الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1209

(2010/12)

السلسلة X: شبكات المعطيات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

قُدُرات تقاسم وتبادل معلومات الأمن السيبراني وسيناريوهاتها المناظرة

التوصيـــة ITU-T X.1209

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

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

التوصيـــة ITU-T X.1209

قُدُرات تقاسم وتبادل معلومات الأمن السيبراني وسيناريوهاتها المناظرة

الملخص

تتناول التوصية ITU-T X.1209 بالوصف سيناريوهات رفيعة المستوى لتقاسم معلومات الأمن السيبراني وتبادلها وما يدعمها من قُدُرات. وتقدم هذه التوصية قدرات مهمة لدعم قابلية التشغيل البيني بين تطبيقات تقاسم معلومات الأمن السيبراني وتبادلها.

ويمكن استخدام القدرات المعروضة في سيناريوهات/مواقف تدعم كيانات فاعلة كانت مستقلة من قبل لتشارك في جهود مختلفة منسقة مثل منع تصرف مستهدف أو إيقافه أو تنسيق جهود التحليل والتحديد.

والهدف من القدرات المُدرجة والموصوفة هنا هو دعم عمليات أمن أكثر فاعلية وكفاءة عن طريق دعم تقاسم المعلومات وتبادلها بشكل متبادل بين أطراف موثوق بها تعمل معاً لمراقبة أمن الأنظمة والشبكات ورعايته وإدارته بشكل عام.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1209	2010/12/17	17

الكلمات المفتاحية

معلومات الأمن السيبراني، تقاسم المعلومات، تبادل المعلومات

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة 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 رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظـــة

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 "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" 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 الاختراع 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 قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

المحتـــويات

الصفحة

التوصيـــة ITU-T X.1209

قُدُرات تقاسم وتبادل معلومات الأمن السيبراني وسيناريوهاتها المناظرة

1 مجال التطبيق

تقدم هذه التوصية قدرات مهمة لدعم قابلية التشغيل البيني بين تطبيقات تقاسم معلومات الأمن السيبراني وتبادلها. ومن أجل ذلك، تحتوي الفقرة 7 أوصافاً لسيناريوهات استعمال رفيعة المستوى تُستعمل لتهيئة السياق من أجل القُدرات الواردة في الفقرة 8. ولزيادة توضيح الغرض من هذه القدرات، تضم الفقرة 9 أوصاف القدرات التي يُرجح أن يتطلبها كل موقف.

والجمهور المستهدف لهذه التوصية هو كل من له دور في عمليات الأمن المعتمدة.

2 المراجع

لا توجد.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلح التالي المعرَّف في وثائق أخرى:

1.1.3 الأمن السيبراني [التوصية b-ITU-T X.1205]: مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية. ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتضم الأهداف العامة للأمن ما يلي:

- التيسُّر
- السلامة، التي قد تضم الاستيقان وعدم الرفض
- السرية.

2.3 مصطلحات معرّفة في هذه التوصية

تُعرّف هذه التوصية المصطلح التالي:

1.2.3 معلومات الأمن السيبراني: معلومات أو معارف مهيكلة قد تتضمن على سبيل المثال لا الحصر: "حالة" المعدات أو البرمجيات أو أنظمة الشبكات، والأدلة القضائية المتعلقة بالوقائع أو الأحداث؛ والأطراف المنفذة لقدرات تبادل المعلومات المتعلقة بالأمن السيبراني؛ ومواصفات تبادل المعلومات المتعلقة بالأمن السيبراني بما في ذلك الوحدات والمخططات والأرقام المخصصة، والهويات، ونعوت الثقة لكل ما سبق ومتطلبات التنفيذ ومبادئه التوجيهية وممارساته.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

DDoS الرفض الموزع للخدمة *(Distributed Denial of Service)*

FTP بروتوكول نقل الملفات *(File Transfer Protocol)*

HTTP بروتوكول نقل النصوص الموسوعية *(Hyper-Text Transfer Protocol)*

HTTPS بروتوكول النقل الآمن للنصوص الموسوعية (البروتوكول HTTP عبر طبقة مقبس آمن) (*Secure-Hyper-Text Transfer Protocol (HTTP over SSI)*)

IPS نظام منع الاقتحام *(Intrusion Prevention System)*

5 الاصطلاحات

لا توجد.

6 المقدمة

يزداد انتشار الهجمات السيبرانية، التي تتضمن الفيروسات والديدان وغير ذلك، سرعةً من خلال الشبكات باستخدام تقنيات متنوعة لا تفتأ تتطور لتتخذ أشكالاً أكثر خطورة. وقد طُورت حلول أمنية متنوعة، من بينها مكافحة الفيروسات وكشف برامج التجسس وجدران الحماية والشبكات الافتراضية الخاصة وكشف الاقتحام والحماية منه وغير ذلك، حتى يمكن مجابهة الحوادث الأمنية الناتجة عن مثل هذه الهجمات الخطيرة بنظام للاستجابة السريعة من خلال اتخاذ تدابير مضادة فعالة.

وقد اتخذ خط الدفاع الأكثر شيوعاً ضد الانتهاكات والفيروسات والديدان والبرمجيات الروبوتية لدى المسؤولين عن إدارة الأمن أساساً شكل منتديات نقاش متنوعة يشترك فيها الكثير من محترفي الأمن. وفي العادة تُسد الثغرات وتُرتق مواطن الضعف خلال مدة تتراوح بين يومين وأسبوع تعود الأمور بعدها إلى أوضاعها الطبيعية.

ولكنه من المؤسف أن من شأن استغلال الفيروسات والديدان والبرمجيات الروبوتية لنقاط الضعف أن يؤدي إلى انتشارها بسرعة عاليةً جداً عبر الشبكات، ففي خلال ثوانٍ معدودات، يمكن أن تتأثر شبكات بأكملها تأثراً بالغاً.

يمكن تبادل معلومات الأمن السيبراني ضمن منظمة ما بشكل سريع. غير أن تبادل مجموعة واسعة من المعلومات بين المنظمات غير مدعوم بشكل كاف باستخدام الطرائق الحالية. ومن شأن افتقاد وسائل اتصال فعالة أن يجعل من كل منظمة جزيرة منعزلة فيما يتعلق بالأمن.

ولذلك فإنه من المهم أن تتقاسم منظمات كثيرة معلومات الأمن السيبراني فيما بينها، بمن فيهم مشغلو الاتصالات ومورّدو خدمات الاتصالات ومراكز عمليات الأمن. وتتطلب إمكانية تحقيق تبادل المعلومات على هذا النحو ما يلي:

- طرائق آمنة وموثوق بها يستخدمها المشاركون في تبادل المعلومات بشكل أسرع،
- طرائق تكفل حماية الخصوصية.

وتقدم هذه التوصية سيناريوهات جرى بحثها وما يدعمها من قدرات لتبادل معلومات الأمن السيبراني بين المشاركين بطريقة آمنة وموثوق بها ويمكن الاعتماد عليها.

7 سيناريوهات القدرات

في سبيل وضع القدرات المذكورة في البند 8 ضمن سياق سليم من أجل فهم هذه التوصية، تضم هذه التوصية سيناريوهات استعمال رفيعة المستوى مقدمة في خمس تشكيلات مختلفة للمساعدة في شرح مجموعات القدرات المنطقية الخمس الواردة أدناه.

1.7 السيناريو العام

ينطبق هذا السيناريو العام على كل السيناريوهات التالية له.

السيناريو: يتقاسم شركاء تبادل المعلومات ما يتعلق بالأحداث والوقائع الأمنية من معلومات قد تفيد في التعرف على الهجمات العدوانية على شبكاتهم ومنعها.

ويمثل الجانب الهام في هذا السيناريو في أنه يمكن للطرفين جمع أنماطٍ متشابهة من البيانات ولكن من مصادر مختلفة و/أو في أنساق مختلفة و/أو محتويات مختلفة اختلافاً طفيفاً من أنماط متشابهة من البيانات.

2.7 السياسات التشغيلية

يصف هذا السيناريو حالة تُفرض فيها على شركاء تبادل المعلومات المختلفين قيود للنفاذ إلى مختلف عناصر المعلومات الخاضعة للتقاسم.

السيناريو: يبرم شركاء تبادل المعلومات اتفاق عمل لتقاسم المعلومات المتعلقة بالأحداث والوقائع الأمنية.

ومن الجوانب المهمة لهذا السيناريو أنه من الممكن تقييد النفاذ إلى معلومات كلّ من شركاء تبادل المعلومات من خلال منح النفاذ على أساس علاقة ثقة قائمة سابقًا. ومن الجوانب المهمة أيضًا إمكانية ربط الثقة الموضوعة في المعلومات الواردة بعلاقة الثقة القائمة.

3.7 السياسات الإقليمية

يصف هذا السيناريو وضعًا يتعدد فيه شركاء تبادل المعلومات وتكون لدى هؤلاء الشركاء المختلفين قيوداً قانونية و/أو تنظيمية مختلفة بشأن عناصر مختلفة تنتمي إلى نفس نمط المعلومات الخاضعة للتقاسم. وعلى نفس منوال السيناريو السابق، يبرز هذا السيناريو كذلك إمكانية أن يُسمح لأحد الأطراف التقاسم في معلومات لا يُسمح له نفسه بالنفاذ إليها أو الاطلاع عليها بالفعل.

ويختلف هذا السيناريو عن سابقه باختلاف مصدر القيود الموضوعة على تبادل المعلومات. ففي السيناريو السابق تنشأ القيود عن سياسات تشغيلية يحددها كلّ شريك من شركاء تبادل المعلومات، بينما تنشأ في هذا السيناريو عن سياسات تشغيلية مفروضة من جهات خارجية، مثل الولايات القضائية الإقليمية.

السيناريو: يستطيع طرفان يعمل كلٌ منهما في إقليم مختلف تبادل معلومات بمقتضى متطلبات مختلفة يفرضها عليهما كل إقليم.

ويتمثل الجانب الهام لهذا السيناريو في أنه بالإضافة إلى اختلاف السياسات التشغيلية لدى كل طرف، فقد تكون هناك أيضاً سياسات مرتبطة بالإقليم الذي يجري فيه تبادل المعلومات.

4.7 نسق التبادل

السيناريو: يقدم واحد من شركاء تبادل المعلومات معلومات – تتضمن المنافذ أو نطاقات المنافذ المعنية – إلى شريك ثانٍ بشأن نمط من الحركة ذي مسلك مثير للمشاكل. وتستخدم المعلومات المتقاسمة للتعرف على وقائع هجمة معينة.

ويتمثل الجانب الهام لهذا السيناريو في ضرورة أن تكون محتويات المعلومات المتبادلة سهلة الفهم على شركاء تبادل المعلومات المعنيين ومتفقاً عليها فيما بينهم.

5.7 حماية الخصوصية

تبرز السيناريوهات التي يتضمنها هذا البند قضايا مختلفة متعلقة بالخصوصية، سواء كانت "الخصوصية" مؤسسية أو شخصية. وبالإضافة إلى ذلك، فهي تبرز الحاجة إلى القدرة على ضمان خصوصية عمليات تبادل المعلومات نفسها.

- السيناريو: يتولى مركز عمليات أمنية جمع المعلومات المتعلقة بأي هجمة خبيثة على إحدى الشبكات أو الأنظمة أو – بشكل أعم – الأصول التي يديرها. ومن ثم ترسل هذه المعلومات إلى مورّد خدمات شبكية لتحديد مصدر أو مصادر الهجمة الخبيثة المعنية.

  ويتمثل الجانب الهام لهذا السيناريو في قدرة مورّد الخدمات الشبكية على التعرف بنفسه على المصدر/المصادر المشتبه في شنها الهجوم دون أن يلزمه الكشف عن تلك المعلومات لمركز العمليات الأمنية.

- السيناريو: قد تحتوي مجموعة المعلومات الكاملة التي جمعها أحد شركاء تبادل المعلومات على عناصر ربما يرغب في الكشف عنها لشركاء تبادل المعلومات ضمن مؤسسته أو عملياته لكنه لا يرغب في الكشف عنها لمن هم خارج نطاق عملياته.

  ويتمثل الجانب الهام لهذا السيناريو في تمتّع أطراف تبادل المعلومات بالحرية في اختيار تقاسم كل المعلومات المتاحة أو مجموعة فرعية منها، أو أن يُخفوا، بشكل أو بآخر، جانباً من المعلومات التي يتقاسمونها أو كلها.

- السيناريو: يتبادل طرفان معلومات حساسة عبر شبكات "عمومية".

  ويتمثل الجانب الهام لهذا السيناريو في ضرورة ضمان خصوصية المعلومات المتبادلة بصرف النظر عن وسيلة الاتصال المستخدمة.

6.7 تجزئ النفاذ

يُبرز هذا السيناريو وضعاً يُسمح فيه بتقاسم أنماط أو عناصر مختلفة من المعلومات الأمنية تحت ظروف مختلفة وحسب هذه الظروف.

السيناريو: تُنشر خدمةٌ ما توجيهات إرشادية وتحذيرات مجانًا أو على أساس اشتراك مدفوع لتوصيل مستويات مختلفة من المعلومات حسب تعريف الخدمات لاشتراكٍ ما بعينه.

ومن الأمثلة على اختلاف المستويات إتاحة بيانات غير معالجة على مستوىً معين، بينما تُتاح بيانات غير معالجة ومعالجة على مستوىً مختلف.

ويتمثل الجانب الهام لهذا السيناريو في احتمال إتاحة "مستويات" مختلفة من المعلومات لمختلف الأطراف الثانية، حتى ولو كانت كل المعلومات المتاحة من نمط واحد.

7.7 التحقق من المصدر

يُبرز هذا السيناريو الحاجة إلى الاستيقان من شركاء تبادل المعلومات.

السيناريو: يتلقى أحد شركاء تبادل المعلومات معلومات من شريك ثانٍ ويتحقق من ورود تلك المعلومات بالفعل من الشريك الثاني.

ويتمثل الجانب الهام لهذا السيناريو في ضرورة تحقق الأطراف التي تتبادل معلومات فيما بينها من ورود المعلومات من المرسل المعني بالفعل وليس من طرف ثالث يحاول تقمص هوية المرسل المعني.

8.7 التوزيع متعدد القنوات

على الرغم من تشابه هذا السيناريو مع "تجزئ النفاذ"، فإنه يبرز وضعًا قد تتاح فيه مستويات مختلفة من المعلومات باستخدام طرائق مختلفة.

السيناريو: يُتيح أحد شركاء تبادل المعلومات إخطارات وتنبيهات أمنية عبر وسائل مختلفة وتحت ظروف متباينة. وقد تتاح البيانات للتنزيل من دليل قابل للبحث مجانًا أو ترسل عبر البريد الإلكتروني لأحد مستويات الخدمة يتم اختياره أو تتاح في نسق قابل للقراءة والنفاذ إليه من آلة لمستوى خدمة آخر.

ويتمثل الجانب الهام لهذا السيناريو في إمكانية إتاحة معلومات من نمط واحد أو أنماط مختلفة عبر مجموعة متنوعة من الوسائل وتحت ظروف متباينة.

9.7 التوافق العكسي

السيناريو: بعد مرور زمن على شريكي تبادل معلومات وهما يتبادلان بالفعل معلومات معينة باستخدام أنساق وبروتوكولات معينة، يُتاح معيار جديد يدعم طرائق تبادلهما الحالية حيث يقدم وظائف جديدة وإضافية.

ويتمثل الجانب الهام لهذا السيناريو في ضرورة دعم التطبيقات القائمة إلى أبعد حد ممكن مع تزويدها في نفس الوقت بمسار للترقية تحسبًا لظهور معايير جديدة.

8 القُدُرات

تسرد البنود التالية مختلف القدرات التي تدعم أنماط السيناريوهات المذكورة أعلاه في الفقرة 7.

1.8 قُدرات النسق/التشفير

- يجب أن يكون نسق المعلومات الأمنية وبنيتها معروفين ومفهومين لكلا الطرفين.
  - تتسم المعلومات الأمنية المتبادلة بطبيعة غير متجانسة، ومثال ذلك رسائل وتوقيعات جُدُر الحماية أو غير ذلك من تجهيزات أمن الشبكات، إضافة إلى الأنماط المختلفة من المعلومات المتعلقة بشكل خاص بكل تطبيق مثل تقارير الإبلاغ عن الأحداث والوقائع والتحليل والاستجابة وتبادل بيانات الأدلة القضائية وما إلى ذلك.
  - يمثل نسق المعلومات المتبادلة أنماطًا متنوعة من المعلومات الأمنية المتولدة عن بيئات أنظمة غير متجانسة والقابلة للتطبيق عليها.
- يجب أن تتاح إمكانية تقاسم أنماط متنوعة من المعلومات المتعلقة بالأمن. ويتضمن ذلك على سبيل المثال لا الحصر توقيعات مسلك الحركة وتوقيعات النفاذ إلى النظام وعنوان (عناوين) بروتوكول الإنترنت للمصدر ونطاقات منافذ المصدر و/أو المقصد وما إلى ذلك.
- يجب أن تتمكن الأطراف من إدراج مستويات مختلفة من المعلومات، بدءًا بمحتويات رزمة واحدة وصولاً إلى كل الرزم المعرضة لهجوم DDoS واسع.
- يجب أن تكون محتويات المعلومات الأمنية معروفة ومفهومة لكلا الطرفين.
- يجب أن تتاح إمكانية التعرف على موضوع المعلومات وإمكانية استعمالها وتطبيقها.

2.8 قُدرات النقل/التبادل

- يجب أن تتمكن الأطراف من نقل المعلومات الأمنية وتسليمها وتسلمها عبر نطاق واسع وقابل للامتداد من وسائط التوزيع والإرسال.
- ربما يلزم أن تدعم التطبيقات عمليات التبادل المتزامن وغير المتزامن بين الأطراف خلال تقاسم المعلومات الأمنية وتبادلها.
- ربما يلزم أن تدعم التطبيقات توصيل المعلومات على أساس الإرسال والاستقبال والاشتراك.
- يلزم أن تدعم التطبيقات التشغيل المستقر أثناء تبادل كميات كبيرة من المعلومات الأمنية وتبادلها.

- يجب أن توظف بروتوكولات التبادل المستخدمة البروتوكولات القائمة المستخدمة على نطاق واسع بالفعل، و/أو أن تنبني عليها.

3.8 قُدرات الأمن

- يجب أن تتاح إمكانية الاستيقان من معلومات الأمن السيبراني الخاضعة للتقاسم والتبادل والتحقق منها.
- يجب أن تدعم التطبيقات موثوقية المعلومات وسريتها وسلامتها وتيسرها.
- يجب أن يتاح التعرف على الأطراف المعنية على نحوٍ مستيقن منه وقابل للتحقق.
- يجب أن تمنع التطبيقات الهجمات على أي تقاسم أو تبادل لمعلومات الأمن السيبراني الناتجة عن تزوير و/أو تزييف في المعلومات المتضمَّنة أو في مصدر/مقصد المعلومات المتضمّنة.
- يجب أن تتاح لأطراف المصدر القدرة على التأكد من عدم إطّلاع أي أطراف غير مصرح لها على معلومات حساسة. والهدف من هذا المطلب هو توفير خصوصية الاتصالات ويبقى قائمًا سواء كانت الخصوصية مطلوبة لمعلومات شخصية معرفة أو معلومات مؤسسة خاصة أو أي شيء يعتبر الحفاظ على خصوصيته وعدم إتاحته لإطّلاع أشخاص غير مصرح لهم أمرًا مهماً.
- يجب أن تتاح لأطراف المصدر القدرة على التحكم في النفاذ على مستوىً جزئي بحيث لا يتمكن من النفاذ إلى عناصر محددة ضمن جزء معين من المعلومات الأمنية إلا الأطراف المصرح لها بذلك دون النفاذ إلى عناصر لم يُصرح لهم بها.
- يجب أن تتاح للأطراف القدرة على تأمين المعلومات المتعلقة بالأمن من نفاذ أطراف غير مصرح لها إليها حتى وإن كان ذلك في بيئة مفتوحة تتاح فيها المعلومات المتعلقة بالأمن للجميع، بما في ذلك الأطراف غير المصرح لها.

4.8 قُدرات السياسات

- يجب أن تتاح لكل طرف على حدة القدرة على تعريف السياسات المتعلقة بتوفير معلومات الأمن السيبراني و/أو النفاذ إليها – سواء كانت محلية و/أو إقليمية – والإعلان عنها. ومن أمثلة ذلك عدم الإفصاح عن معلومات التسيير التي يحتمل انكشافها في عناوين المقصد على أنها مسألة "سياسة".
- يجب أن يتاح للأطراف القدرة على توفير معلومات أمنية والنفاذ إليها على نحوٍ يتسق مع سياسات كل منهم المطبّقة فيما يتعلق بتوفير معلومات أمنية و/أو النفاذ إليها.
- يجب أن تتاح للأطراف القدرة على الإعلان عن الولاية القضائية التي تنطبق في نطاقها مجموعة محددة من إعلانات السياسات.
- يجب أن تتاح لكل طرف على حدة القدرة على تعريف متطلبات وقيود الولاية القضائية المحتملة فيما يتعلق بتوفير معلومات أمنية و/أو النفاذ إليها ضمن ولايته القضائية والإعلان عنها.
- يجب أن تتاح لكل طرف القدرة على توفير المعلومات الأمنية والنفاذ إليها على نحو يتماشى مع متطلبات ولايته القضائية.

5.8 قُدرات حياديّة البائعين

في سبيل دعم تقاسم وتبادل أوسع نطاق ممكن من معلومات الأمن السيبراني، يجب أن توفر التطبيقات خدماتها بأقل قدر ممكن من الاعتماد على نظام أي بائع محدد أو بيانات خاصة حصرياً ببائع معين. وفي نفس الوقت، يُفضّل ألا تُستبعد أنظمة أي بائع محدد أو بياناته كذلك.

9 قابلية القُدرات للتطبيق

توفر السيناريوهات والقدرات الموضحة في هذه التوصية مجموعة من "الأدوات" المميّزة التي يمكن للمرء أن يمزج بينها في استخداماته لإنشاء تطبيقه. وربما لا تحتاج بعض التطبيقات الأقل تعقيداً مثل تطبيقات تجميع البيانات و/أو البحث في المعلومات البسيطة إلا لعدد قليل من القدرات المذكورة، فيما قد تحتاج تطبيقات أخرى ثرية بالخصائص وتوفر خدمات أوسع إلى الجمع بين مزيدٍ من القدرات وتنفيذها.

وفيما يلي تناول للحالات التي ربما تزيد فيها الحاجة إلى أنماط محددة من القدرات، والحالات التي قد يغلب عليها الطابع الاختياري.

1.9 قُدرات النسق/التشفير

يتعيّن في أي تقاسم وتبادل لمعلومات الأمن السيبراني أن يتمكن كلٌ من مرسل المعلومات ومستقبلها من فهم ما يتبادلان من محتوى بدقة تامة. وعلى ذلك، تنطبق قدرات النسق والتشفير على كلٍ من السيناريوهات التي يجري من خلالها تقاسم معلومات الأمن السيبراني و/أو تبادلها.

2.9 قُدرات النقل/التبادل

بنفس أهمية قدرات النسق والتشفير، يحتاج أي شريكين ضالعين في تبادل المعلومات أو أكثر إلى طريقة لتوصيل المعلومات من الطرف المرسل إلى الطرف المستقبل.

3.9 قُدرات الأمن

لا يكاد يفيد تبادل المعلومات المتعلقة بالأمن ما لم يتوافر على الأقل قدر ما من الضمان الأمني يكفي للوقوف على هوية الشريكين المتبادلين ولتأمين أي قناة اتصال بينهما.

ومع ذلك، فإن المتطلبات الأمنية تختلف باختلاف الأوضاع والتطبيقات، ولذلك فإن من المهم أن يدرس القائمون على التكييف وعلى التنفيذ احتياجات تطبيقاتهم على وجه الخصوص دراسة وافية.

فمن الممكن، على سبيل المثال، أن يجري التبادل بين شريكين في تطبيق ما عبر خط اتصال مخصص منفذ عليه تدابيره الأمنية الخاصة، وفي هذه الحالة تقل أو تنعدم كلية الحاجة إلى اعتبارات أمنية خاصة فوق ما توفره بيئة التبادل بالفعل.

ومن جهة أخرى، إذا أُتيحت المعلومات باستخدام قنوات اتصال مفتوحة للنفاذ العمومي، فيرجح أن توجد حاجة إلى نطاق عريض من التدابير الأمنية.

4.9 قُدرات السياسات

لا تنسحب الحاجة إلى توظيف قدرة الإعلان عن قيود و/أو حدود و/أو تصاريح على كل التطبيقات التي تدعم وظائف تقاسم وتبادل معلومات الأمن السيبراني. ومع ذلك، فإن إمكانية الإعلان عن مثل هذه الأنماط من المعلومات المتعلقة بالسياسات تمثل أهمية في كثير من الأوضاع التجارية والشخصية.

وكما هو الشأن في قدرات الأمن، ففي الظروف أو الأوضاع التي تتوفر فيها الوظائف المتعلقة بالسياسات خارج نطاق تطبيق ما – ربما بسبب اتفاقات تشغيلية أو تعاقدية – فربما لا توجد حاجة إلى إمكانية إعلان سياسات وفرضها ضمن التطبيق نفسه.

5.9 قُدرات حيادية البائعين

تعتمد حيادية البائع إلى حد كبير جدًا على الأوضاع. فإذا كان المرء يتقاسم أو يتبادل بيانات مولدة من منتج بائع معين باستخدام نسق تبادل و/أو بروتوكولات تبادل ذلك البائع، فهنا لا تنطبق حيادية البائع بالقطع.

وعلى الجانب الآخر، إذا كان تطبيق ما يستهدف أوسع تطبيق ودعم لتبادل المعلومات، ففي هذه الحالة يعتبر الحفاظ على موقف حيادي فيما يتعلق بالطرائق و/أو المعلومات الخاصة ببائع معين أمراً مهمّاً.

التذييل I

مقدمة إلى تقاسم معلومات الأمن السيبراني وتبادلها

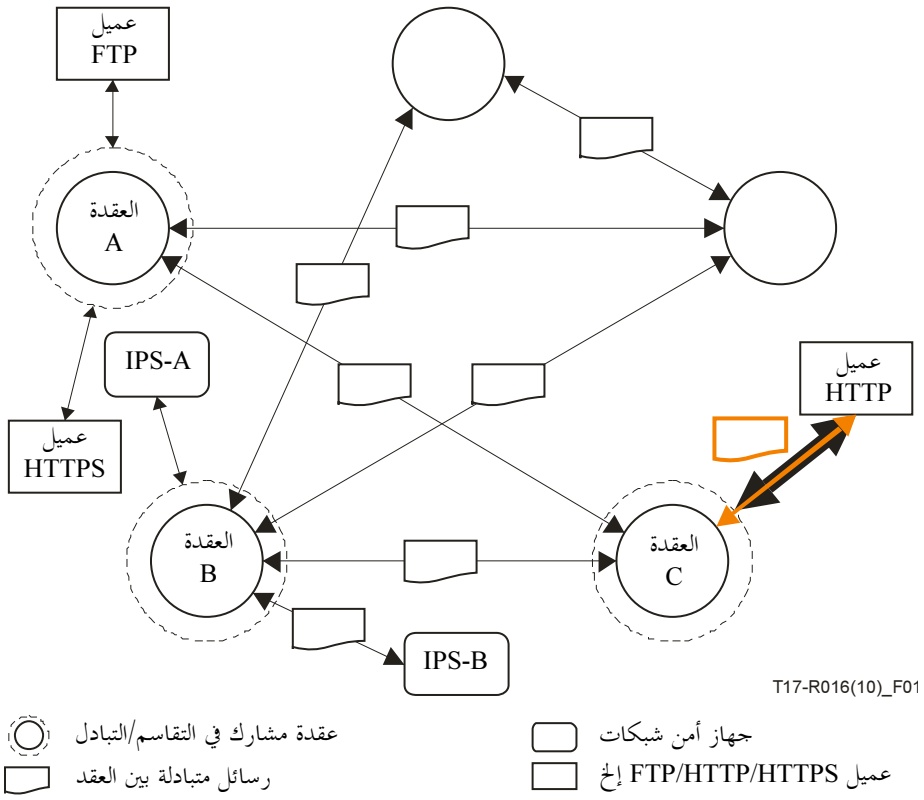
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يتناول هذا التذييل بالوصف البنية المفاهيمية لنموذج من تطبيقات معلومات الأمن السيبراني كما يبين الشكلان I.1 وI.2. ويظهر في الشكلين عرضان مختلفان لطوبولوجيا التطبيق مفعّلان بالقدرات المذكورة في البند 7. وبالرغم من احتمال وجود طوبولوجيات أخرى، فإن الطوبولوجيا المبينة تتضمن استخدام كل القدرات، فيما لا تحتاج الطوبولوجيات المحتملة الأخرى إلا إلى مجموعة جزئية من القدرات الموضحة.

ويبيّن الشكل الأول سيناريو شركاء تقاسم متعدّدين، لكلّ منهم وظائف وتطبيقات ومعلومات متقاسمة مختلفة. وهو يبين طرائق مختلفة لكيفية النفاذ إلى معلومات من عقدة ما من جانب تطبيقات تستخدم هذه المعلومات.

وجدير بالملاحظة أن هذا التذييل لا يقيد كيفية استخدام المعلومات ولا الغرض منه، بل يكتفي ببيان إمكانية النفاذ إليها عبر وسائل شتى. كما يبين الشكل الأول أن كل عمليات التبادل بين العقد مدعومة من خلال استخدام نسق تراسل معياري.

أما الشكل الثاني فهو عرض ثلاثي الأبعاد للشكل الأول يبين شريكي تبادل معلومات نموذجيين ويوضح القدرات التي يتعيّن على كلّ منهما في الغالب تنفيذها من أجل المشاركة في عملية التبادل. وكما كان شأن الشكل الأول، ربما لا يحتاج الأمر في التنفيذ أو التطبيق الفعلي إلى كل الوظائف التي تدعمها كل القدرات المذكورة، مما يتيح قدراً من الحرية في اختيار الوظائف المطلوب تضمينها فعلياً في أي تنفيذ/تطبيق بعينه.



الشكل I.1 – مثال لنشر عملية تقاسم وتبادل معلومات الأمن السيبراني

- تتواصل كل العقد المشاركة فيما بينها عبر رسائل معيارية.

تمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

  – قدرات النسق/التشفير (الفقرة 1.8)

  – قدرات النقل/التبادل (الفقرة 2.8)

- تقدّم البيانات المطلوبة من عقدة ما فعلياً عن طريق عقدة أخرى.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

  – قدرات الأمن (الفقرة 3.8)

  – قدرات السياسات (الفقرة 4.8)

- اقتصار عقدة ما على تنفيذ البروتوكولات الإطارية فقط أو قد تتيح البيانات الإطارية من خلال بروتوكولات/ خدمات أخرى، كأن يُستخدم البروتوكولان FTP أو HTTP للنفاذ إلى البيانات الإطارية من العقدة A.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

  – قدرات النسق/التشفير (الفقرة 1.8)

  – قدرات النقل/التبادل (الفقرة 2.8)

  – قدرات حيادية البائعين (الفقرة 5.8)

- إمكانية نفاذ تجهيزات الأمن مثل نظام منع الاقتحام (IPS-A) ونظام آخر لمنع الاقتحام (IPS-B) الموصلة بالعقدة B إلى معلومات الأمن السيبراني إما مباشرة، مثل حالة IPS-B، أو عبر خدمة التفاف، مثل حالة IPS-A، مما يسمح للأجهزة بالانتفاع بوظيفة التقاسم والتبادل إما بالأسلوب المعياري لتقاسم معلومات الأمن السيبراني وتبادلها أو باستخدام طرائق تعتمد على الأجهزة أو طرائق مسجلة الملكية.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

  – قدرات النسق/التشفير (الفقرة 1.8)

  – قدرات النقل/التبادل (الفقرة 2.8)

  – قدرات حيادية البائعين (الفقرة 5.8)

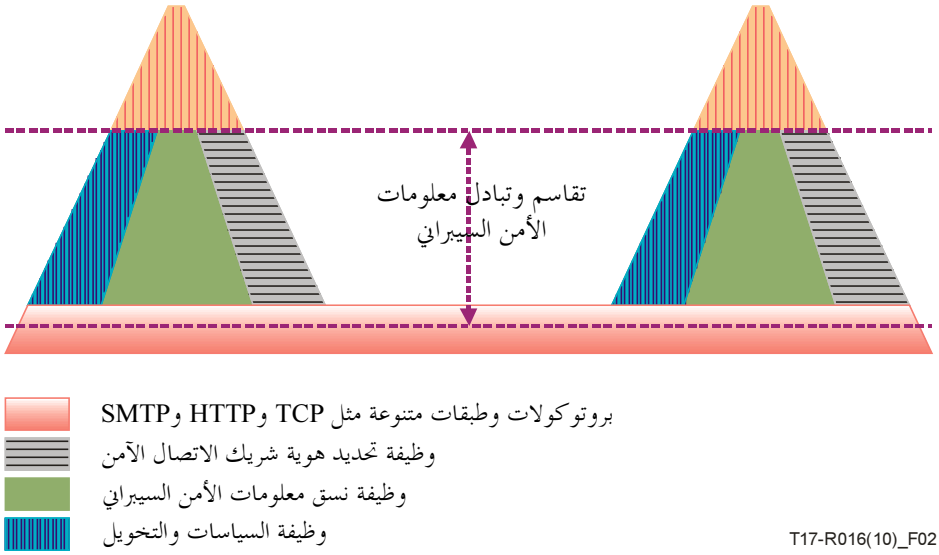
- إمكانية استخدام جهاز أمن لأي بروتوكول أو طبقة بروتوكولات تدعم حمل الرسائل مثل TCP/IP وHTTP وHTTPS وSSL مما يستخدمه العملاء الذين يطلبون خدمات من العقدة C.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

  – قدرات النسق/التشفير (الفقرة 1.8)

  – قدرات النقل/التبادل (الفقرة 2.8)

  – قدرات حيادية البائعين (الفقرة 5.8)



الشكل 2.I – منظور بعقدتين

- إمكانية تبادل الطلبات والردود بين العقد المشاركة من خلال مختلف البروتوكولات وطبقات البروتوكولات.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

– قدرات النسق/التشفير (الفقرة 1.8)

– قدرات النقل/التبادل (الفقرة 2.8)

- بالنسبة إلى كثير من التطبيقات، يلزم وجود طرائق موثوق بها للتعرّف على هوية شركاء الاتصال.

تمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

– قدرات الأمن (الفقرة 3.8)

– قدرات السياسات (الفقرة 4.8)

- إمكانية حيازة العقد لبيانات مقدمة من عقد أخرى واستخدامها.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

– قدرات النسق/التشفير (الفقرة 1.8)

– قدرات الأمن (الفقرة 3.8)

– قدرات السياسات (الفقرة 4.8)

– قدرات حيادية المورّدين (الفقرة 5.8)

- إمكانية استخدام التطبيقات مختلف وظائف التحقق من التخويل وفاء بمختلف المتطلبات الأمنية ذات الصلة كما يقتضي الحال حسب التطبيق.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

– قدرات السياسات (الفقرة 4.8)

- احتمال احتياج التطبيقات في مختلف العقد إلى الاستفادة من معلومات الهوية من عقد أخرى لأسباب متنوعة، كأن يطلب أحد عملاء العقدة A النفاذ إلى معلومات الأمن السيبراني المتاحة في العقدة B، مثلاً.

وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:

– قدرات السياسات (الفقرة 4.8)

- تتمثل الوظائف الأساسية لأي عقدة مشاركة فيما يلي:
  - تلقّي معلومات الأمن السيبراني.
  - تخزين/أرشفة معلومات الأمن السيبراني.
  - خدمة طلبات معلومات الأمن السيبراني.

  وتمثل القدرات التالية أهمية في سبيل دعم الوظائف المذكورة:
  - قدرات النسق/التشفير (الفقرة 1.8)
  - قدرات النقل/التبادل (الفقرة 2.8)
  - قدرات السياسات (الفقرة 4.8)
- إمكانية استخدام التطبيقات لأدوات ذات صلة، مثل الاستيقان والتحقق من التخويل للتعامل مع المسائل المتعلقة بالنفاذ.

  وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:
  - قدرات الأمن (الفقرة 3.8)
  - قدرات السياسات (الفقرة 4.8)
- إمكانية استخدام التطبيقات لنموذج بيانات موحّد للتعامل مع المسائل المتعلقة بالنفاذ بين العقد.

  وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:
  - قدرات النسق/التشفير (الفقرة 1.8)
  - قدرات النقل/التبادل (الفقرة 2.8)
  - قدرات حيادية البائعين (الفقرة 5.8)
- إمكانية استخدام التطبيقات معرفات هوية موثوق بها في الاتصالات بين العقد وبين العملاء على السواء.

  وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:
  - قدرات الأمن (الفقرة 3.8)
  - قدرات السياسات (الفقرة 4.8)
- اعتبار الطلبات والردود بين العقد وبعضها بمثابة "معيار" مع إمكانية تقديم التطبيقات سطح بيني لطبقة التطبيق بين طلبات وردود العقد إلى العملاء لأولئك العملاء الذين لا يطبقون الطرائق و/أو البروتوكولات المعيارية المستخدمة بين العُقد.

  وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:
  - قدرات النسق/التشفير (الفقرة 1.8)
  - قدرات النقل/التبادل (الفقرة 2.8)
  - قدرات حيادية البائعين (الفقرة 5.8)
- دعم الإطار أسلوبي الإرسال والاستقبال إضافة إلى أسلوبي عمل الحالة المستقلة والحالة المتكاملة.

  وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:
  - قدرات النقل/التبادل (الفقرة 2.8)
- إمكانية توفير معماريات التطبيقات "نقاط دخول" إلى ما قد تحتاجه التطبيقات من نماذج تحديد الهوية وبيانات تحديد الهوية الموثوق بها.

  وتمثل القدرات التالية أهمية في سبيل دعم هذه الوظيفة:
  - قدرات الأمن (الفقرة 3.8)
  - قدرات السياسات (الفقرة 4.8)

التذييل II

أنشطة ذات صلة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II المعلومات الأمنية العامة

المعلومات الأمنية العامة هي معلومات أمنية مفتوحة تقدمها منظمات لا تستهدف الربح مثل CERT/CC أو MITRE أو Open Project. فعلى سبيل المثال، توجد معلومات مواطن الضعف والتعرض الشائعة (CVE) وسرد مواطن الضعف الشائعة (CWE) وسرد البرمجيات الخبيثة الشائعة (CME) وسرد وتصنيف أنماط الهجمات الشائعة (CAPEC) وقاعدة بيانات مواطن الضعف مفتوحة المصدر (OSVDB) والتوقيعات التي توفرها [b-Snort] أو [b-Bro] وما إلى ذلك.

وفي حالة MITRE، فإن CVE تمثل دليلاً بالمعلومات المعروفة للجمهور عن مواطن الضعف والتعرّض الأمنية. وهو يُستخدم كأساس لقاعدة بيانات مواطن الضعف الوطنية (NVD) التي طوّرها المعهد الوطني للمعايير والتكنولوجيا بالولايات المتحدة. وتوفر CWE مجموعة موحدة وقابلة للقياس من مواطن ضعف البرمجيات تتيح مزيداً من الفعالية في مناقشة ووصف واختيار واستخدام أدوات وخدمات أمن البرمجيات التي تستطيع اكتشاف مواطن الضعف هذه في شفرة المصدر والأنظمة التشغيلية. وتوفر CME معرّفات هوية فريدة ومشتركة للتهديدات الفيروسية الجديدة ولمعظم التهديدات الفيروسية السائدة للتخفيف من ارتباك الجماهير أثناء حوادث البرمجيات الخبيثة. وهذه ليست محاولة لاستبدال المنتجات المستخدمة للفيروسات وغيرها من البرمجيات الخبيثة والتي تحمل اسم شركة معينة، بل لتيسير اعتماد إمكانية فهرسة مشتركة ومحايدة للبرمجيات الخبيثة. وتوفر CAPEC دليلاً متاحاً للجمهور بأنماط الهجمات إضافةً إلى مخطط شامل للتصنيف.

أما عن OSVDB، فهو مشروع مستقل وقاعدة بيانات مفتوحة المصدر من إعداد المجتمع المعني بالأمن ومخصصة لاستخدامه. والغرض منه أن يقدم معلومات تقنية دقيقة ومفصلة وحديثة ومحايدة بشأن مواطن الضعف الأمنية. وستوفر كذلك قدراً أكبر وأكثر انفتاحاً من التعاون بين الشركات والأفراد، مع تفادي تكرار الأعمال وخفض المصروفات المرتبطة ضمنياً بتطوير قواعد بيانات مواطن الضعف الأمني وصيانتها داخلياً.

ويوجد نظام مفتوح المصدر اسمه Snort يكتشف محاولات اقتحام الشبكات ويمنعها باستخدام لغة موجهة بالقواعد ويجمع بين فوائد طرائق التفتيش القائمة على التوقيعات والبروتوكولات والمسلك غير الطبيعي. وقد خضعت قواعد هذا النظام لاختبارات صارمة إزاء نفس المعايير التي يستخدمها فريق أبحاث مواطن الضعف (VRT) للعملاء.

وأخيرًا هناك مشروع مفتوح المصدر اسمه Bro قائم على اكتشاف محاولات اقتحام الشبكات عن طريق مراقبة حركة الشبكة بشكل منفعل ويبحث عن أي نشاط مشبوه. وتصف قواعد هذا النظام الأنشطة أو ما هي الأنشطة التي تستحق التنبيه أو التوقيعات التي تصف هجمات معروفة أو نفاذًا إلى مواطن ضعف معروفة.

2.II المعلومات الأمنية الجديدة

المعلومات الأمنية الجديدة عبارة عن توقيعات مولدة بشكل أوتوماتي لما يستجد من التهديدات أو الهجمات أو الحركة غير الطبيعية أو دودة غير معروفة وما إلى ذلك. وقد حظي موضوع توليد توقيعات الهجمات مؤخرًا باهتمام بحثي مكثف، مما أدى إلى اقتراح حلّين تجريبيين مثل "Early bird" و"Polygraph". ويتمثل الدور الأساسي لهذين الحلّين في اكتشاف الهجمات السيبرانية والتقاط تسلسلات البايتات التي تمثل هوية الهجمة. وتوفر خدمة التوقيع FirstLight أو الحماية النشطة من البرمجيات الخبيثة في Endeavor Security وZASMIN (البنية التحتية لإدارة توقيعات هجمات يوم الصفر) في ETRI توقيعات جديدة تخضع للتحديث والمراجعة والتوسيع بشكل متواصل. وهذه التكنولوجيا لتوليد أنماط متقدمة تتيح لنا توليد توقيعات بشكل أوتوماتي على أساس حركة الهجمات. وبالرغم من إحراز تقدم في تحسين جودة التوقيعات، فما زال تقاسم التوقيعات في مراحلها المبكرة.

3.II أنشطة ذات صلة بتقاسم المعلومات الأمنية

1.3.II أفرقة الاستجابة للحوادث الحاسوبية (CIRT)

تدرس أفرقة الاستجابة للحوادث الحاسوبية (CIRT) مواطن الضعف الأمني في الشبكات وتبحث في التغيرات طويلة المدى في أنظمة الشبكات وتضع معلومات ودورات تدريب للمساعدة في تحسين الأمن. وهي تواصل الاستجابة للحوادث الأمنية الكبرى وتحلل مواطن الضعف في المنتجات. ومع الزيادة السريعة في حجم الإنترنت واستخدامها في وظائف حيوية، حدثت تغيّرات مطّردة في تقنيات الاقتحام وزيادة في حجم الأضرار وصعوبة أكبر في اكتشاف الهجمات وضبط المهاجمين.

2.3.II الوكالة الأوربية لأمن الشبكات والمعلومات

قدمت الوكالة الأوربية لأمن الشبكات والمعلومات (ENISA) أول دراسة جدوى بشأن نظام أوروبي لتقاسم المعلومات والإنذار (EISAS) لتوعية المؤسسات الصغيرة والمتوسطة الحجم (SME) والمواطنين في الاتحاد الأوروبي بالتهديدات ومواطن الضعف والهجمات. وتخلص دراسة الجدوى إلى أن الأسلوب الأمثل أمام الاتحاد الأوروبي لتيسير تقاسم المعلومات هو الاضطلاع بدور المسهّل والمنسّق للمناقشات و"الراعي للممارسات الجيدة" بين أنظمة تقاسم المعلومات والإنذار الوطنية بدلاً من القيام بوظيفة مركزية تشغيلية بنفسه. ومن أجل إجراء الدراسة، تم افتراض إمكانية إقامة نظام أوربي لتقاسم المعلومات والإنذار وضرورة التحقق منه. ويمثل النظام الأوروبي لتقاسم المعلومات والإنذار نموذجاً عاماً يتألف من ثلاثة مكوّنات رئيسية، وكان المقصود من هذا النموذج هو الوقوف على المجالات الوظيفية التي يستطيع النظام EISAS تقديم قيمة مضافة إلى أنشطة تقاسم المعلومات القائمة في الدول الأعضاء وعلاج الثغرات في التغطية مع معلومات أمن الشبكات والمعلومات. والمكونات الثلاث هي مكون جمع المعلومات (IGC) ومكون معالجة المعلومات (IPC) ومكون نشر المعلومات (IDC).

3.3.II منتدى أفرقة الأمن والاستجابة للحوادث

منتدى أفرقة الأمن والاستجابة للحوادث (FIRST) هو المنظمة الأولى والرائدة المعتمدة عالمياً فيما يتعلق بالاستجابة للحوادث. وتتيح عضوية هذا المنتدى لأفرقة الاستجابة للحوادث أن تستجيب بمزيدٍ من الفعالية لوقائع الأمن كردّ فعل أو استجابة استباقية. ويجمع هذا المنتدى بين مجموعة متنوعة من أفرقة الاستجابة لحوادث الأمن الحاسوبية تنتمي إلى منظمات حكومية وتجارية وتعليمية. ويهدف هذا المنتدى إلى تعزيز التعاون والتنسيق في تفادي الحوادث وحفز ردود الفعل السريعة للحوادث والنهوض بتقاسم المعلومات بين الأعضاء وفي المجتمع بشكل عام.

4.3.II فريق منطقة آسيا والمحيط الهادئ للاستجابة للطوارئ الحاسوبية

يتعاون فريق منطقة آسيا والمحيط الهادئ للاستجابة للطوارئ الحاسوبية (APCERT) مع أفرقة الاستجابة للطوارئ الحاسوبية (CERT) وأفرقة الاستجابة لحوادث الأمن الحاسوبية (CSIRT) لضمان أمن الإنترنت في منطقة أسيا والمحيط الهادئ، وهذا التعاون يتمحور حول التقاسم الفعلي للمعلومات والثقة والتعاون. وهو ييسر تقاسم المعلومات وتبادل التكنولوجيا، بما في ذلك المعلومات الأمنية والفيروسات والبرمجيات الخبيثة، بين أعضاء المنطقة. كما يعزز الفريق أعمال البحث والتطوير المشتركة بشأن الموضوعات التي تحظى باهتمام أعضائه ويقدم توصيات للمساعدة على التعامل مع المسائل القانونية المتعلقة بالمعلومات الأمنية والاستجابة للطوارئ عبر الحدود الإقليمية.

5.3.II مركز تقاسم المعلومات وتحليلها لأغراض الاتصالات

تشكل الإنترنت وغيرها من شبكات الاتصالات القاعدة لهيكل اجتماعي واقتصادي على مستوىً عالمي. وقد أصبح ضمان أمن المعلومات القضية الأكثر إلحاحاً في الحياة الاجتماعية والاقتصادية.

ويهدف مركز تقاسم المعلومات وتحليلها لأغراض الاتصالات (Telecom-ISAC) إلى جمع المعلومات المتعلقة بالحوادث وتحليلها وتقاسمها واتخاذ تدابير فورية لضمان تشغيل خدمات الاتصالات بصورة مستقرة وخالية من المشاكل. وعلاوة على ذلك، فقد أنشأ هذا المركز منتدىً يضم نطاق عريض من الأعضاء المتعاونين الذين يتقاسمون أفكارهم وتجاربهم، بما في ذلك المعلومات المتعلقة بالمخاطر الأمنية ومواطن الضعف والحلول الأمنية وخلاف ذلك.

التذييل III

أنشطة ذات صلة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

[APCERT] فريق آسيا والمحيط الهادئ للاستجابة للطوارئ الحاسوبية، http://www.apcert.org

[CERT] فريق استجابة للطوارئ الحاسوبية، http://www.cert.org

[ENDEAVOR] شركة Endeavor للأمن، http://www.endeavorsecurity.com

[FIRST] منتدى أفرقة الأمن والاستجابة للحوادث، http://www.first.org

[MITRE] شركة MITRE، http://makingsecuritymeasurable.mitre.org/

[Telecom-ISAC] مركز تقاسم معلومات الاتصالات وتحليلها، https://www.telecom-isac.jp

[WIKI] الويكيبديا، http://en.wikipedia.org

ثُبت المراجع

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity.*

[b-Bro] Bro (November 2004), *Quick Start Guide Manual*.

[b-EISAS] European information sharing and Alert System (2006/2007), *A feasibility study.*

[b-OSVDB] Open Source Vulnerability DataBase. *Project Aims and Objectives.*

[b-Snort] Snort (May 2008), *Snort User Manual 2.8.2*.

[b-ZASMIN] Information Security Research Division of ETRI, *Zero-day Attack Signature Management Infrastructure*

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
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	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) 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
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
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 وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2011