cliente.
- (T4) Un atacante podría llevar a cabo un ataque de tipo fuerza bruta o de diccionario, o descifrar las contraseñas correspondientes utilizando herramientas de código abierto, para acceder al servidor HAR.
- (T5) Los atacantes podrían ocultar sus actividades en las computadoras cliente borrando los datos de registro. Por esta razón, las organizaciones que explotan los sistemas de control pueden ser incapaces de rastrear las actividades de los atacantes cuando investigan los incidentes.
- (T6) Un atacante podría explotar el acceso físico a las computadoras cliente.

7.2 Amenazas a los servidores HAR

El servidor HAR puede instalarse en una máquina IHM de un sistema de control conectado a Internet. El hecho de que el servidor tenga que abrir un servicio conectado a Internet, brinda a los atacantes la oportunidad de explotar el puerto del servicio. Si el servicio no goza de una protección adecuada, los atacantes podrían acceder al sistema de control a través del servicio en cuestión.

En este caso, conviene tener en cuenta las siguientes amenazas a las computadoras cliente y los clientes HAR:

- (T7) Un atacante podría explotar las vulnerabilidades de un servidor HAR o de la máquina en la que esté instalado dicho servidor para causar daños a la máquina o el servidor en cuestión. Con este tipo de ataque, el atacante podría controlar plenamente el sistema de control. Por ejemplo, una vez que los atacantes lograran acceder a la máquina o al servidor HAR, podrían ampliar sus derechos en el dispositivo o hacerse con el control total del servidor HAR.
- (T8) Un atacante podría llevar a cabo un ataque de tipo DDoS o DoS contra el servidor HAR.

7.3 Amenazas al canal de comunicación entre el cliente y los servidores

Habida cuenta de que el servidor y el cliente HAR están conectados a través de Internet en el marco de un sistema de control conectado a Internet, otras entidades pueden acceder el canal de comunicación. Si las comunicaciones no se encriptan, o se encriptan utilizando métodos deficientes que adolezcan de vulnerabilidades conocidas para el público, los atacantes podrían aprovecharse de ellas y acceder tanto a la información transferida como a los canales.

En este caso, conviene tener en cuenta las siguientes amenazas a las computadoras cliente y los clientes HAR:

- (T9) Un atacante podría aprovechar la falta de protección de la comunicación para obtener información sensible (por ejemplo, el identificador de acceso y la contraseña) y utilizar la información obtenida para acceder al servidor HAR. En los casos en que el sistema criptográfico utilizado para proteger el canal de comunicación es deficiente, los atacantes pueden obtener el mismo resultado. Una vez que logran acceder al servidor HAR, los atacantes pueden llegar a controlar plenamente el sistema de control.
- (T10) Un atacante podría aprovecharse de un protocolo débil que contenga vulnerabilidades conocidas para el público y obtener acceso al servidor HAR o causar una denegación de servicio para los usuarios de los servidores HAR.

8 Directrices para una utilización segura de HAR en sistemas de control conectados a Internet

8.1 Directrices de seguridad para los clientes HAR

8.1.1 Actualización del *software*

Control de seguridad

Conviene mantener actualizados el *software* HAR, el sistema operativo y cualquier otro tipo de *software* del lado del cliente.

Objetivo

El *software* podría adolecer de vulnerabilidades desconocidas, ya que las técnicas de ataque han avanzado. Cuando se anuncia una nueva vulnerabilidad, esta se denomina "vulnerabilidad de día 0". Los atacantes podrían explotar una vulnerabilidad de día 0 para causar daños al dispositivo de cliente HAR. El número de vulnerabilidades relacionadas con el *software* HAR ha aumentado recientemente. En 2019, se detectó un total de 31 vulnerabilidades para la computación de red virtual o el *software*

de tipo red virtual para operadores. Cuando se hace pública una nueva vulnerabilidad, los proveedores de *software* HAR ponen a disposición un parche de seguridad, que los usuarios pueden adoptar para mitigar sus efectos. Mantener el *software* actualizado es una de las formas más fáciles de garantizar la seguridad de los dispositivos cliente.

Directrices de aplicación

Para mantener el *software* actualizado, lo más importante es comprobar periódicamente si existen nuevas actualizaciones. Habida cuenta de que, desgraciadamente, no es fácil garantizar que los usuarios lleven a cabo estas comprobaciones periódicas, debería considerarse el siguiente enfoque para mantener el *software* actualizado de forma automática.

a) El procedimiento de comprobación de las actualizaciones de seguridad debería ponerse en marcha cada vez que se ejecute el *software* de cliente HAR.

b) En caso de detectar una nueva versión del *software* o una nueva actualización de seguridad, esta debería aplicarse al *software* de cliente antes de su ejecución.

c) El procedimiento de comprobación de las actualizaciones de seguridad también puede activarse periódicamente mientras se ejecuta el cliente HAR.

d) En caso de detectar una nueva versión del *software* o una nueva actualización de seguridad, esta debería aplicarse al *software* de cliente cuando el mismo concluya su actividad.

En algunos casos, el dispositivo de cliente HAR debe reiniciarse tras la instalación del parche de seguridad. A diferencia de una computadora cliente típica, un cliente HAR de un sistema de control no puede reiniciarse en cualquier momento, ya que el operador/ingeniero remoto debe realizar un seguimiento constante del sistema de control. En este contexto, el procedimiento de comprobación de actualizaciones de seguridad exige la obtención de la confirmación del usuario antes de instalar las actualizaciones.

También cabría actualizar el sistema operativo y cualquier otro tipo de *software* existente en el dispositivo que ejecuta el *software* de cliente HAR. En ese sentido, conviene habilitar la función de actualización automática de los sistemas operativos. La existencia de actualizaciones de seguridad de las distintas aplicaciones debería comprobarse periódicamente y los parches de seguridad deberían aplicarse tan pronto como estuviesen disponibles.

8.1.2 Integridad del *software*

Control de seguridad

Conviene proteger la integridad del *software* HAR en el lado del cliente.

Objetivo

Cabe la posibilidad de instalar una versión modificada del *software* HAR en el lado del cliente. Un atacante podría poner en peligro el servidor de actualización o distribuir actualizaciones anómalas a través de correos electrónicos de suplantación de identidad. El *software* HAR infectado con un código malicioso se comporta con normalidad, mientras el código en cuestión facilita el filtrado de información o el establecimiento de conexiones con el atacante, en su caso. Por consiguiente, para evitar comportamientos indebidos del *software* HAR malicioso, conviene proteger la integridad del *software* HAR.

Directrices de aplicación

Dado que, como se ha mencionado anteriormente, los atacantes son capaces de distribuir *software* HAR malicioso a través de la cadena de suministro oficial, al usuario no le resulta fácil detectar si el *software* correspondiente ha sido modificado o no. En consecuencia, conviene aplicar el procedimiento de comprobación automática de la integridad, a fin de proteger la integridad del *software* HAR.

En lo que atañe al procedimiento de comprobación automática de la integridad, debe considerarse el siguiente enfoque.

a) El procedimiento de comprobación de la integridad debería ponerse en marcha en el momento en que se ejecutase el *software* o se inicie el procedimiento de actualización.

b) Si nada indica que el *software* haya sido modificado, cabría poner en marcha el *software* o el procedimiento de actualización.

c) El estado del procedimiento de comprobación de la integridad debería mostrarse en la pantalla, para que el usuario supiera que el *software* es normal.

d) El valor de integridad del *software* debería generarse utilizando un método criptográfico, con objeto de garantizar que nadie más haya modificado el *software* en cuestión. En este caso, debería utilizarse un algoritmo criptográfico seguro.

8.1.3 Configuración segura del cliente HAR

Control de seguridad

La configuración del lado del cliente HAR debería ser acorde a la política de seguridad de la organización titular del sistema de control conectado a Internet.

Objetivo

Aunque el *software* HAR ofrece una serie de funciones de seguridad para una comunicación segura, este sólo puede utilizarse de forma segura cuando está configurado adecuadamente. En general, los usuarios prefieren ahorrarse la molestia de habilitar las funciones de seguridad y utilizar una contraseña sólida. Además, en lo que respecta a la seguridad del protocolo Internet, los usuarios no suelen estar al tanto de los detalles de la configuración correcta. Con estos errores de configuración aumentan los posibles abusos del *software* de cliente HAR.

Directrices de aplicación

A fin de reducir los posibles errores en la configuración del cliente HAR, es preferible que la organización que gestiona el sistema de control se encargue de configurarlo. A efectos de la configuración del cliente HAR por dicha organización, deben considerarse los siguientes enfoques.

a) Utilizar un protocolo de Internet (IP) estático para el servidor HAR: Si se utiliza un localizador uniforme de recursos (URL) para acceder a la pasarela de la red privada virtual VPN o al servidor HAR, los operadores/ingenieros remotos pueden verse expuestos a varios ataques, entre ellos, ataques de suplantación de identidad, usurpación del servidor de nombres de dominio (DNS) y envenenamiento de la caché del DNS. El uso de una dirección IP estática o una dirección IP altamente codificada en el lado del servidor permite atenuar estas amenazas y brinda a los operadores/ingenieros remotos la posibilidad de autenticar el servidor en un canal de comunicación seguro.

b) Solución de control de acceso a la red (CAR) o gestión de dispositivos móviles (GDM): La solución CAR permite verificar el estado de una computadora o computadora portátil, mientras que la GDM permite verificar y controlar los dispositivos móviles. Las organizaciones pueden valerse de la primera solución para inducir a los operadores/ingenieros remotos a configurar la computadora en el que se ejecute el cliente HAR, de tal manera que las configuraciones de los dispositivos se verifiquen antes del establecimiento de cualquier conexión. Si un dispositivo está mal configurado, el sistema CAR bloquea el tráfico de red procedente del dispositivo en cuestión hasta que los operadores/ingenieros remotos corrijan los errores en su configuración. Si los operadores remotos utilizan dispositivos móviles para acceder al servidor HAR, se puede optar por la GDN en lugar del CAR.

c) Imagen de máquina virtual (MV): La organización titular del sistema de control puede distribuir una imagen MV entre los operadores/ingenieros remotos. Cuando la organización crea la imagen, todas las configuraciones relacionadas con el dispositivo cliente, el cliente VPN y el cliente HAR deben configurarse con arreglo a la política de seguridad de la organización. Además, para proteger la imagen MV en sí misma, conviene encriptarla y almacenarla en los dispositivos de los operadores/ingenieros remotos siempre que no se esté utilizando.

8.1.4 Control del acceso de los usuarios al dispositivo cliente

Control de seguridad

Sólo los usuarios autorizados deberían poder acceder al *software* de cliente HAR.

Objetivo

Los posibles abusos al cliente HAR podrían reducirse limitando el acceso al *software* de cliente HAR a los operadores/ingenieros remotos autorizados.

No obstante, en el momento en que los operadores/ingenieros remotos legítimos abandonan ese espacio temporalmente para utilizar el *software* HAR, podrían cometerse abusos contra la sesión iniciada. Así pues, cuando los operadores/ingenieros remotos detienen o pausan su trabajo, conviene bloquear el dispositivo. Acto seguido, cuando los operadores/ingenieros remotos regresan frente al dispositivo de cliente HAR, pueden reanudar su labor aplicando el procedimiento de identificación y autenticación establecido.

Directrices de aplicación

Este control puede ejercerse haciendo que los operadores/ingenieros remotos usen una cuenta diferente a la utilizada para realizar las tareas cotidianas a fin de ejecutar el *software* de cliente HAR. En otras palabras, esos operadores/ingenieros remotos deberían disponer de otra cuenta para utilizar el cliente HAR. Además, la contraseña de la cuenta debe ser segura.

Otra forma eficaz de resolver este último problema es bloquear la sesión. Existen dos tipos de bloqueo de sesión: 1) el bloqueo de sesión a nivel del sistema operativo y 2) el bloqueo de sesión a nivel de las aplicaciones. La mayoría de los sistemas operativos permite bloquear la sesión a través de una función que, en principio, debe activarse tras un periodo de inactividad determinado. Depende del software HAR, que difiere en función de si proporciona o no la función de bloqueo de sesión a nivel de las aplicaciones. En consecuencia, cuando la organización que controla el sistema operativo se disponga a elegir el *software* HAR, el hecho de que este último permita el bloqueo de sesión debería figurar entre los principales criterios de selección.

8.1.5 Seguridad física

Requisitos de seguridad

Sólo los operadores/ingenieros remotos autorizados deberían poder acceder físicamente al dispositivo en que se ejecuta el *software* de cliente HAR. Además, el lugar donde los operadores/ingenieros utilizan los dispositivos debería estar protegido contra accesos no autorizados.

Objetivo

Aunque el dispositivo y el *software* de cliente HAR estén configurados de forma segura para utilizar las funciones de seguridad adecuadamente, el dispositivo y el lugar en que se encuentra este último deberían estar protegidos contra el acceso no autorizado de cualquier atacante.

Directrices de aplicación

Con objeto de garantizar la seguridad física de los dispositivos, el *software* y el entorno que los utiliza, conviene tener en cuenta lo siguiente:

a) La oficina en la que trabajan los operadores/ingenieros remotos debería estar protegida por un sistema adecuado de control de acceso a la puerta, que utilice tecnología de comunicación en campo cercano o de identificación por radiofrecuencia. Para una mayor seguridad, podría considerarse la posibilidad de utilizar un sistema de control de acceso biométrico (por ejemplo, mediante huellas dactilares, iris o reconocimiento facial).

b) Debería instalarse una cámara de televisión en circuito cerrado (TVCC) frente a la puerta de la oficina.

c) Los dispositivos en que se ejecute el *software* de cliente HAR deberían estar protegidos contra robos mediante un cable con candado u otros elementos disuasorios.

8.2 Directrices de seguridad para los servidores HAR

8.2.1 Autenticación de usuarios

Control de seguridad

El servicio HAR debería permitir el acceso remoto de los usuarios a los recursos únicamente previa aplicación de un procedimiento de autenticación con dos factores.

Objetivo

Los tradicionales sistemas de autenticación mediante identificador y contraseña pueden quebrantarse y los factores de conocimiento por sí solos, véanse en especial las contraseñas o los números de identificación personal (PIN), no garantizan que el usuario que está accediendo sea la persona titular de los permisos adecuados.

Para el acceso local, los métodos de control de acceso físico permiten identificar a los usuarios legítimos y les brindan acceso a los recursos del sistema. De esta forma, aunque un atacante conozca el identificador y la contraseña de un usuario legítimo, no le resulta fácil acceder directamente a los recursos del sistema. Sin embargo, en lo que atañe al acceso remoto, los métodos de seguridad físicos y los de identificación de usuarios no son fáciles de aplicar. Por tanto, en lugar de recurrir a dichos métodos de seguridad físicos, puede aplicarse un sistema de autenticación con dos factores para reducir las posibles usurpaciones de identidad, incluso en caso de robo del identificador y la contraseña.

Directrices de aplicación

Entre los factores de autenticación pueden figurar algo que sepa (factor de conocimiento), algo que tenga (factor de posesión) o algo que sea (factor inherente) el interesado, así como el lugar en que se encuentre (factor de ubicación). Actualmente, los sistemas de autenticación con dos factores tienden a combinar factores de posesión y de conocimiento, o factores inherentes y de conocimiento.

Últimamente, la mayoría de los dispositivos móviles (por ejemplo, computadoras portátiles, tabletas y teléfonos inteligentes) utiliza métodos biométricos, por lo que los factores inherentes, como la huella dactilar, el iris o el rostro, podrían ser probablemente la mejor opción para estos sistemas.

Sin embargo, en algunas circunstancias, no es posible utilizar métodos biométricos. Por ejemplo, si los usuarios remotos tienen que llevar guantes durante su jornada laboral, conviene evitar la autenticación mediante huella dactilar. En esos casos, pueden aplicarse factores de posesión como los testigos criptográficos.

La mayoría de los *softwares* HAR permiten limitar el tiempo de espera para la autenticación. De esta forma, si el servidor HAR no recibe una respuesta del usuario en un plazo de tiempo determinado, descarta la solicitud de autenticación. De este modo, es más fácil reducir las probabilidades de que se produzcan ataques de denegación de servicio.

8.2.2 Autorización de usuarios

Control de seguridad

Las cuentas de los usuarios remotos sólo deberían disponer de los privilegios estrictamente necesarios para realizar su función.

Objetivo

Para limitar el impacto de un ataque, los usuarios remotos sólo deberían disponer de los privilegios estrictamente necesarios para realizar su función.

Directrices de aplicación

Generalmente, el *software* HAR no prevé un método de autorización pormenorizado. La mayoría de estos *softwares* comprende dos modos, el de "sólo lectura" y el de "control total". De ahí que, si los atacantes logran acceder al servidor HAR, puedan hacerse con el control total del dispositivo. Para evitar esta amenaza, la concesión de privilegios a cuentas de usuarios remotos debería limitarse a los estrictamente necesarios para realizar las funciones correspondientes.

En ese sentido cabe señalar, en primer lugar, que una cuenta de usuario remoto no debería equivaler a una cuenta de administrador, ni poseer ningún privilegio que permita al usuario remoto modificar el servidor HAR. Entre estos privilegios limitados pueden figurar la instalación de *software*, la configuración del sistema operativo y la configuración del sistema.

En segundo lugar, conviene aplicar un sistema de control del acceso a las aplicaciones. La cuenta del usuario remoto no puede ejecutar ningún *software* que no sea el destinado a la explotación y supervisión del sistema de control. Si un usuario remoto puede abrir un programa terminal en la máquina del servidor HAR, es capaz de acceder a otro sistema a través del servidor HAR, lo que brindaría una oportunidad de oro a los atacantes.

8.2.3 Renovación periódica de la autenticación

Control de seguridad

El servidor HAR debería volver a autenticar a los usuarios y dispositivos cliente una vez transcurrido un cierto periodo de tiempo.

Objetivo

Para garantizar que sólo los operadores/ingenieros remotos autorizados puedan utilizar el acceso remoto, el servidor HAR debería exigirles que volvieran a autenticarse periódicamente durante las sesiones de acceso remoto más prolongadas. Este sistema ayudaría a evitar que otras personas no autorizadas utilizasen el acceso remoto, incluso aunque el dispositivo fuera robado en un momento que la conexión entre el servidor HAR y el cliente estuviese activa.

Además, la renovación de la autenticación a nivel de red ayuda a reducir las probabilidades de sufrir un ataque por apropiación de la sesión.

Directrices de aplicación

El *software* del servidor HAR no incluye una función de renovación periódica de la autenticación, pero la mayoría de las pasarelas VPN sí ofrece esta función de seguridad. Por consiguiente, para ejercer ese control de forma adecuada, conviene emplear una VPN entre el cliente y el servidor HAR.

La mayor parte de las pasarelas VPN incluye una función de renovación de la autenticación del cliente. En consecuencia, la organización debería habilitar la función de la pasarela VPN para que los usuarios o dispositivos vuelvan a autenticarse una vez transcurrido un cierto periodo de tiempo. Por ejemplo, cuando la comunicación HAR se lleva a cabo utilizando la versión 1.3 del protocolo de seguridad de la capa de transporte (SCT), la extensión de autenticación del cliente con posterioridad a la primera toma de contacto debería estar habilitada. Si dicha extensión está habilitada, el servidor SCT solicita la autenticación del cliente tras establecer la conexión SCT.

8.2.4 Actualización del *software*

Control de seguridad

Conviene mantener actualizados el *software* del servidor HAR, el sistema operativo y cualquier otro tipo de *software* presente en el dispositivo del servidor.

Objetivo

La finalidad del control descrito en la cláusula 8.2.4 es la misma que la especificada en la cláusula 8.1.1.

Directrices de aplicación

Las directrices correspondientes al control de la cláusula 8.2.4 son las mismas que las especificadas en la cláusula 8.1.1.

8.3 Directrices de seguridad para las redes

8.3.1 Control del acceso a la red

Control de seguridad

Sólo los usuarios legítimos deberían poder acceder a las comunicaciones de red entre el servidor HAR y el cliente HAR.

Objetivo

El acceso a las comunicaciones de red es uno de los primeros pasos para quebrantar un servicio o sistema. De esta forma, los atacantes pueden recopilar parte de la información y los datos transmitidos entre el servidor y el cliente HAR e inyectar datos falsificados en el canal de comunicación, lo que podría desembocar en un ataque por intermediario, de distribución de programas maliciosos o de tipo DoS. Para proteger el servicio HAR y el sistema de control, conviene restringir el acceso de los usuarios malintencionados a las comunicaciones de red entre el servidor HAR y el cliente.

Directrices de aplicación

Existen diversas formas de controlar el acceso a las comunicaciones de red y de proteger su contenido. A tal efecto, puede considerarse la posibilidad de adoptar uno de los siguientes métodos.

- Se puede utilizar una línea alquilada para evitar que los usuarios no autorizados accedan a la conexión entre el sistema de gestión de datos de medición (MDMS)y los proveedores de servicios terceros.
- Deberían aplicarse métodos de comunicación seguros, como IPsec y VPN de la capa de zócalo segura (SSL), a la comunicación entre el cliente y el servidor HAR. El tráfico de las HAR debería tunelizarse a través de una VPN.
- Si no fuese factible utilizar una VPN, el acceso remoto debería realizarse utilizando al menos la versión 1.3 del protocolo SCT.

Cuando se emplee un método de comunicación seguro, como las VPN y los protocolos SCT, debería considerarse la posibilidad de utilizar un algoritmo criptográfico seguro. La norma [b-UIT-T X.1197] incluye una lista de ejemplos de algoritmos y longitudes de clave seguros. Durante la configuración del canal de comunicación, la pasarela VPN o el servidor HAR deberían rechazar las solicitudes de conexión de los clientes que no utilicen algoritmos y longitudes de clave seguros.

8.3.2 Autenticación mutua a nivel de red

Control de seguridad

Conviene aplicar un procedimiento de autenticación mutua en el canal de comunicación entre el servidor HAR y el cliente HAR.

Objetivo

Conviene aplicar un procedimiento de autenticación mutua en los canales de comunicación, de modo que el cliente HAR pueda verificar la legitimidad del servidor HAR antes de proporcionarle las credenciales de autenticación. Gracias a esta función, el servicio HAR puede evitar los ataques por intermediario entre el cliente HAR y el servidor.

Directrices de aplicación

Cuando se emplean métodos como IPsec, SSL VPN o el protocolo SCT en las comunicaciones HAR, la autenticación mutua debería llevarse a cabo en base a los certificados tanto del servidor como del cliente. De esta forma, el cliente puede verificar el certificado del servidor para autenticarlo y asegurarse de que es legítimo.

La mayoría de las soluciones VPN incluye una función de autenticación del servidor, que, en muchos casos, no está habilitada. En consecuencia, cuando un sistema de control emplea una VPN para proteger el servicio HAR, debe habilitar la opción de autenticación del servidor.

Además, en SCT, lo normal es que exista un servidor encargado de autenticar a los clientes verificando sus credenciales, por ejemplo sus certificados, puesto que la autenticación del servidor es una opción. Por tanto, si la comunicación entre el servidor y el cliente está protegida gracias al protocolo SCT para servicios HAR, debería exigirse el intercambio de certificados entre el servidor y el cliente en cuestión.

Por último, conviene habilitar las funciones de limitación del tiempo para la autenticación y del número de sesiones concurrentes. El correcto rechazo de las peticiones de conexión que esperan la respuesta de autenticación del cliente reviste una importancia decisiva para atenuar los ataques de denegación de servicio.

8.3.3 Detección de comportamientos indebidos en la red

Control de seguridad

Conviene aplicar un procedimiento de detección de comportamientos indebidos en la red a la red a la que está conectado el servidor HAR.

Objetivo

Aunque se apliquen varios métodos de seguridad en el lado del cliente HAR, sigue existiendo la posibilidad de que el dispositivo que ejecuta el cliente HAR sufra un ataque. Por ejemplo, si los atacantes logran acceder a la red de un sistema de control conectado a Internet a través de un cliente HAR comprometido, también obtienen acceso a cualquier recurso permitido para el servidor HAR. En este caso, la única diferencia entre los operadores/ingenieros remotos y los atacantes es su comportamiento. Los operadores/ingenieros remotos conocen la red y el sistema al que se conectan, mientras que los atacantes deben emprender una misión de reconocimiento para averiguar dónde se halla el objetivo en la red. En ese sentido, la aplicación de un procedimiento de detección de

comportamientos indebidos en la red, basado en el tráfico de la misma, podría facilitar la detección de ciberataques.

Directrices de aplicación

El procedimiento de detección de comportamientos indebidos en la red debería incluir la supervisión y el examen de todos los mensajes intercambiados entre el cliente HAR y el servidor HAR. Además, el sistema de detección también debería supervisar y examinar todos los mensajes enviados desde el dispositivo en que se ejecuta el servidor HAR a cualquier otro dispositivo del sistema de control conectado a Internet. Por tanto, el sistema de detección debería situarse en la misma subred que el servidor HAR y recopilar datos de tráfico del dispositivo de red que tiene la política de duplicación de puertos activada. Por ejemplo, en una red como la que se muestra en la Figura 2, la política de duplicación de puertos del conmutador de red de la red exterior está habilitada y el sistema de detección recopila datos de tráfico de la interfaz en la que la política de duplicación de puertos está habilitada.

Cuando se aplica un método de comunicación seguro, como IPsec, SSL VPN o la comunicación por SCT, el dispositivo de seguridad que proporciona el canal de comunicación seguro debería situarse en el perímetro de la subred en que se encuentra el servidor HAR. Por ejemplo, conviene ubicar un dispositivo VPN antes que el dispositivo de red, para que el sistema de detección de comportamientos indebidos en la red pueda comprobar todos los paquetes.

Existen tres tipos de procedimientos de detección: la detección estática, la detección de utilización indebida y la detección de anomalías. En el caso de las herramientas de acceso remoto que operan en el entorno, conviene adoptar una combinación de procedimientos de detección de utilización indebida y de detección de anomalías para detectar los ataques tanto conocidos como desconocidos.

8.3.4 Configuración segura de la red

Control de seguridad

La red en la que está instalado el servidor HAR debería estar segmentada y segregada según proceda.

Objetivo

Por segmentación de la red se entiende la división de una red en varias redes más pequeñas, mientras que por segregación de la red se entiende la aplicación de una política para controlar las comunicaciones entre los dispositivos principales. Al separar la red en la que está instalado el servidor HAR de otras redes, se logra evitar que los atacantes accedan a otros recursos del sistema de control incluso aunque hayan logrado quebrantar el servidor HAR.

Directrices de aplicación

La red en la que se instala el servidor HAR debería estar separada de otras redes en el marco del sistema de control, y la comunicación desde/hacia el servidor HAR debería controlarse de acuerdo con las normas típicas de una lista blanca. A fin de aplicar medidas de seguridad de esta índole, puede recurrirse al concepto de zona desmilitarizada (ZDM). En ese contexto, un cortafuegos divide la subred que contiene el servidor HAR y sólo permite las comunicaciones autorizadas, por ejemplo, 1) entre el cliente HAR y el servidor HAR, y 2) entre el servidor HAR y otros recursos del sistema de control, con arreglo a las normas del cortafuegos. También se podría aplicar una lista de control de acceso a nivel de servicio a las normas del cortafuegos. De esta forma, las normas se definirían como una combinación de direcciones IP y números de puerto.

Por ejemplo, un cortafuegos podría separar la IHM de la red externa de los demás recursos de dicha red, según se indica en la Figura 3. El cortafuegos comprueba todos los paquetes desde/hacia el servidor HAR de acuerdo con sus propias normas, las cuales determinan qué servicios del servidor en cuestión pueden comunicarse con qué servicios de otros dispositivos. La comunicación iniciada por un servicio del *software* de la estación de trabajo de ingeniería (ETI) en la IHM puede llegar al

dispositivo de control (representado por el controlador lógico programable (CLP) en la Figura 3). En cambio, el cortafuegos bloquea la comunicación iniciada por el intérprete de comandos seguro (ICS) en la IHM.

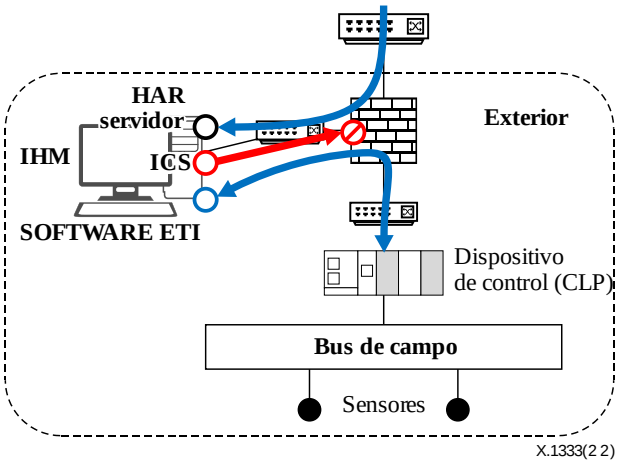

Figura 3 – Segmentación y segregación de la red para el uso de HAR en una red externa

8.4 Directrices de seguridad para los registros de auditoría

8.4.1 Registro

Control de seguridad

Conviene registrar los eventos de seguridad del sistema y de la red, así como proteger los registros en cuestión.

Objetivo

Los registros de eventos de seguridad del sistema y de la red son la piedra angular de la gestión de la seguridad de cualquier sistema. Al revisar y analizar los eventos relacionados con la seguridad, es posible detectar a tiempo diversos problemas de seguridad. Así pues, cuanto más exhaustivos sean los registros de eventos generados por el servidor HAR, más fácil será para la organización detectar los problemas de seguridad.

Directrices de aplicación

Algunos tipos de *software* HAR permiten mantener registros más exhaustivos, que incluyen datos relativos al uso de cada aplicación y a la manipulación de los datos en el dispositivo del servidor, mientras que otros se limitan a registros sencillos, que comprenden datos de conexión y desconexión del servidor HAR. En consecuencia, para elegir el *software* HAR adecuado, las organizaciones deberían tener en cuenta el grado de exhaustividad de los registros de eventos de seguridad generados.

Si el *software* HAR genera registros sencillos, la organización interesada debería considerar la posibilidad de utilizar la función de registro del sistema operativo en que está instalado el servidor HAR. A tal efecto, conviene separar las cuentas de usuario remoto del dispositivo del servidor de las demás cuentas. En este caso, un administrador de seguridad debería revisar los eventos de seguridad registrados por las cuentas de usuario remoto para detectar comportamientos indebidos.

Además del registro de eventos del sistema, también conviene generar un registro de eventos de red. Deberían registrarse todas las solicitudes de conexión HAR y sus resultados (es decir, éxito o fracaso). Del mismo modo, cabría registrar todos los eventos relacionados con los protocolos de conexión remota (por ejemplo, protocolos de terminal, protocolos de control industrial y PMCI). Como se ha mencionado anteriormente, en la primera fase de un ataque, los atacantes suelen emprender una misión de reconocimiento del sistema y, con ese fin, pueden utilizar varios protocolos de conexión

remota. De esta forma, los registros de eventos de red ayudan a los administradores de seguridad a detectar comportamientos indebidos del servidor HAR.

Los registros generados deberían almacenarse de forma segura en el servidor de registros. Si los registros se guardaran en el espacio de almacenamiento local del sistema, los atacantes podrían manipularlos o dañarlos. Por tanto, los registros de eventos deberían almacenarse en un servidor de registros independiente.

El administrador de seguridad debería revisar y analizar el registro periódicamente.

8.5 Relación entre las amenazas a la seguridad y los controles de seguridad

En el Cuadro 4 se muestra la relación entre las amenazas a la seguridad y los controles de seguridad. En este caso, los círculos indican que conviene aplicar un control de seguridad específico para atenuar la amenaza en cuestión.

Cuadro 1 – Relación entre amenazas a la seguridad y controles de seguridad

		7.1 Clientes						**7.2 Servidores**		**7.3 Redes**	
		T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
Clientes	8.1.1 Actualización del *software*	O									
	8.1.2 Integridad del *software*	O	O								
	8.1.3 Configuración segura	O	O	O							
	8.1.4 Control del acceso de los usuarios				O		O				
	8.1.5 Seguridad física						O				
Servidores	8.2.1 Autenticación de usuarios								O		
	8.2.2 Autorización de usuarios						O				
	8.2.3 Renovación periódica de la autenticación						O				
	8.2.4 Actualización del *software*							O			
Redes	8.3.1 Control del acceso a la red									O	
	8.3.2 Autenticación mutua								O	O	
	8.3.3 Detección de comportamientos indebidos					O				O	O
	8.3.4 Configuración segura de la red										O
Auditorías	8.4.1 Registro					O					

Apéndice I

Ejemplo de configuración segura de herramientas de acceso remoto en un sistema energético sostenible

(Este apéndice no forma parte integrante de la presente Recomendación.)

I.1 Visión general del sistema

En los generadores, hay instalados numerosos sensores y accionadores. Los sensores proporcionan datos medidos a los dispositivos de control (véase el CLP de la Figura I.1) y los operadores supervisan el estado de los generadores basándose en dichos datos, a través de la IHM o la estación de trabajo de ingeniería. En función del estado, los operadores controlan los accionadores a través de la IHM (o la estación de trabajo de ingeniería) y el CLP. Por ejemplo, cuando llega un tifón, los operadores proceden a detener la rotación de las aspas del generador eólico. La red que conecta los sensores, accionadores y dispositivos de control se denomina *red externa*. En la red externa, suele instalarse una IHM para la supervisión y el control de los generadores.

En algunos casos, los generadores que utilizan recursos energéticos sostenibles, como el viento (turbinas eólicas), el hidrógeno (pilas de combustible) y la energía solar (sistemas fotovoltaicos), son gestionados por operadores remotos. Los operadores remotos supervisan el estado de los generadores y los controlan para generar electricidad de forma eficiente.

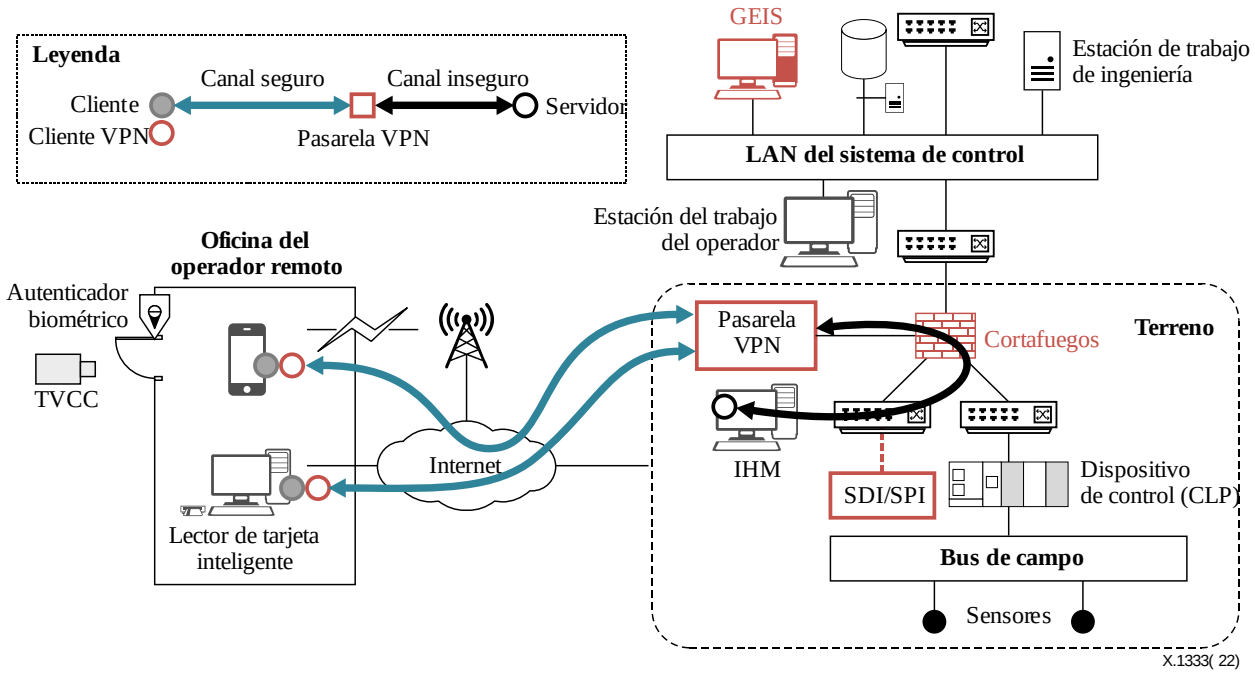

Figura I.1 – Ejemplo de red segura para un sistema de control de recursos energéticos sostenibles

I.2 Configuración segura

La Figura I.1 ilustra un ejemplo de configuración de red segura para un sistema energético sostenible. A continuación, se describen diversas medidas de seguridad para cada componente, incluidos el cliente HAR, el servidor HAR, la red y el registro de eventos de seguridad.

I.2.1 Cliente HAR

En primer lugar, se crea una cuenta independiente para el cliente HAR, que constituirá el único medio de acceso al *software* de cliente.

Cada vez que un operador remoto pone en marcha el *software* de cliente HAR, se inician los procesos de comprobación de actualizaciones y comprobación de la integridad. En su caso, las actualizaciones se instalarán antes de ejecutar el *software* de cliente HAR.

El cliente CAR comprueba el nivel de seguridad del dispositivo y bloquea la conexión a Internet si falta alguna configuración de seguridad. Por ejemplo, si el *software* antivirus y el cortafuegos personal no están activados, el CAR no permite ninguna conexión de comunicación.

Todos los dispositivos que ejecutan el cliente HAR se gestionan en la oficina de los operadores remotos. El control de acceso a la oficina se lleva a cabo con ayuda de un autentificador biométrico (por ejemplo, huella dactilar o reconocimiento facial) y un sistema de TVCC instalado frente a la puerta de la oficina.

I.2.2 Servidor HAR

Cuando los operadores remotos intentan establecer una conexión HAR a través del cliente HAR, se activa el procedimiento de autenticación con dos factores (es decir, contraseña y tarjeta inteligente). Además, se utilizan direcciones IP estáticas para la pasarela VPN y el servidor HAR.

Antes de la autenticación mutua, el dispositivo principal que solicita la conexión se somete a un procedimiento de filtrado basado en su dirección IP y su dirección de control de acceso a medios (MAC) en la pasarela VPN. Además, el canal de comunicación entre el cliente VPN y la pasarela VPN se mantiene activo durante 8 horas. De esta forma, para mantener la conexión VPN, los operadores remotos deben facilitar su contraseña e introducir tarjeta inteligente cada 8 horas.

En la IHM, las cuentas de los operadores remotos están separadas de las demás cuentas, a fin de limitar los permisos de dichos operadores y generar registros exhaustivos para las cuentas.

I.2.3 Red

La VPN con IPsec protege el canal de comunicación entre el cliente y el servidor HAR. Antes de conectarse al servidor HAR, el cliente VPN instalado en el dispositivo del operador remoto debería establecer un canal seguro con una pasarela VPN. Para garantizar el nivel mínimo de seguridad de 128 bits, se utiliza la serie criptográfica, *Suite-B-GCM-256*, para VPN con IPsec, según se indica en [b-IETF RFC 6379]. A efectos de la autenticación IKEv2, se aplica *ECDSA-256* para VPN con IPsec, según se indica en [b- IETF RFC 6380]. Para lograr un equilibrio entre seguridad y sobrecarga, el protocolo IKE SA permanece activo durante 24 horas y el IPsec SA durante 8 horas.

En el exterior, la red se divide en dos segmentos, que se componen de una ZDM para la IHM y una red externa para los CLP, los sensores y los accionadores. Además, existe un cortafuegos entre la red de área local (LAN) del sistema de control, la red exterior y la ZDM para la segregación de la red. De este modo, la comunicación de la ETI en la IHM puede transferirse a la red exterior, pero el cortafuegos bloquea cualquier otro tipo de tráfico procedente de la IHM y destinado a cualquier otra red.

En la ZDM se instala un sistema de detección de intrusiones (SDI) o un sistema de prevención de intrusiones (SPI), que recibe el tráfico de red entrante y saliente desde un puerto de conmutador configurado para la duplicación del tráfico.

I.2.4 Registro de eventos de seguridad

Los eventos de seguridad generados por las cuentas de acceso remoto se registran en el sistema IHM y se transmiten al sistema de gestión de eventos e información de seguridad (GEIS). El administrador de seguridad de la organización que gestiona el sistema energético sostenible examinará los registros periódicamente utilizando el sistema GEIS.

Bibliografía

[b-ITU-T X.1197] Recomendación UIT-T X.1197 (2012), *Directrices sobre criterios para la selección de algoritmos criptográficos para la protección de los servicios y contenidos de TVIP*.

[b-IEC 61924-2] IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems – Integrated navigation systems – Part 2: Modular structure for INS – Operational and performance requirements, methods of testing and required test results.*

[b-RFC6379] RFC 6379 (2011), *Suite B Cryptographic Suites for IPsec.*

[b-RFC6380] RFC 6380 (2011), *Suite B Profile for Internet Protocol Security (IPsec).*

[b-Kruglov et al.] Kirill Kruglov, Evgeny Goncharov (2018), *Threats posed by using RATs in ICS*, Technical Report, Kaspersky Lab ICS CERT. https://ics-cert.kaspersky.com/reports/2018/09/20/threats-posed-by-using-rats-in-ics/

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, 2022