التـوصيــة

ITU-T X.1382 (03/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

مبادئ توجيهية بشأن تبادل معلومات التهديدات الأمنية التي تتعرض لها المركبات الموصولة

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
القياس الحيوي عن بُعد	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن شبكة الويب (1)	X.1140–X.1149
أمن التطبيقات (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1350–X.1369
أمن أنظمة النقل الذكية (ITS)	**X.1370–X.1399**
أمن تكنولوجيا السجلات الموزعة (DLT)	X.1400–X.1429
أمن التطبيقات (2)	X.1450–X.1459
أمن شبكة الويب (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1500–X.1519
تبادل معلومات بشأن مواطن الضعف/الحالة	X.1520–X.1539
تبادل معلومات بشأن الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل معلومات بشأن السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
أمن شبكات الاتصالات المتنقلة الدولية–2020	X.1800–X.1819

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1382

مبادئ توجيهية بشأن تبادل معلومات التهديدات الأمنية التي تتعرض لها المركبات الموصولة

ملخص

تواجه المركبات الموصولة، في الوقت الحاضر، مع سرعة تطورها، مشاكل ملحوظة على نحو متزايد تتعلق بأمن الشبكات. ويُقصد بمعلومات التهديدات الأمنية المعرضة لها المركبات الموصولة، التي تؤدي دوراً أساسياً في تحقيق أمن هذه المركبات، جميع المعلومات التي يمكن أن تساعد المنظمة المعنية في تعريف هوية المركبة الموصولة وتقييمها ومراقبتها والاستجابة لها. وتستطيع المنظمات المتبادلة لمعلومات التهديدات الأمنية التي تتعرض لها المركبات الموصولة تحسين الوضع الأمني لكل منها والأوضاع الأمنية لغيرها من المنظمات.

وتقدم التوصية ITU-T X.1382 إرشادات بشأن مبادئ تبادل المعلومات الأمنية للمركبات الموصولة، وقواعده، ومنهجياته، وإجراءاته. كما تبين بإيجاز مختلف مجالات عمل شتى المنظمات المعنية ومختلف أدوارها ودرجات فعاليتها أثناء مشاركتها في دورة حياة عملية تبادل معلومات التهديدات الأمنية.

والغرض من هذه التوصية مساعدة المنظمات المعنية على إدامة اتصالها بالمجتمع المتبادل للمعلومات المتعلقة بالمركبات الموصولة وعلى المساهمة بتقديم معلومات عن التهديدات التي قد تواجهها هذه المركبات تدعم ممارسات حماية سلامتها. وبوجه عام، ترمي هذه التوصية إلى تحسين تبادل معلومات التهديدات الأمنية وتخفيف الآثار المحتملة لما قد تتعرض له المركبات الموصولة من هجمات تستهدف أمنها السيبراني.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1382	2023-03-03	17	11.1002/1000/15104

مصطلحات أساسية

المركبات الموصولة، تبادل معلومات التهديدات.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات/حقوق تأليف ونشر برمجيات يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قواعد البيانات ذات الصلة لقطاع تقييس الاتصالات (ITU-T) في موقع قطاع تقييس الاتصالات http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مبادئ توجيهية بشأن تبادل معلومات التهديدات الأمنية التي تتعرض لها المركبات الموصولة

1 مجال التطبيق

إن الغرض من هذه التوصية تقديم مبادئ توجيهية لمعلومات التهديدات المتعلقة بالأنظمة الإيكولوجية للمركبات الموصولة، تشمل أدوار المنظمات المعنية في تبادل معلومات التهديدات المعرضة لها المركبات الموصولة، وشراكاتها الرامية إلى ذلك، ومجال تطبيق هذا التبادل وإجراءاته ومتطلباته.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة، يشجَّع مستعملو هذه التوصية على بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1371] التوصية ITU-T X.1371 (2020)، *التهديدات الأمنية التي تتعرض لها المركبات الموصولة*.

[NIST SP 800-150] *دليل إلى تبادل معلومات التهديدات السيبرانية*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الإنذار (alert) [NIST SP 800-150]: هو إخطار تقني موجز بمواطن الضعف ووقائع الاستغلال الحالية وغيرها من المشاكل الأمنية الراهنة، يمكن للإنسان عادةً قراءته. ويُعرف أيضاً بالإشعار أو البلاغ أو بملاحظة عن مواطن الضعف.

2.1.3 معلومات التهديدات الأمنية (security threat information) [NIST SP 800-150]: هي معلومات تتعلق بتهديد معين يمكن أن تساعد المنظمة المعنية في حماية نفسها منه أو في كشف أنشطة طرف فاعل.

3.1.3 التهديد (threat) [b-ISO/IEC 27000]: هو سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 تكتيكات الطرف الفاعل (actor tactics): هي وصف لغايات الطرف الفاعل التقنية من أداء فعل معين.

2.2.3 تقنيات الطرف الفاعل (actor techniques): هي وصف للكيفية التي يحقق بها الطرف الفاعل غاياته التقنية بأداء فعل معين.

3.2.3 إجراءات الطرف الفاعل (actor procedures): هي وصف لقيام الطرف الفاعل بتنفيذ تقنية محددة.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

ACL قائمة مراقبة النفاذ (*Access Control List*)

APP تطبيق (*Application*)

CERT فريق الاستجابة للطوارئ الحاسوبية (*Computer Emergency Response Team*)

CSIRT فريق الاستجابة للحوادث الأمنية الحاسوبية (*Computer Security Incident Response Team*)

ECU وحدة التحكم الإلكتروني (*Electronic Control Unit*)

GSMA رابطة النظام العالمي للاتصالات المتنقلة *(GSM Association)*

ISAC مركز تبادل وتحليل المعلومات (*Information Sharing and Analysis Center*)

MEC حوسبة الحافة المتعددة النفاذ (*Multi-access Edge Computing*)

T-BOX صندوق البيانات التليماتية (*Telematics BOX*)

TSP مورد خدمة بيانات تليماتية (*Telematics Service Provider*)

TTP تكتيكات وتقنيات وإجراءات (*Tactics, Techniques and Procedures*)

V2X الاتصالات من مركبة إلى كل شيء (*Vehicle-to- Everything*)

5 اصطلاحات

في هذه التوصية:

يدل الفعل الأساسي "يوصى" على متطلب يوصى باستيفائه لكن لا يُشترط ذلك حتماً. ومن ثَم، لا يُشترط استيفاء هذا المتطلب لادعاء المطابقة.

6 لمحة عامة

تشمل العناصر الأساسية لعملية تبادل معلومات التهديدات المعرضة لها المركبات الموصولة أنواع معلومات التهديدات ومبادئ التبادل وأدواره وقواعده ومجتمعاته وإجراءاته. وبصفة عامة، تختلف أنواع معلومات التهديدات الأمنية التي قد تتعرض لها المركبات الموصولة باختلاف المنظمات المعنية بالمركبات الموصولة المنتجة لهذه المعلومات. وتتباين الأدوار في أنشطة تبادل معلومات التهديدات المعرضة لها المركبات الموصولة بتباين أنواع الوسطاء المضطلِعين بهذه الأدوار. وفي ظل اختلاف آثار معلومات التهديدات، من اللازم أن تتبع أنشطة التبادل هذه فيما بين المنظمات المعنية مبادئ وقواعد وإجراءات محددة. ويمكن لمنظمات مختلفة أن تشكل مجتمعاً يتبادل المعلومات وفقاً لأسلوب تبادل محدد وعلى أساس منصة للتبادل.

1.6 أنماط معلومات التهديدات المعرضة لها المركبات الموصولة

وفقاً للدليل [NIST SP 800-150] الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST)، يمكن تصنيف معلومات التهديدات المعرضة لها المركبات الموصولة إلى مؤشرات، وتكتيكات وتقنيات وإجراءات (TTP)، وإنذارات أمنية، وتقارير عن معلومات التهديدات، على النحو التالي:

أ) تشكل المؤشرات دلائل ملحوظة على أن هناك هجوماً وشيكاً أو أنه جارٍ بالفعل ويمكن استخدام المؤشرات لكشف التهديدات المحتملة والتصدي لها. وتشمل بعض مؤشرات المركبات الموصولة منظمات المهاجمين المشبه بهم للاتصالات من مركبة إلى كل شيء (V2X).

ب) تصف التكتيكات والتقنيات والإجراءات سلوك الطرف الفاعل، ويمكنها بيان نزوعه إلى استخدام نسخة محددة من برمجية ضارة أو ترتيب محدد من العمليات أو أنماط محددة من أدوات الهجوم وآليات التوصيل أو نظام استغلال محدد. وتتنوع مجموعة التهديدات لتشمل التهديدات المتعلقة بالمخدِّمات الخلفية والمخدِّم، والتهديدات التي تستهدف قنوات الاتصالات في المركبات. ومن الممكن أن تشمل هذه التكتيكات والتقنيات والإجراءات أفعالاً للتلاعب بتوصيلية وظائف المركبة أو لتجاوز نظام المراقبة بها، حيث تختلف عن التهديدات الشبكية التقليدية.

ج) أما الإنذارات الأمنية فهي إخطارات تقنية بمواطن الضعف ووقائع الاستغلال والبرمجيات الضارة وغيرها من المشاكل الأمنية. وعادةً ما تصدر هذه الإنذارات من مصادر موثوقة كأفرقة الاستجابة للطوارئ الحاسوبية (CERT) أو أفرقة الاستجابة للحوادث الأمنية الحاسوبية (CSIRT). وتصدر الإنذارات الأمنية في حال تنوع المركبات الموصولة المتضررة أو في حال احتمال وقوع أذى بالغ جراء التهديدات المبلَّغ بها.

د) تقدم تقارير معلومات التهديدات تحليلات متعمقة للتهديدات تشمل المشاركين في الواقعة والنظام المستهدف ونمط الهجوم وغيرها من المعلومات، وتُسدي المشورة بشأن إجراءات التخفيف من آثار التهديدات. كما يمكن أن تبين تقارير معلومات التهديدات الاتجاهات المستقبلية للتهديدات. وتؤدي هذه التقارير دوراً مهماً في منع تعرض المركبات الموصولة لهجمات جديدة.

2.6 منافع وتحديات تبادل معلومات التهديدات المعرضة لها المركبات الموصولة

باعتماد نهج تبادل معلومات التهديدات المعرضة لها المركبات الموصولة، تستطيع المنظمات المعنية بصناعة هذه المركبات تحسين الوضع الأمني لكل منها بالاستفادة المسبقة من معارف المنظمات الشريكة لها وخبراتها وقدراتها. وتشمل المنافع المحققة من تبادل معلومات التهديدات المعرضة لها المركبات الموصولة ما يلي:

أ) تعزيز القدرات الدفاعية للمنظمات المعنية بالمركبات الموصولة. ومع تعرض هذه المركبات لتهديدات جديدة، يمكن لتبادل المعلومات أن يساعد هذه المنظمات في تعزيز قدراتها على مواجهة التهديدات. وغالباً ما تُستخدم مواطن الضعف الجديدة كأداة رئيسية لشن الهجمات. وبالتالي، يمكن أن يُفيد تبادل معلومات التهديدات في التعامل في الوقت المناسب مع الهجمات المدفوعة بكشف مواطن ضعف جديدة، وفي تعزيز القدرة على صدِّ الهجمات. ومع تعدد الهجمات الجديدة التي تواجهها المركبات الموصولة، يساعد تبادل معلومات التهديدات في التعامل مع التهديدات الجديدة التي قد تتعرض لها المركبات الموصولة، ويحسِّن القدرة الدفاعية.

ب) الحفاظ على صحة النظام الإيكولوجي للمركبات الموصولة. فتبادل معلومات التهديدات يساعد في تعزيز أمن البيئة الاقتصادية للمركبات الموصولة وترسيخ الأمن الإيكولوجي لجميع المركبات الموصولة. وأمن سلسلة تصنيع المركبات الموصولة يشمل أمن موردي الخدمات، وموردي خدمات البيانات التليماتية (TSP)، وشركات تصنيع المركبات، ومشغلي الاتصالات، فضلاً عن موردي معدات مطاريف المركبات والمطاريف المحمولة باليد، وموردي معدات المطاريف المتنقلة الذكية، وغيرهم.

ورغم ما لتبادل معلومات التهديدات من منافع، فما زال يطرح بعض التحديات. ومن تحديات تبادل المعلومات ما يلي:

أ) إنشاء نظام قياسي لتبادل معلومات التهديدات المعرضة لها المركبات الموصولة. فحفاظاً على صحة النظام الإيكولوجي للمركبات الموصولة، من الضروري إنشاء نظام قياسي معقول لتبادل معلومات التهديدات المتعلقة بها. ولا يوجد في الوقت الراهن نظام قياسي دولي موحد لتبادل معلومات التهديدات المعرضة لها المركبات الموصولة. وإن لم يُنشأ النظام القياسي المرجو، فسيعرقل ذلك عملية تبادل المعلومات ليؤثر في النهاية على تطورها.

ملاحظة – يمكن أن توفر بعض المبادئ التوجيهية مثل [ITU-T X.1371] والمبادئ التوجيهية لرابطة النظام العالمي للاتصالات المتنقلة بشأن أمن إنترنت الأشياء [b-GSMA CLP.11] مسائل الأمن التي يمكن اعتبارها أفضل الممارسات الممكنة لتبادل المعلومات.

ب) تحديد نطاق معلومات التهديدات. إذ تتألف السلسلة الصناعية للمركبات الموصولة من حلقات مختلفة، تواجه كل منها أنماطاً مختلفة من التهديدات. فيلزم تحديد عملية تبادل معلومات التهديدات في كل حلقة، وأسلوب تبادل هذه المعلومات فيما بين هذه الحلقات.

ج) حماية المعلومات الحساسة والمعلومات المصنفة. إن تبادل معلومات التهديدات التي قد تتعرض لها المركبات الموصولة يواجه خطر الإفصاح عن المعلومات الحساسة. وتكنولوجيات التجفير معرضة للمساس بها أو غير مطبقة بدرجة كافية. وقد يؤدي عدم كفاية استخدام تكنولوجيات التجفير أيضاً إلى تسرب مفاتيح أو إثباتات التجفير.

علاوةً على ذلك، قد يزداد خطر تسرب المعلومات باستخدام تكنولوجيات التجفير المعطلة أو المتقادمة أصلاً. ومن المعلومات الحساسة التي ينبغي حمايتها برمجيات المركبات، المحمية بحقوق ملكية فكرية أو الخاصة بالملكية؛ والمعلومات الخاصة لمالك المركبة كهويته الشخصية، ومعلومات حساب الدفع الخاص به، ومعلومات دفتر العناوين الخاص به، ومعلومات الموقع، ومعرِف هوية المركبة الإلكتروني؛ ومفاتيح التجفير، وما إلى ذلك. إضافةً إلى ذلك، لا يجوز للمنظمات غير المخولة للنفاذ إلى معلومات سرية النفاذ إليها. والحصول على المخالصات اللازمة لمواصلة النفاذ إلى مصادر المعلومات المصنفة، واستبقاؤها، مسألتان مكلفتان ومهدرتان للوقت بالنسبة إلى المنظمات المعنية.

7 مبادئ تبادل معلومات التهديدات المعرضة لها المركبات الموصولة

لضمان فعالية عملية تبادل وتناقل معلومات التهديدات ودقتها وأمنها، من اللازم أن تتبع المنظمات والشركات المعنية بعض المبادئ.

1.7 المنافع المتبادلة

إن الأصل في تبادل معلومات التهديدات الأمنية هو تعزيز القدرة الحمائية لأمن الشبكات المتعلقة بالمركبات الموصولة، بتضافر الجهود. وتُوصى الأطراف المشاركة في عملية تبادل معلومات التهديدات الأمنية المعرضة لها المركبات الموصولة بإدراك الحقوق والواجبات والمسؤوليات القانونية المتبادلة في أنشطة تبادل معلومات التهديدات. وإضافةً إلى أن المنظمات المعنية تُوصى بتلقي معلومات التهديدات، التي تخص كلا منها، فإنها توصى أيضاً بأن تساهم بفاعلية بجهودها الخاصة في تحقيق منافع متبادلة ومواقف مربحة لجميع الأطراف.

2.7 التجميع في فئات والتصنيف

تختلف الأدوار في عملية تبادل معلومات التهديدات الأمنية باختلاف المنظمات التي تؤديها. ويبدو أن معنى بعض معلومات التهديدات وأهميتها يتباينان بتباين المنظمات التي تتلقاها. فتُوصى المنظمة المعنية بتجميع معلومات التهديدات المعرضة لها المركبات الموصولة في فئات، وتصنيفها، وتحديد نطاقاتها الفعلية. ويُوصى بإنشاء مستويات مختلفة لنظام إدارة هذه المعلومات وفقاً لفئاتها وتصنيفها ووسوم نطاقاتها. كما يُوصى باستخدام تكنولوجيات تجفير مناسبة بغرض إدامة حماية سرية المعلومات الحساسة وسلامتها و/أو استيقانها.

3.7 أمن البيانات

إن مشاكل من قبيل الاستخدام غير القانوني للبيانات المتعلقة بمعلومات التهديدات وسرقتها والعبث بها والنفاذ غير المخول إليها من جانب المستخدمين، تؤثر تأثيراً بالغاً على مبادرة الأطراف المتبادلة للبيانات إلى تبادل المعلومات وتحد من أمن وفعالية أنشطة تبادل هذه المعلومات. ولذلك، تركز عملية تبادل معلومات التهديدات أيضاً على مكافحة تبادل المخاطر. ومن تدابير المكافحة تبادل استخدام تكنولوجيات التجفير، وإزالة حساسية البيانات التي يتم تبادلها وتحديدها وتدميرها وغير ذلك من التدابير، وهي تدابير فعالة في حماية البيانات المتعلقة بمعلومات التهديدات التي تستهدف أمن المركبات الموصولة.

8 المنظمات وأدوارها وشراكاتها

1.8 المنظمات وأدوارها

1.1.8 شركات صناعة السيارات

تضطلع شركات صناعة السيارات بأهم دور في أنشطة تبادل معلومات التهديدات المعرضة لها المركبات الموصولة، لأنها تتواصل مباشرة مع المستخدمين وتتحمل مسؤولية أمن المركبات التي تصنعها.

فعن طريق جمع البيانات من أنظمة الإنتاج، والمكونات المثبتة على متن المركبات، والبنى التحتية للمركبات الموصولة، الخاصة بشركات صناعة السيارات، تقوم هذه الشركات بجمع معلومات التهديدات الأمنية المعرضة لها المركبات الموصولة ودمجها وإنتاجها وتحليلها وتتخذ تدابير لتخفيف حدة التهديدات.

2.1.8 الموردون

يوفر الموردون العتاد أو البرمجيات المثبتة داخل المركبات الموصولة، ومنها شرائح المركبات ومعدات صندوق البيانات التليماتية (T-BOX) والبوابات الداخلية/الخارجية. يقوم الموردون بجمع واستلام معلومات التهديدات الأمنية، المتعلقة بمنتجاتهم، وتساعد أفرقةَ التنسيق وشركاتِ تصنيع السيارات وغيرها من الأطراف المعنية في تخفيف حدة التهديدات و/أو الوقاية والحد من الحوادث الأمنية، المتصلة بمنتجاتهم.

3.1.8 موردو المنتجات والخدمات من الأطراف الثالثة

يعود مصطلح موردي المنتجات والخدمات من الأطراف الثالثة، أساساً، إلى المنظمات التي تقدم منتجات وخدمات مستقلة تتعلق بالمركبات الموصولة بخلاف شركات تصنيع السيارات وموردي قطع غيارها كموردي خدمات البيانات التليماتية (TSP)، وموردي خدمات الحوسبة السحابية، وشركات بيع العتاد، وشركات تصنيع المطاريف المتنقلة، فضلاً عن موردي خدمات التأمين على المركبات، والأطراف الثالثة الأخرى من مشغلي منصات الخدمات، وغيرها من الأطراف الثالثة.

وتقوم الأطراف الثالثة من موردي المنتجات والخدمات بجمع/إنتاج/تبادل معلومات التهديدات الأمنية المتعلقة بمنتجاتها أو منصات خدماتها، كمعلومات التهديدات المتمثلة في تعطل المركبات الموصولة أو عدم مشروعية بعض سلوكيات المستخدمين أو تنفيذ هجمات عن بُعد، وتساعد الأطراف المعنية كأفرقة التنسيق المعنية بالمركبات الموصولة، وشركات تصنيع السيارات، في تخفيف حدة التهديدات و/أو التعامل مع الحوادث الأمنية التي قد تتعرض لها المركبات الموصولة. وموردو خدمات الحوسبة السحابية مسؤولون أيضاً عن تبادل المعلومات التي تتضمن سوء التشكيل أو الأخطاء، وتلك التي تشير إلى إساءة استخدام منافذ التحكم، والإدارة غير السليمة للإثباتات، وتسرب البيانات السحابية، وغيرها من التهديدات.

4.1.8 أفرقة التنسيق

تعمل أفرقة التنسيق المعنية بالمركبات الموصولة عادةً ككيانات مستقلة تركز على تنسيق معلومات التهديدات الأمنية وتنسيق الاستجابة للحوادث، كفرق الاستجابة للطوارئ الحاسوبية (CERT)/فرق الاستجابة للحوادث الأمنية الحاسوبية (CSIRT)، ومركز تبادل وتحليل المعلومات المتعلقة بصناعة السيارات (Auto-ISAC).

وتساعد أفرقة التنسيق المعنية بالمركبات الموصولة الأطرافَ المعنية في تنسيق تبادل معلومات التهديدات الأمنية فيما بين جميع المنظمات، وتقدم إليها خدمتي الإخطار، والإنذار المبكر.

5.1.8 مشغلو الاتصالات

يقدم مشغلو الاتصالات خدمات الاتصالات الأساسية للمركبات الموصولة.

ويعمل مشغلو الاتصالات، على ضمان أمن البنية التحتية لشبكة الاتصالات، كالشبكات الأساسية والمحطات القاعدة ومنصات حوسبة الحافة المتعددة النفاذ (MEC) وغيرها.

ملاحظة – يمكن النظر في المبادئ التوجيهية لرابطة النظام العالمي للاتصالات المتنقلة بشأن مشغلي الشبكات [b-GSMA CLP.14] كمثال لمشغلي الاتصالات في سياق المركبات الموصولة.

6.1.8 شركات بيع خدمات الأمن السيبراني

شركات بيع خدمات الأمن السيبراني هي الشركات أو المنظمات المعنية بالشبكات، التي تعمل مع الشركات والمنظمات المعنية بالمركبات وتقدم منتجات أو خدمات الأمن السيبراني.

وعن طريق مصادر من قبيل المعدات الأمنية، وبرمجيات المطاريف، والإنترنت، تساعد شركات بيع خدمات الأمن السيبراني المنظمات المعنية في جمع معلومات التهديدات الأمنية المعرضة لها المركبات الموصولة ودمجها وتحليلها وتقدم الدعم الأمني والخدمات الأمنية اللازمين للوقاية من الحوادث الأمنية والحد منها.

2.8 نطاقات تبادل المعلومات فيما بين المنظمات

تُوصى المنظمات المعنية بتحديد نطاق أنشطة تبادل المعلومات، بما يشمل تحديد أنواع معلومات التهديدات التي يمكن تبادلها والظروف التي يجوز فيها تنفيذ أنشطة تبادل معلومات التهديدات وأولوية تبادل معلومات التهديدات المعرضة لها المركبات الموصولة.

ويتفاوت نطاق أنشطة تبادل المعلومات تبعاً لموارد المنظمة المعنية وقدراتها. كما أن نطاقات تبادل معلومات التهديدات التي قد تتعرض لها المركبات الموصولة تختلف بين شتى أشكال المنظمات المعنية. فعلى سبيل المثال، تتنوع نطاقات التبادل هذه فيما بين شركات بيع خدمات الأمن السيبراني وشركات صناعة السيارات وموردي معدات الاتصالات من المركبات إلى كل شيء وموردي معدات الاتصالات ومشغلي الاتصالات وغيرها من الأطراف. فتُوصى المنظمات المحدودة الموارد من تلك المنتجة لمعلومات التهديدات المعرضة لها المركبات الموصولة بالتركيز على مجموعة صغيرة من أنشطة إنتاج/جمع معلومات التهديدات، التي تقدم معلومات أعلى قيمة للمنظمة المعنية ولشركائها الذين يتبادلون معلومات التهديدات هذه. وقد تتمكن المنظمة من توسيع نطاق تبادل معلومات التهديدات، كقدرات وموارد إضافية. وللمنظمة الحائزة لحجم كبير من الموارد وقدرات متقدمة أن تختار نطاقاً أولياً واسعاً يُتيح التعامل مع مجموعة أوسع من أنشطة تبادل معلومات التهديدات لدعم تحقيق غاياتها وأهدافها.

ويقدم الجدول 1 أشكال المنظمات المحتمل تأثرها بكل نوع من أنواع التهديدات المحددة في التوصية [ITU-T X.1371].

الجدول 1 – تقابل المنظمات المختلفة المحتمل تأثرها بكل نوع من أنواع التهديدات المعرضة لها المركبات الموصولة

أنواع التهديدات	المنظمات التي ينبغي أن تتبادل معلومات التهديدات					
	شركات صناعة السيارات	الموردون	الأطراف الثالثة من موردي المنتجات والخدمات	أفرقة التنسيق	مشغلو الاتصالات	شركات بيع خدمات الأمن السيبراني
التهديدات المتعلقة بالمخدِّمات الخلفية	✓		✓	✓		✓
التهديدات التي تستهدف المركبات وتخص قنوات الاتصالات فيها	✓	✓	✓	✓	✓	✓
التهديدات التي تستهدف المركبات وتخص إجراءات التحديث المتعلقة ببرمجياتها	✓		✓	✓		✓
التهديدات التي تستهدف المركبات وتخص الأفعال البشرية غير المقصودة	✓	✓	✓			
التهديدات التي تستهدف المركبات وتخص توصيليتها وتوصيلاتها الخارجية	✓	✓	✓	✓	✓	✓

الجدول 1 – تقابل المنظمات المختلفة المحتمل تأثرها بكل نوع من أنواع التهديدات المعرضة لها المركبات الموصولة

أنواع التهديدات	المنظمات التي ينبغي أن تتبادل معلومات التهديدات					
	شركات صناعة السيارات	الموردون	الأطراف الثالثة من موردي المنتجات والخدمات	أفرقة التنسيق	مشغلو الاتصالات	شركات بيع خدمات الأمن السيبراني
الأهداف المحتملة للهجمات، أو دوافع تنفيذ هجمات	✓	✓	✓	✓		✓
مواطن الضعف المحتملة	✓	✓	✓	✓	✓	✓

3.8 قواعد تبادل المعلومات فيما بين المنظمات

استناداً إلى خصائص معلومات التهديدات المعرضة لها المركبات الموصولة وإلى تصنيف هذه المعلومات، يمكن بيان قواعد تبادل معلومات التهديدات فيما بين المنظمات على النحو التالي:

أ) تُوصى المنظمات بتبادل معلومات التهديدات المعرضة لها المركبات الموصولة.

ب) يُنفذ تبادل معلومات التهديدات المعرضة لها المركبات الموصولة غالباً على مستويات منصات إدارة المركبات الموصولة، وموردي خدمات السفر المشتركة، وشركات تصنيع المركبات، وموردي معدات الاتصالات من المركبات إلى كل شيء، وموردي تجهيزات الاتصالات، ومشغلي الاتصالات.

ج) تؤدي منظمات عديدة كشركات صناعة السيارات وشركات بيع خدمات الأمن السيبراني دوراً بصفتها جهات منتجة وجهات مستهلكة، في آن، لمعلومات التهديدات.

د) يُوصى بأن يتسم منتجو معلومات التهديدات بالاحترافية.

هـ) يُوصى بتحديد المتطلبات الإدارية من قبيل فرز معلومات التهديدات والتحقق من الاشتراكات.

4.8 إنشاء مجتمع للتبادل

يُوصى بإنشاء مجتمع يعنى بتبادل معلومات التهديدات المعرضة لها المركبات الموصولة وتحليلها. وتشمل أساليب تبادل معلومات التهديدات التبادل بين النظراء، والتبادل بين المصدر والمشترِك، والتبادل بين المحور وروافده [b-OASIS TAXII]. فعن طريق مجتمع للتبادل، يمكن للمنظمات أن تتلقى بيانات في الوقت الفعلي عن التهديدات ومواطن الضعف الشبكية المتعلقة بالمركبات الموصولة. إن مركز تبادل وتحليل المعلومات المتعلقة بصناعة السيارات (AUTO-ISAC)، الذي أنشأته شركات السيارات في عام 2015، هو مثال على ذلك. إذ يركز هذا الكيان على إنشاء مجتمع لتبادل المعلومات يتزايد فيه عدد المركبات الذكية. وتتيح بوابة المركز الإلكترونية لأعضائه تقديم المعلومات وتلقيها على أساس إخفاء الهوية، وتساعدهم على التعامل مع التهديدات الشبكية على نحو أكثر فعالية. وما برح المركز ينشط في تعزيز التعاون والتبادل في المعلومات فيما بين الموردين وشركات المركبات التجارية وشركات تصنيع السيارات، في مجال أمن شبكات المركبات. ويورد التذييل I مقدمة إلى أنشطة تبادل معلومات التهديدات، التي يباشرها المركز.

ومن الممكن أن يُنشئ مجتمع التبادل مجتمعات تبادل فرعية متعددة، وبإمكان المنظمات المعنية أن تختار الانضمام إلى مجتمع فرعي واحد أو أكثر من المجتمعات الفرعية المعنية بالمركبات الموصولة. ويُوصى مجتمع التبادل بأن يكون مجتمعاً مفتوحاً يسمح بانضمام مختلف المنظمات إليه وخروجها منه، بحرية وبالتعاون الطوعي. وفي حال اختيار المنظمة الانضمام إلى مجتمع فرعي، تُوصى المنظمة باختيار المجتمع الذي تتوفر لديه موارد تكميلية لمعلومات التهديدات المعرضة لها المركبات الموصولة. وتنشر جميع المنظمات طواعيةً لمجتمع التبادل معلومات التهديدات التي قد تتعرض لها المركبات الموصولة، وهي مسؤولة عن ضمان ملاءمة معلومات التهديدات المقدمة إليه للتبادل.

9 إجراءات وإرشادات بشأن تبادل معلومات التهديدات التي تتعرض لها المركبات الموصولة

1.9 مقدمة

تحدد التوصية [ITU-T X.1371] وتبين التهديدات التي قد تتعرض لها المركبات الموصولة. وتستطيع المنظمات المعنية كشف التهديدات الأمنية وتحليلها والتعامل معها باستخدام مواردها الداخلية، ويمكنها أيضاً أن تتبادل معلومات التهديدات بإنشاء إطار للتبادل فيما بينها جميعاً. وتُتيح إجراءات التبادل فيما بين جميع المنظمات المعنية لهذه المنظمات ما يلي:

أ) الحصول على معلومات التهديدات من مصادر خارجية، واستخدامها، لوقاية المركبات الموصولة من التعرض لتهديدات وتخفيف خطورة هذه التهديدات.

ب) إنتاج وتقديم معلومات عن التهديدات المعرضة لها المركبات الموصولة بالاشتراك مع سائر المنظمات المعنية لتعزيز النظام الإيكولوجي لهذه المركبات.

ويمكن تصنيف المنظمات المعنية تبعاً لموقعها في سلسة تناقل معلومات التهديدات إلى نمطين، هما: منظمات مستهلكة ومنظمات منتجة. وعادةً ما تضطلع منظمات عديدة كشركات صناعة السيارات وشركات بيع المنتجات والخدمات الأمنية السيبرانية بدوريْ المنظمات المنتجة لمعلومات التهديدات والمنظمات المستهلكة لها، كليهما.

2.9 الإجراءات المتعلقة بأنشطة تبادل معلومات التهديدات

إن الجهة المستهلكة هي الضحية المحتملة للتهديدات التي قد تتعرض لها المركبات الموصولة. وبحصول المنظمات المستهلكة المعنية على معلومات التهديدات واستخدامها إياها، يتسنى لها أن تحدد بسرعة أماكن الأصول المحتمل تأثرها وتتخذ التدابير المضادة اللازمة لتخفيف خطورة هذه التهديدات. ومن جملة المنظمات المعنية، تشكل شركات صناعة السيارات المنظمات المستهلكة أساساً لمعلومات التهديدات. وتتألف الإجراءات المتعلقة بالمنظمات المستهلكة من خمس مراحل، هي:

أ) الإعداد: استحداث آليات تأهب ملائمة بغرض الانخراط في أنشطة تبادل معلومات التهديدات؛

ب) التلقِّي: تلقي معلومات التهديدات من مصادر خارجية؛

ج) التحليل: إجراء تحليل لمعلومات التهديدات الواردة؛

د) التخفيف: اتخاذ تدابير تخفِّف خطورة التهديدات استناداً إلى نتائج تحليل المعلومات؛

هـ) الوقاية: اتخاذ إجراءات لاتقاء حدوث وقائع مماثلة في المستقبل.

أما المنظمات المنتجة لمعلومات التهديدات، فهي الكيانات التي تتوفر لديها القدرة التقنية والقدرة التحليلية ونية التبادل في النظام الإيكولوجي للمركبات. وعادةً ما تحتاج المنظمات المنتجة، أيضاً، إلى استهلاك معلومات التهديدات الأمنية نظراً إلى أن إنتاج/جمع معلومات التهديدات يستلزم مصادر متعددة، منها المعلومات الواردة عن التهديدات. وتتألف الإجراءات المتعلقة بالمنظمات المنتجة من ثلاث مراحل، هي:

أ) الإعداد: استحداث آليات تأهب ملائمة بغرض الانخراط في أنشطة تبادل معلومات التهديدات؛

ب) التحليل: إجراء تحليل لإنتاج معلومات عالية الجودة عن التهديدات؛

ج) التبادل: تبادل معلومات التهديدات الناتجة مع الأطراف المهتمة.

3.9 إرشادات مراحل الإجراءات

1.3.9 الإرشادات الموجهة إلى المنظمات المعنية بصفتها منظمات مستهلكة

1.1.3.9 إرشادات مرحلة الإعداد

توصى المنظمات بوضع سياسات داخلية لمعلومات التهديدات الأمنية المعرضة لها المركبات الموصولة، تشمل تحديد الغاية من هذه المعلومات ونطاقها وعملية اتخاذ القرارات المتعلقة بها. وفيما يلي إرشادات تنفيذ ذلك:

أ) تحديد الغاية: لابد للمنظمات المعنية من أن تحيط علماً بأنها تواجه تهديدات أمنية. وبناءً على تحليل هذه التهديدات، توصى المنظمات بتحديد أهدافها المتعلقة بالسلامة لتعزيز قدرتها على حماية سلامتها.

ب) تحديد النطاق: بعدما تؤخذ في الاعتبار الأهداف الأمنية للمنظمة المعنية وقدراتها التقنية وميزانيتها المالية والآثار المحتملة لمختلف التهديدات التي قد تستهدفها، مجتمعةً، يوصى بتحديد نطاق المعلومات اللازمة للمنظمة عن هذه التهديدات، وبترتيب هذه المعلومات بحسب الأولوية.

ج) تحديد عملية اتخاذ القرار: يوصى بتحديد الوقت اللازم لعملية اتخاذ القرار وفقاً لنمط المعلومات اللازمة عن التهديدات، ودرجة أولويتها، تلافياً لآثار إطالة عملية اتخاذ القرار على معلومات التهديدات عند توفرها في الوقت المناسب.

2.1.3.9 إرشادات مرحلة التلقّي

فما يلي إرشادات هذه المرحلة:

أ) توصى المنظمات بتخزين المعلومات المشتركة عن التهديدات الأمنية تخزيناً سليماً.

ب) توصى المنظمات باتخاذ تدابير تضمن مأمونية تخزين معلومات التهديدات.

ج) توصى المنظمات بحذف المعلومات المتقادمة وغير المفيدة عن التهديدات.

3.1.3.9 إرشادات مرحلة التحليل

فما يلي إرشادات هذه المرحلة:

أ) توصى المنظمات بتقييم أهمية معلومات التهديدات. ويبين التذييل II إحدى المنهجيات المرجعية لتقييم أهمية هذه المعلومات. ويوصى باتباع أسلوب التقييم التلقائي.

ب) توصى المنظمات بالتحقق من مدى خطورة الأضرار التي قد تلحق بمنتجاتها وخدماتها وإجراء تحليل لتقييمها.

ج) توصى المنظمات بتحليل السياق لتحديد معلومات من قبيل هوية المهاجمين، والتكتيكات والتقنيات والإجراءات المتبعة، والأهداف المحتملة.

د) توصى المنظمات بتحديد الأصول المحتمل تأثرها كالمخدِّمات، والميدان (الميادين)، ووحدات التحكم الإلكتروني (ECUs)، والنظام (الأنظمة)، وغيرها من الأصول.

هـ) توصى المنظمات بتنفيذ عمليتي الغربلة والتحقق وإجراء التحليلات في بيئة مأمونة لتجنب تأثيرها على الأنظمة الحساسة بها.

4.1.3.9 إرشادات مرحلة التخفيف

فما يلي إرشادات هذه المرحلة:

أ) توصى المنظمات باستحداث حلول تتعلق بكيفية التعامل مع التهديدات المحتملة وبأن تُسند عمليات التعامل التي تنفذها إلى معلومات التهديدات ونتائج تحليلها. ومن هذه الحلول عزل الأجهزة المتضررة وتنفيذ إصلاحات وتحديث البرمجيات وتعديل التشكيل وغيرها من الحلول.

ب) في حال افتقار المنظمة المعنية إلى قدرات التعامل، توصى بالاتصال بأفرقة التنسيق المعنية بالمركبات الموصولة وطلب مساعدتها.

ج) فيما يتعلق بالمؤشرات، توصى المنظمات بتنفيذ المؤشرات الواردة إليها في الأجهزة الأمنية السيبراني.

د) بخصوص التهديدات الأمنية التي قد يسببها مستخدمون شرعيون بقيامهم بتعديل التشكيل أو نشر برامج ضارة، توصى المنظمات بتحليل نظام الإدارة وتعزيزه، فوراً. وبإمكان المنظمات إصلاح وإدارة مواطن الضعف أو العيوب أو أنساق التشكيل غير الملائم القابلة للاستغلال في الشبكة باستخدام معلومات التهديدات بما في ذلك تدابير التخلص مما يلزم التخلص منه.

5.1.3.9 إرشادات مرحلة الوقاية

توصى المنظمات بمواصلة رصد منتجاتها وخدماتها.

2.3.9 الإرشادات الموجهة إلى المنظمات المعنية بصفتها منظمات منتجة

1.2.3.9 إرشادات مرحلة الإعداد

توصى المنظمات بوضع سياسات داخلية لمعلومات التهديدات، تشمل تحديد الغاية من هذه المعلومات، ونطاقها، وعملية اتخاذ القرارات المتعلقة بها. وفيما يلي إرشادات تنفيذ ذلك:

أ) توصى المنظمات بإنشاء عملية لإدارة الاستجابة تستهدف منع تسرب المعلومات المهمة.

ب) توصى المنظمات بنشر الموارد والأدوات اللازمة لإنتاج المؤشرات وغيرها من بيانات التهديدات.

ج) توصى المنظمات بتحديد البيانات المتعددة المصادر للتهديدات المعرضة لها الشبكات غير المتجانسة، وتقييم هذه البيانات وتصنيفها، لضمان أن تكون جميع المعلومات المتعلقة بكل تهديد مبينة بالكامل ومحدثة باستمرار.

د) توصى المنظمات بأن تُنشئ مجتمعاً للتبادل أو تنضم إليه، وتحصل على البيانات بشراء/تلقي البيانات الاستخباراتية غير العلنية وجمع البيانات الاستخباراتية العلنية، وأن تحلل هذه البيانات وفقاً لبعض سيناريوهات التطبيقات والمتطلبات التجارية، ثم تُنتج المعلومات الاستخباراتية المتعلقة بالتهديدات المرصودة. وفي إطار عملية التبادل، يكمِّل مجتمع التبادل معلومات التهديدات المشتركة بين جميع أعضائه وفقاً للاحتياجات الفعلية إلى إنتاج معلومات استخباراتية عن التهديدات أكثر تحديداً وأكمل وأدق، ويتبادلها في شكل معلومات مفتوحة المصدر أو مبيعات مدفوعة الثمن وفقاً لنمط المعلومات الاستخباراتية وقيمتها.

هـ) توصى المنظمات بتحديد نطاق أنشطة تبادل المعلومات، بما يشمل تحديد معلومات التهديدات المعتزم تبادلها وتقرير نسق عملية التبادل.

2.2.3.9 إرشادات مرحلة التحليل

فما يلي إرشادات هذه المرحلة:

أ) توصى المنظمات بغربلة سجلات التنبيهات تلقائياً أو يدوياً لإزالة التنبيهات عديمة الجدوى أو حتى الكاذبة.

ب) توصى المنظمات بتقييم أهمية المعلومات المشتركة وتحديد مجالات عمل المنظمات التي تتبادل المعلومات.

ج) توصى المنظمات بالوقوف على مدى وضوح مختلف سيناريوهات التهديدات الشبكية والمعلومات الوصفية المتعلقة بها، ثم تحليل ومعالجة نتائج المقارنة بين هذه المؤشرات لخصائص التهديدات.

3.2.3.9 إرشادات مرحلة التبادل

فما يلي إرشادات هذه المرحلة:

أ) توصى المنظمات بتنفيذ عمليات تبادل معلومات التهديدات وفقاً للنطاق المحدد.

ب) توصى المنظمات بتقديم معلومات التهديدات بأنساق قياسية.

ج) توصى المنظمات بتقديم مزيد من المعلومات السياقية.

د) توصى المنظمات بصوغ نماذج التبادل وآلياته، وحسم مسألتي مدى صلاحية تبادل المعلومات الاستخباراتية ومدى عدالة المعاملات.

هـ) في ظل الاحتياجات الإنمائية لصناعة المركبات الموصولة، يوصى بإنشاء منصة لتبادل معلومات التهديدات التي قد تتعرض لها هذه المركبات، لتنفيذ عمليات تبادل المعلومات.

و) توصى المنظمات بإنشاء آليات لمراقبة تبادل البيانات المتعلقة بمعلومات التهديدات، تشمل تقنيات إزالة حساسية البيانات المشتركة واستيقانها وإزالتها.

ز) في ظل القدرة على إنتاج معلومات عن التهديدات المعرضة لها المركبات الموصولة، توصى المنظمات بتبادل معلومات التهديدات مع المنظمات الحسنة السمعة.

التذييل I

أفضل الممارسات لمركز تبادل وتحليل المعلومات المتعلقة بصناعة السيارات (Auto-ISAC) في مجال أنشطة تبادل معلومات التهديدات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

أصدر مركز تبادل وتحليل المعلومات المتعلقة بصناعة السيارات [b-AUTO-ISAC] في عام 2019 الإصدار 3.1 من دليل أفضل الممارسات المعنون *"التعاون والعمل مع الأطراف الثالثة المناسبة"*. وفي دليل أفضل الممارسات هذا، يورد المركز أفضل ممارسات تبادل المعلومات، بما يشمل الأطراف الثالثة المعنية ومستوى الانفتاح ونوع المحتوى الذي سيُستفاد من تبادله وعمليات تبادل المعلومات، وغيرها من عناصر هذه الممارسات.

فلتعزيز الأمن السيبراني للمركبات الموصولة، قد تتعاون المنظمات المعنية وتعمل مع عدة أنماط من الأطراف الثالثة في جميع مستويات النظام الإيكولوجي لهذه المركبات. وتشمل الأطراف الثالثة المعنية الجهات الشريكة لصناعة المركبات الموصولة والمنظمات العاملة في هذه الصناعة والحكومات والمؤسسات الأكاديمية والباحثين ووسائط الإعلام.

وبوسع المنظمة المعنية أن تحدد درجة الانفتاح التي تناسبها على أساس خصوصية أهدافها المتعلقة بالأمن السيبراني للمركبات وتفرُّد مشهد المخاطر فيها. ويمكن تقسيم درجات الانفتاح إلى محدود ومعتدل وواسع.

وتتضمن الإجراءات الرئيسية لتبادل المعلومات فيما بين مختلف الجهات صاحبة المصلحة ما يلي:

أ) تحديد المحتوى الذي سيُستفاد من تبادله.

ب) إشراك الجهات الداخلية المناسبة من الجهات صاحبة المصلحة.

ج) استحداث إجراءات لاعتماد المعلومات المشتركة ولاتخاذ إجراءات استناداً إليها.

د) استحداث إجراءات لإحالة المعلومات إلى أطراف ثالثة خارجية.

هـ) الحصول على الأدوات والتكنولوجيات المناسبة.

التذييل II

منهجية لتقييم أهمية معلومات التهديدات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

عند تقييم أهمية جميع معلومات التهديدات، يمكن للمنظمات المعنية أن تُجري هذا التقييم على أساس خمسة عوامل على نحو المسرود أدناه:

أ) مدى موثوقية مصادر معلومات التهديدات: إذ تختلف درجة موثوقية هذه المصادر، وتستطيع المصادر التي تحظى بدرجة عالية من الموثوقية أن تقدم معلومات قيمة عن التهديدات.

ب) الإطار الزمني: إن قيمة معلومات التهديدات مرهونة زمنياً. فتلقِّي المعلومات في مرحلة مبكرة يمكن أن يساعد المنظمة المعنية في حماية أصولها ووقايتها من التعرض لهجمات.

ج) مدى اكتمال بيان المعلومات: عادةً ما تكون معلومات التهديدات المبينة بمزيد من التفاصيل ومن المعلومات السياقية أقيم.

د) مدى علاقة المعلومات بالمنظمة وتأثيرها عليها: فبعض معلومات التهديدات تستهدف صناعة محددة أو منتجات محددة بل حتى شركات محددة. فلا بد من أن تكون علاقة المعلومات بالمنظمة المعنية ملحوظة جداً.

هـ) مدى فعالية معلومات التهديدات: حيث يتسبب تعدد مصادر معلومات التهديدات في ازدواجية المعلومات أو تعارضها. ومن الممكن أن يسهم دمج التهديدات المتشابهة وتحديد مدى أصالة معلومات التهديدات في تعزيز فعالية هذه المعلومات في المنظمة.

بيبليوغرافيا

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

[b-ISO/IEC 27000] ISO/IEC 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*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2023