ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1382 (03/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Aplicaciones y servicios con seguridad (2) – Seguridad en los sistemas de transporte inteligentes (STI)

Directrices para el intercambio de información sobre amenazas de seguridad en vehículos conectados

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	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)	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.1319
Seguridad de las redes eléctricas inteligentes	X.1330-X.1339
Correo certificado	X.1340-X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350-X.1369
Seguridad en los sistemas de transporte inteligente (STI)	**X.1370-X.1399**
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400-X.1429
Seguridad de las aplicaciones (2)	X.1450-X.1459
Seguridad en 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
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
Protección de los datos	X.1770-X.1789
SEGURIDAD EN LAS REDES IMT-2020	X.1800-X.1819

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

Recomendación UIT-T X.1382

Directrices para el intercambio de información sobre amenazas de seguridad en vehículos conectados

Resumen

Con su veloz desarrollo, los vehículos conectados afrontan retos de seguridad de red cada vez más notables. La información sobre amenazas de seguridad de los vehículos conectados, que desempeña un papel esencial en la protección de dichos vehículos, es toda aquella que permite a una organización identificar, evaluar, supervisar y responder a un vehículo conectado. Las organizaciones que intercambian información sobre amenazas de seguridad para vehículos conectados pueden mejorar sus propias condiciones de seguridad, así como la de otras organizaciones.

La Recomendación UIT-T X.1382 proporciona orientación sobre los principios, las normas, la metodología y los procedimientos de intercambio de información de seguridad para vehículos conectados. También facilita una breve descripción de los diferentes cometidos, funciones y niveles de eficacia de las múltiples organizaciones que participan en el ciclo de vida del intercambio de información sobre amenazas de seguridad.

La Recomendación tiene como objetivo ayudar a las organizaciones a que se mantengan al corriente con la comunidad de intercambio de información sobre vehículos conectados, y también a que contribuyan con información sobre amenazas que fomente las prácticas de protección y seguridad de los vehículos conectados. De forma general, esta Recomendación pretende mejorar el intercambio de información sobre amenazas de seguridad y mitigar las potenciales repercusiones de los ataques a la ciberseguridad en vehículos conectados.

Historia *

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	ITU-T X.1382	2023-03-03	17	11.1002/1000/15104

Palabras clave

Intercambio de información sobre amenazas, vehículos conectados.

* 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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, 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 patentes/derechos de autor de *software*, 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 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

Recomendación UIT-T X.1382

Directrices para el intercambio de información sobre amenazas de seguridad en vehículos conectados

1 Alcance

El objetivo de esta Recomendación es facilitar directrices relativas al intercambio de información sobre amenazas en los entornos de los vehículos conectados, incluidas las funciones y asociaciones de las organizaciones, los niveles de alcance del intercambio, los procedimientos y los requisitos para el intercambio de información sobre amenazas en vehículos conectados.

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.

[UIT-T X.1371] Recomendación UIT-T X.1371 (2020), *Amenazas a la seguridad de los vehículos conectados.*

[NIST SP 800-150] *Guía de intercambio de información sobre ciberamenazas.*

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 alerta [NIST SP 800-150]: Una notificación técnica breve, por lo general legible por humanos, en relación con vulnerabilidades, intentos de explotación y otros problemas de seguridad. También se denomina "aviso", "boletín" o "nota de vulnerabilidad".

3.1.2 información sobre amenazas de seguridad [NIST SP 800-150]: Información relativa a una amenaza que puede ayudar a una organización a protegerse contra una amenaza o a detectar las actividades de un actor.

3.1.3 amenaza [b-ISO/CEI 27000]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 tácticas del actor: Descripciones de los objetivos técnicos de un actor para ejecutar una acción.

3.2.2 técnicas del actor: Descripciones de cómo un actor alcanza los objetivos técnicos mediante la ejecución de una acción.

3.2.3 procedimientos del actor: Descripciones de la aplicación de una técnica específica del actor.

4 Abreviaturas y acrónimos

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

ACL Lista de control de acceso (*access control list*)

APP Aplicación (*application*)

ECU Unidad de control electrónico (*electronic control unit*)

EIEI Equipo de intervención en caso de emergencia informática

EIISI Equipo de intervención en caso de incidente de seguridad informática

GSMA Asociación GSM (*GSM association*)

ISAC Centro de Análisis e Intercambio de Información (*information sharing and analysis center*)

MEC Computación periférica multiacceso (*multi-access edge computing*)

T-BOX Caja telemática (*telematics BOX*)

TSP Proveedor de servicios telemáticos (*telematics service provider*)

TTP Tácticas, técnicas y procedimientos

V2X Vehículo a su entorno (*vehicle-to-everything*)

5 Convenios

En esta Recomendación:

La expresión "se recomienda" indica que un requisito está recomendado, pero que no es absolutamente obligatorio. Por ende, su cumplimiento no es indispensable para poder declarar la conformidad.

6 Generalidades

Entre los elementos principales del intercambio de información sobre amenazas en vehículos conectados se incluyen los tipos de información sobre amenazas y los principios, las funciones, las normas, las comunidades y los procedimientos de intercambio. Por lo general, distintas organizaciones de vehículos conectados generan distintos tipos de información sobre amenazas de seguridad. Diferentes tipos de agentes desempeñan diversas funciones en las actividades de intercambio de información sobre amenazas en vehículos conectados. Las actividades de intercambio de información sobre amenazas en vehículos conectados entre organizaciones deben seguir ciertos principios, normas y procedimientos. Por su parte, la información sobre amenazas tiene efectos diferentes. Varias organizaciones pueden formar una comunidad de intercambio con arreglo a un cierto modo de intercambio y en torno a una plataforma para tal fin.

6.1 Tipos de información sobre amenazas en vehículos conectados

Tomando como referencia el documento [NIST SP 800-150], la información sobre amenazas en vehículos conectados puede clasificarse de la siguiente manera: indicadores, tácticas, técnicas y procedimientos (TTP), alertas de seguridad e informes de inteligencia sobre amenazas:

a) Los indicadores son signos observables de que un ataque es inminente o está en curso. Es posible valerse de los indicadores para detectar potenciales amenazas y actuar contra ellas. Entre los indicadores de los vehículos conectados se encuentran las organizaciones de supuestos atacantes a comunicaciones entre vehículos y su entorno (V2X).

b) Los TTP describen el comportamiento de un actor. Los TTP pueden describir la tendencia de un actor a utilizar una variante de programas malignos, una secuencia de operaciones, una herramienta de ataque, un mecanismo de entrega o un sistema de explotación específicos. Existen diversos tipos de amenazas, entre las que se encuentran las que afectan al servidor principal y los servidores de soporte, y también las que afectan a los vehículos en relación con sus canales de comunicación. Los TTP pueden incluir acciones para manipular la conectividad de las funciones de los vehículos o para eludir el sistema de supervisión, por lo que difieren de las amenazas de red tradicionales.

c) Las alertas de seguridad son notificaciones técnicas sobre vulnerabilidades, abusos, programas malignos y otros problemas de seguridad. Las alertas de seguridad suelen generarse en fuentes de reputación reconocida, como los equipos de intervención en caso de emergencia informática (EIEI) y los equipos de intervención en caso de incidente de seguridad informática (EIISI). Las alertas de seguridad se emiten cuando los vehículos conectados afectados son de diversa índole o cuando las amenazas tienen el potencial de causar daños de envergadura.

d) Los informes de inteligencia sobre amenazas facilitan el análisis en profundidad de las amenazas, comprenden los participantes en el evento, el sistema objetivo, el tipo de ataque y otros tipos de información, y aconsejan sobre las acciones necesarias para mitigar las amenazas. Los informes de inteligencia sobre amenazas también pueden mostrar las tendencias futuras de éstas. Los informes de inteligencia sobre amenazas desempeñan un importante papel en la prevención de la aparición de nuevos ataques a vehículos conectados.

6.2 Ventajas y retos del intercambio de información sobre amenazas en vehículos conectados

Por medio de la información compartida sobre amenazas en vehículos conectados, las organizaciones relacionadas con este sector pueden aprovechar de manera proactiva los conocimientos, la experiencia y las capacidades de sus socios para mejorar su posición de seguridad. Entre las ventajas del intercambio de información sobre amenazas en vehículos conectados se encuentran las siguientes:

a) Mejora de la capacidad de defensa de las organizaciones de vehículos conectados: los vehículos conectados implican nuevas amenazas, mientras que el intercambio de información puede ayudar a las organizaciones a mejorar sus capacidades de defensa contra tales amenazas. Las nuevas vulnerabilidades suelen aprovecharse como herramienta primaria para los ataques. El intercambio de información sobre amenazas permite abordar a tiempo los ataques asociados a las nuevas vulnerabilidades, así como mejorar la capacidad de defensa ante los ataques. Si bien los vehículos conectados se enfrentan a multitud de ataques nuevos, el intercambio de información sobre amenazas contribuye a enfrentarse a las nuevas amenazas que afectan a los vehículos conectados y mejora la capacidad de defensa.

b) Mantenimiento del buen estado del ecosistema de vehículos conectados: el intercambio de información sobre amenazas contribuye a promover la seguridad del entorno económico de los vehículos conectados y a establecer una seguridad ecológica para todos ellos. La seguridad de la cadena de fabricación de vehículos conectados incluye la seguridad de los proveedores de servicios, los proveedores de servicios telemáticos (TSP), los fabricantes de vehículos, los operadores de telecomunicaciones, los proveedores de equipos de terminales móviles y en vehículos, los proveedores de equipos terminales inteligentes móviles, etc.

Aunque el intercambio de información sobre amenazas presenta ventajas, no está exento de problemas. Entre ellos, se encuentran los siguientes:

a) Establecimiento de un sistema estándar de intercambio de información sobre amenazas en vehículos conectados: para mantener el buen estado del ecosistema de vehículos conectados, es necesario formular un sistema estándar razonable para el intercambio de información sobre las amenazas que les afectan. Por el momento no existe un sistema estándar internacional

unificado para el intercambio de información sobre amenazas en vehículos conectados. Si no se establece un sistema estándar, el intercambio de información se verá obstaculizado y su desarrollo podrá verse afectado en último término.

NOTA – Algunas directrices, como [UIT-T X.1371] y las directrices de seguridad IoT de la GSMA [b-GSMA CLP.11], pueden establecer que las cuestiones de seguridad se consideren posibles prácticas idóneas en materia de intercambio de información.

b) Definición del alcance de la información sobre amenazas: la cadena industrial de los vehículos conectados se compone de diversos eslabones, cada uno de los cuales afronta distintos tipos de amenazas. Es necesario definir el nivel de intercambio de información sobre amenazas para cada eslabón, así como el modo de intercambio de información entre distintos eslabones.

c) Protección de la información sensible y clasificada: el intercambio de información sobre amenazas en vehículos conectados está expuesto al riesgo de divulgación de información sensible. Las tecnologías criptográficas pueden quedar comprometidas o aplicarse de manera insuficiente. El uso insuficiente de tecnologías criptográficas puede dar lugar a una filtración de claves criptográficas o credenciales.

Además, el riesgo de filtración de información puede acrecentarse con el uso de tecnologías criptográficas ya quebradas u obsoletas. Entre los datos sensibles que deben protegerse se encuentran: los derechos de autor o *software* patentado del vehículo; la información privada del propietario, como datos personales, información de la cuenta de pago, información del libro de direcciones, información de localización y el identificador electrónico del vehículo, además de las claves criptográficas, entre otros. Por otra parte, no se permite el acceso de organizaciones no autorizadas a la información clasificada. Los procesos de obtención y mantenimiento de los permisos necesarios para el acceso continuo a las fuentes de información clasificada son costosos para las organizaciones y requieren mucho tiempo.

7 Principios de intercambio de información sobre amenazas en vehículos conectados

Para garantizar la efectividad, la precisión y la seguridad de los procesos de intercambio y transmisión de la información sobre amenazas de seguridad, es necesario que las organizaciones y las empresas adhieran a ciertos principios.

7.1 Beneficio mutuo

La esencia del intercambio de información sobre amenazas de seguridad es la mejora de las capacidades de protección de la seguridad de la red en vehículos conectados a través de esfuerzos colaborativos. Se recomienda que las partes que participan en el intercambio de información sobre amenazas de seguridad en vehículos conectados conozcan los derechos, las obligaciones y las responsabilidades que para todas ellas entrañan las actividades de intercambio de información. También se recomienda a las organizaciones que, además de recibir la información sobre amenazas que les concierne individualmente, contribuyan activamente con sus propios esfuerzos en pro de un beneficio mutuo y para generar situaciones favorables para todas las partes.

7.2 Categorización y clasificación

Cada organización desempeña una función distinta en el proceso de intercambio de información sobre amenazas de seguridad. El significado y la importancia de una información sobre amenazas dada pueden ser diferir para cada organización. Se recomienza a cada organización que categorice y clasifique la información sobre amenazas en vehículos conectados, y que defina su alcance efectivo. Asimismo, se recomienda el establecimiento de distintos niveles en el sistema de gestión en función del tipo de categorización, clasificación y alcance, así como el uso de un sistema criptográfico apropiado para mantener la confidencialidad y la integridad de la información confidencial y/o para proteger su autenticidad.

7.3 Seguridad de los datos

Problemas como el uso ilegal, el robo y la manipulación de los datos sobre amenazas, así como el acceso de usuarios no autorizados, afectan gravemente a las iniciativas de las partes que comparten datos para el intercambio de información y reducen la seguridad y la eficacia de estas actividades. Por este motivo, el intercambio de información sobre amenazas también se centra en el control de los riesgos asociados al intercambio mismo. Las medidas para contrarrestar los riesgos, como la criptografía, la desensibilización de los datos compartidos, su identificación y destrucción, etc., son eficaces para proteger los datos en el marco de la seguridad de la información sobre amenazas en vehículos conectados.

8 Organizaciones, funciones y asociación

8.1 Organizaciones y sus funciones

8.1.1 Fabricantes de automóviles

Los fabricantes de automóviles desempeñan la función más importante en el marco de las actividades de intercambio de información sobre amenazas en vehículos conectados, ya que interactúan directamente con los usuarios y son los responsables de la seguridad de sus vehículos.

A través de la recogida de datos de sus propios sistemas de producción, los componentes de a bordo y la infraestructura de los vehículos conectados, los fabricantes de automóviles recogen, integran, producen y analizan información sobre amenazas de seguridad en relación con los vehículos conectados y toman medidas para mitigar las amenazas.

8.1.2 Proveedores

Los proveedores suministran *hardware* o *software* intravehicular para vehículos conectados, lo que incluye chips para vehículos, equipos de cajas telemáticas (T-BOX, *telematics BOX*) y pasarelas internas o externas. Los proveedores recogen y reciben información sobre amenazas a la seguridad de sus productos y ayudan al equipo de coordinación, a los fabricantes de automóviles y a otras partes pertinentes a mitigar las amenazas y/o a prevenir y reducir los incidentes de seguridad que afectan a sus productos.

8.1.3 Proveedores terceros de productos y servicios

Los proveedores terceros de productos y servicios son principalmente aquellas organizaciones que suministran productos y servicios independientes asociados a los vehículos conectados, más allá de los fabricantes de vehículos y sus propios proveedores de componentes; entre ellos, se encuentran los proveedores de servicios telemáticos (TSP, *telematics service provider*), los proveedores de servicios de computación en la nube, los vendedores de *hardware*, los fabricantes de terminales móviles, los proveedores de servicios de seguros de vehículos, otros operadores de plataformas de servicios terceros, etc.

Los proveedores de productos y servicios terceros recogen, producen y comparten información sobre amenazas de seguridad que afectan a sus productos o plataformas de servicios, como la información sobre amenazas de fallos de funcionamiento de los vehículos conectados, comportamientos no autorizados del usuario o ataques a distancia, y ayudan a las partes pertinentes, como los equipos de coordinación para vehículos conectados y los fabricantes de automóviles, a mitigar las amenazas y/o gestionar los incidentes de seguridad en los vehículos conectados. Los proveedores de servicios de computación en la nube, además, son responsables del intercambio de información relativa, entre otras cosas, a errores o configuraciones erróneas, abusos de los puertos de control, gestión inapropiada de credenciales, fugas de datos en la nube, etc.

8.1.4 Equipo de coordinación

Los equipos de coordinación para vehículos conectados, como los EIEI/EIISI o el Auto-ISAC, suelen funcionar como entidades independientes que se centran en la coordinación de la información sobre amenazas de seguridad y la respuesta a incidentes.

Los equipos de coordinación para vehículos conectados asisten a las partes pertinentes en la coordinación entre organizaciones del intercambio de información sobre amenazas de seguridad y les ofrecen servicios de notificación y alerta temprana.

8.1.5 Operadores de telecomunicaciones

Los operadores de telecomunicaciones ofrecen servicios básicos de telecomunicaciones para vehículos conectados.

Garantizan la seguridad de la infraestructura de la red de telecomunicaciones, como las redes básicas, las estaciones base, las plataformas de computación periférica multiacceso (MEC, *Multi-access Edge Computing*), etc.

NOTA – Como ejemplo de operadores de telecomunicaciones en el contexto de los vehículos conectados, se pueden tener en cuenta las directrices de la GSMA para operadores de redes [b-GSMA CLP.14].

8.1.6 Proveedores de ciberseguridad

Los proveedores de ciberseguridad son empresas u organizaciones vinculadas a la red e implicadas en las empresas u organizaciones de vehículos que ofrecen servicios o productos de ciberseguridad.

A través de fuentes como dispositivos de seguridad, *software* de terminales o Internet, los proveedores de ciberseguridad asisten a las organizaciones pertinentes en la recogida, la integración y el análisis de la información sobre amenazas de seguridad en los vehículos conectados, y ofrecen servicios y soporte de seguridad para prevenir y reducir los incidentes de seguridad.

8.2 Alcance del intercambio entre organizaciones

Se recomienda a las organizaciones que definan el alcance de las actividades de intercambio de información, lo que incluye identificar los tipos de información sobre amenazas que se puede intercambiar, las circunstancias en las que se permite el intercambio de información sobre amenazas y la prioridad de intercambio de información sobre amenazas en vehículos conectados.

La magnitud de las actividades de intercambio de información varía en función de los recursos y las capacidades de una organización. El alcance del intercambio de información sobre amenazas en vehículos conectados puede variar entre distintos tipos de organizaciones. Por ejemplo, es distinto entre proveedores de ciberseguridad, fabricantes de automóviles, proveedores de equipos V2X, proveedores de equipos de comunicación y operadores de telecomunicaciones, etc. Se recomienda a los productores de información de seguridad asociada a vehículos conectados con recursos limitados que se centren en un conjunto más reducido de actividades de producción o recogida de información sobre amenazas, ya que esto les permitirá ofrecer información de mayor valor a la organización y a los socios con los que la intercambien. Es posible que una organización pueda ampliar el alcance de sus actividades de intercambio de información sobre amenazas si incorpora capacidades y recursos adicionales. Una organización con más recursos y capacidades avanzadas puede optar por un alcance inicial más amplio que posibilite un conjunto mayor de actividades de intercambio de información sobre amenazas, para apoyar sus cometidos y sus propósitos.

En el Cuadro 1 se indica qué organizaciones pueden verse afectadas por cada tipo de amenaza, según lo definido en el documento [UIT-T X.1371].

Cuadro 1 – Correlación de distintas organizaciones afectadas por cada tipo de amenaza en vehículos conectados

Tipo de amenaza	Organizaciones que intercambian información sobre amenazas					
	Fabricantes de automóviles	**Proveedores**	**Proveedores de productos y servicios terceros**	**Equipo de coordinación**	**Operadores de telecomunicaciones**	**Proveedores de ciberseguridad**
Amenazas en relación con los servidores de soporte	✓		✓	✓		✓
Amenazas a los vehículos en relación con sus canales de comunicación	✓	✓	✓	✓	✓	✓
Amenazas a los vehículos en relación con sus procedimientos de actualización	✓		✓	✓		✓
Amenazas a los vehículos en relación con acciones humanas impremeditadas	✓	✓	✓			
Amenazas a los vehículos en relación con su conectividad y sus conexiones externas	✓	✓	✓	✓	✓	✓
Posibles objetivos o motivos de ataque	✓	✓	✓	✓		✓
Vulnerabilidades potenciales	✓	✓	✓	✓	✓	✓

8.3 Normas para el intercambio de información entre organizaciones

A partir de las características y la clasificación de la información sobre amenazas en vehículos conectados, las normas para el intercambio de información sobre amenazas entre organizaciones pueden describirse como se indica a continuación.

a) Se recomienda a las organizaciones que intercambien información sobre amenazas en vehículos conectados.

b) El intercambio de información sobre amenazas en vehículos conectados suele producirse en plataformas de gestión de vehículos conectados, proveedores de servicios compartidos de viaje, fabricantes de vehículos, proveedores de equipos V2X, proveedores de equipos de comunicación y operadores de telecomunicaciones.

c) Muchas organizaciones, como los fabricantes de automóviles y los proveedores de ciberseguridad, desempeñan funciones en calidad tanto de productores como de consumidores de información sobre amenazas.

d) Se recomienda que los productores de información sobre amenazas sean profesionales.

e) Se recomienda el cumplimiento de requisitos de gestión como el filtrado de la información de amenazas y la verificación de suscripciones.

8.4 Establecimiento de una comunidad para el intercambio

Se recomienda el establecimiento de una comunidad para intercambiar y analizar la información sobre amenazas en vehículos conectados. Entre los modelos de intercambio de información sobre amenazas se encuentran la modalidad entre pares, el de fuente y suscriptor y el modelo en estrella [b-OASIS TAXII]. Una comunidad de intercambio permite a las organizaciones recibir datos en tiempo real sobre vulnerabilidades y amenazas de red en vehículos conectados. Un ejemplo es Auto-ISAC, establecido por empresas automovilísticas en 2015. Esta entidad se centra en el establecimiento de una comunidad de intercambio de información con un creciente número de vehículos inteligentes. El portal del Auto-ISAC permite a sus miembros presentar y recibir información de forma anónima, y les ayuda a gestionar con mayor eficacia las amenazas de la red. El Auto-ISAC se ha dedicado a promover activamente la cooperación y el intercambio de información entre proveedores, compañías de vehículos comerciales y fabricantes de automóviles en el ámbito de la seguridad de las redes de vehículos. En el Apéndice I se facilita una introducción a las actividades de intercambio de información sobre amenazas del Auto-ISAC.

Una comunidad de intercambio puede establecer diversas subcomunidades, y las organizaciones pueden optar por unirse a una o varias de ellas en relación con los vehículos conectados. Se recomienda que la comunidad de intercambio sea abierta y permita a las distintas organizaciones el acceso y la salida libres a través de la cooperación voluntaria. Al optar por unirse a una subcomunidad, se recomienda que la organización en cuestión escoja una comunidad con recursos complementarios de información sobre amenazas en vehículos conectados. Cada organización puede publicar voluntariamente en la comunidad de intercambio la información sobre amenazas en vehículos conectados, y se responsabilizará de asegurarse de que la información aportada sea apta para su intercambio.

9 Procedimientos y orientación para el intercambio de información sobre amenazas en vehículos conectados

9.1 Introducción

En [UIT-T X.1371] se definen y describen las amenazas que afectan a los vehículos conectados. Las organizaciones pueden detectar, analizar y gestionar las amenazas de seguridad con sus recursos internos, así como intercambiar la información sobre amenazas estableciendo un marco de intercambio entre organizaciones. En un procedimiento de intercambio entre organizaciones, éstas pueden:

a) Obtener y utilizar información externa sobre amenazas para prevenir y mitigar las amenazas en los vehículos conectados.

b) Producir y facilitar a otras organizaciones información sobre amenazas en vehículos conectados para mejorar el ecosistema de seguridad de este sector.

Según la orientación de la cadena de transmisión de la información sobre amenazas, las organizaciones pueden ser de dos tipos: consumidoras y productoras. Muchas organizaciones, como los fabricantes de automóviles y los proveedores de ciberseguridad, suelen desempeñar funciones en calidad tanto de productores como de consumidores de información sobre amenazas.

9.2 Procedimientos de las actividades de intercambio de información sobre amenazas

Los consumidores son las potenciales víctimas de las amenazas a los vehículos conectados. La obtención y el uso de información sobre amenazas permite a sus consumidores localizar rápidamente los activos afectados y tomar las medidas necesarias para mitigar los riesgos. De entre todas las organizaciones pertinentes, los fabricantes de automóviles son los consumidores básicos de información sobre amenazas. Los procedimientos para los consumidores comprenden cinco fases:

a) Preparación: desarrollo de los mecanismos apropiados para prepararse para la aplicación de las actividades de intercambio de información.

b) Recepción: acto de recibir información externa sobre amenazas.

c) Análisis: realización de análisis de la información sobre amenazas recibida.

d) Mitigación: adopción de medidas para mitigar las amenazas a partir de los resultados del análisis.

e) Prevención: acciones encaminadas a prevenir futuros sucesos.

Los productores son entidades con capacidades técnicas y analíticas, y con una intención de intercambiar información en el ecosistema de los vehículos. Por lo general, los productores también necesitan consumir información sobre amenazas de seguridad, ya que la generación o la recogida de información sobre amenazas requiere múltiples fuentes, entre las que se encuentra la información recibida. Los procedimientos para los productores comprenden tres fases:

a) Preparación: desarrollo de los mecanismos apropiados para prepararse para la aplicación de las actividades de intercambio de información.

b) Análisis: realización de análisis para generar información sobre amenazas de alta calidad.

c) Compartición: transmisión de la información sobre amenazas generada a las partes interesadas.

9.3 Orientación durante las fases de los procedimientos

9.3.1 Orientación para organizaciones en calidad de consumidores

9.3.1.1 Orientación en la fase de preparación

Se recomienda a las organizaciones que desarrollen una política propia de información sobre amenazas de seguridad para vehículos conectados que incluya el establecimiento de objetivos, la definición del alcance y la elaboración de un proceso de toma de decisiones. A continuación se indican las orientaciones al respecto:

a) Establecimiento del objetivo: las organizaciones deben ser conscientes de que se enfrentan a amenazas de seguridad. A partir del análisis de las amenazas de seguridad que les afectan, se recomienda a las organizaciones que establezcan sus objetivos de seguridad para aumentar sus capacidades de protección y seguridad.

b) Definición del alcance: se recomienda a las organizaciones que definan el alcance de la información sobre amenazas y su nivel de prioridad teniendo en cuenta sus objetivos de seguridad, sus capacidades técnicas, su presupuesto financiero y las potenciales repercusiones de las múltiples amenazas para la organización en cuestión.

c) Elaboración de un proceso de toma de decisiones: se recomienda que se determine el tiempo necesario para la toma de decisiones, en función del tipo de información sobre amenazas que necesita la organización y su prioridad, a fin de evitar los efectos de un proceso prolongado de toma de decisiones cuando se disponga de información oportuna sobre amenazas.

9.3.1.2 Orientación en la fase de recepción

A continuación se indican las orientaciones al respecto:

a) Se recomienda a las organizaciones que almacenen la información sobre amenazas de seguridad intercambiada de forma apropiada.

b) Se recomienda a las organizaciones que tomen medidas encaminadas a garantizar la seguridad de almacenamiento de la información sobre amenazas.

c) Se recomienda a las organizaciones que eliminen la información sobre amenazas obsoleta o carente de utilidad.

9.3.1.3 Orientación en la fase de análisis

A continuación se indican las orientaciones al respecto:

a) Se recomienda a las organizaciones que evalúen el valor de la información sobre amenazas. En el Apéndice II se incluye una metodología de referencia para dicha evaluación. Se recomienda una evaluación automática.

b) Se recomienda a las organizaciones que lleven a cabo comprobaciones y análisis para valorar los daños potenciales a sus productos y servicios.

c) Se recomienda a las organizaciones que analicen el contexto para identificar información, p. ej., los atacantes, los TTP y los objetivos.

d) Se recomienda a las organizaciones que identifiquen los activos afectados, como servidores, dominios, unidades de control electrónico (ECU, *electronic control unit*), sistemas, etc.

e) Se recomienda a las organizaciones que lleven a cabo las actividades de filtrado, verificación y análisis en un entorno seguro para evitar repercusiones en sus sistemas esenciales.

9.3.1.4 Orientación en la fase de mitigación

A continuación se indican las orientaciones al respecto:

a) Se recomienda a las organizaciones que desarrollen soluciones de gestión y ejecuten los procesos correspondientes a partir de la información sobre amenazas y los resultados de los análisis. Entre dichas soluciones se encuentran el aislamiento del *hardware* afectado, la aplicación de parches, la actualización del *software*, la modificación de la configuración, etc.

b) Si las organizaciones carecen de capacidad de gestión, se recomienda que se pongan en contacto con los equipos de coordinación para vehículos conectados y obtengan asistencia al respecto.

c) En lo que respecta a los indicadores, se recomienda a las organizaciones que implanten indicadores de recepción en los dispositivos de ciberseguridad.

d) En el caso de las amenazas de seguridad provocadas por usuarios legítimos por medio de cambios en la configuración y la diseminación de programas malignos, se recomienda a las organizaciones que analicen y fortalezcan de inmediato la gestión. Las organizaciones pueden subsanar y gestionar las vulnerabilidades expuestas a explotación, los defectos o las configuraciones inapropiadas en la red mediante la información sobre amenazas, lo que incluye las medidas de eliminación.

9.3.1.5 Orientación en la fase de prevención

Se recomienda a las organizaciones que continúen supervisando sus productos y servicios.

9.3.2 Orientación para organizaciones en calidad de productores

9.3.2.1 Orientación en la fase de preparación

Se recomienda a las organizaciones que desarrollen una política propia que incluya el establecimiento de objetivos, la definición del alcance y la elaboración de un proceso de toma de decisiones. A continuación se indican las orientaciones al respecto:

a) Se recomienda a las organizaciones que establezcan un proceso de gestión de respuesta para evitar la fuga de datos importantes.

b) Se recomienda a las organizaciones que desplieguen herramientas y recursos esenciales para generar indicadores y otros datos sobre amenazas.

c) Se recomienda a las organizaciones que identifiquen, evalúen y clasifiquen los heterogéneos datos sobre amenazas de red procedentes de múltiples fuentes, con el fin de asegurarse de que se describa completamente y se actualice en todo momento toda la información relativa a la amenaza.

d) Se recomienda a las organizaciones que establezcan una comunidad de intercambio o se unan a una existente, que obtengan datos mediante la adquisición o la recepción de inteligencia de dominio no público y la recogida de inteligencia de dominio público, que analicen estos datos con arreglo a determinados requisitos empresariales y de situaciones de aplicación y que, en consecuencia, generen la inteligencia sobre amenazas pertinente. En el marco del intercambio, una comunidad de intercambio integra la información sobre amenazas compartida por todos sus miembros, en función de las necesidades del momento, para generar inteligencia sobre amenazas más focalizada, completa y precisa; la información se comparte de forma abierta o previo pago, en función de su tipo y su valor.

e) Se recomienda a las organizaciones que definan el alcance de sus actividades de intercambio de información, incluyendo la definición de la información sobre amenazas que se va a compartir y la decisión sobre el formato de intercambio.

9.3.2.2 Orientación en la fase de análisis

A continuación se indican las orientaciones al respecto:

a) Se recomienda a las organizaciones que filtren automática o manualmente los registros de alarmas para eliminar las que carezcan de valor o incluso las que resulten ser falsas.

b) Se recomienda a las organizaciones que evalúen el valor de la información compartida y que determinen el alcance del intercambio.

c) Se recomienda a las organizaciones que definan el carácter observable de diversas situaciones de amenazas de red y sus metadatos asociados, y que analicen y procesen los resultados comparativos de estos indicadores característicos de amenazas.

9.3.2.3 Orientación en la fase de compartición

A continuación se indican las orientaciones al respecto:

a) Se recomienda a las organizaciones que pongan en práctica sus actividades de compartición de información con arreglo al alcance definido.

b) Se recomienda a las organizaciones que faciliten la información sobre amenazas de seguridad en un formato normalizado.

c) Se recomienda a las organizaciones que faciliten más información contextual.

d) Se recomienda a las organizaciones que formulen el modelo y los mecanismos de compartición, y que resuelvan las cuestiones de la validez del intercambio de inteligencia y de la equidad de la transacción.

e) Dadas las necesidades de desarrollo de la industria, se recomienda el establecimiento de una plataforma de intercambio de información sobre amenazas en vehículos conectados que permita tal intercambio de información.

f) Se recomienda a las organizaciones que establezcan un mecanismo de control para la compartición de los datos sobre amenazas, que puede incluir la desensibilización, la autentificación y la destrucción de datos compartidos.

g) Se recomienda a las organizaciones con capacidad de generar información sobre amenazas en vehículos conectados que compartan la información con organizaciones que gocen de buena reputación.

Apéndice I

Prácticas idóneas para las actividades de intercambio de información sobre amenazas del Auto-ISAC

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

El Centro de Análisis e Intercambio de Información sobre el sector automovilístico [b-AUTO-ISAC] editó en 2019 una guía de prácticas idóneas titulada *Collaboration and engagement with appropriate third parties* (Colaboración y compromiso con terceros apropiados), en su versión 1.3. En esta guía, el Auto-ISAC define las prácticas idóneas de intercambio de información, que contemplan los terceros pertinentes, el nivel de apertura, los contenidos que resulta útil compartir, los procesos de intercambio de información, etc.

Para mejorar la ciberseguridad de los vehículos, estas organizaciones pueden colaborar e interactuar con diversos tipos de terceros en el ecosistema de los vehículos conectados. Entre los terceros pertinentes se encuentran los socios industriales, las organizaciones industriales, los gobiernos, las instituciones académicas, los investigadores y los medios de comunicación.

Las organizaciones pueden determinar el nivel apropiado de apertura en función de sus objetivos individuales de ciberseguridad en los vehículos y su panorama particular de riesgos. La apertura puede estructurarse en tres niveles: limitado, moderado y amplio.

Entre los procesos clave para compartir información entre distintas partes interesadas se encuentran los siguientes:

a) Identificación de contenidos cuyo intercambio resulta útil.

b) Interacción con las partes interesadas internas adecuadas.

c) Creación de procesos para recibir la información compartida y actuar en consecuencia.

d) Creación de procesos para enviar información a terceros externos.

e) Adquisición de las herramientas y las tecnologías apropiadas.

Apéndice II

Metodología de evaluación del valor de la información sobre amenazas

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

Al evaluar el valor de cada información sobre amenazas, las organizaciones pueden emplear los cinco factores que se enumeran a continuación:

a) Reputación de la fuente de la información sobre amenazas: las fuentes de la información sobre amenazas tienen distintas reputaciones. Las fuentes de alta fiabilidad pueden ofrecer información sobre amenazas más valiosa.

b) Puntualidad: el tiempo desempeña un papel clave en la información sobre amenazas. La información temprana puede ayudar a las organizaciones a protegerse y a prevenir ataques a sus activos.

c) Integridad de la descripción: por lo general, es más valiosa la información que incluya una descripción más detallada y más datos contextuales.

d) Pertinencia y repercusiones sobre la organización: ciertos tipos de información sobre amenazas tienen como objetivo una industria en particular, productos concretos o incluso compañías específicas. Es necesario prestar especial atención a la información sobre amenazas que afecta a la organización.

e) Eficacia de la información sobre amenazas: la multiplicidad de recursos múltiples puede causar duplicaciones y colisiones de información sobre amenazas; la fusión de las amenazas similares y la determinación de la autenticidad pueden mejorar la eficacia de la información sobre amenazas en una organización.

Bibliografía

[b-AUTO-ISAC] *Collaboration and Engagement with Appropriate Third Parties Best Practice Guide, Version 1.3, 2019.*

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-GSMA CLP.11] GSMA CLP.11 (2020), *IoT Security Guidelines Overview Document, Version 2.2.*

[b-GSMA CLP.14] GSMA CLP.14 (2020), *IoT Security Guidelines for Network Operators, Version 2.2.*

[b-OASIS TAXII] *OASIS Committee Specification, TAXII™ Version 2.1*.

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

Publicado en Suiza
Ginebra, 2023