الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1207

(2008/04)

السلسلة X: شبكات المعطيات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الاتصالات

مبادئ توجيهية لموردي خدمات الاتصالات للتصدي لمخاطر برمجيات التجسس والبرمجيات المحتملة غير المطلوبة

التوصيـــة ITU-T X.1207

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات المعطيات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للمعطيات	
الخدمات والمرافق	X.19–X.1
السطوح البينية	X.49–X.20
الإرسال والتشوير والتبديل	X.89–X.50
مظاهر الشبكة	X.149–X.90
الصيانة	X.179–X.150
الترتيبات الإدارية	X.199–X.180
التوصيل البيني للأنظمة المفتوحة	
النموذج والترميز	X.209–X.200
تعريفات الخدمات	X.219–X.210
مواصفات بروتوكول بأسلوب التوصيل	X.229–X.220
مواصفات بروتوكول بأسلوب دون توصيل	X.239–X.230
جداول إعلان عن مطابقة تنفيذ بروتوكول	X.259–X.240
تعرّف هوية البروتوكول	X.269–X.260
بروتوكولات الأمن	X.279–X.270
أشياء مسيرة على الطبقة	X.289–X.280
اختبار المطابقة	X.299–X.290
التشغيل البيني للشبكات	
اعتبارات عامة	X.349–X.300
الأنظمة الساتلية لإرسال البيانات	X.369–X.350
الشبكات القائمة على بروتوكول الإنترنت	X.379–X.370
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	
توصيل الشبكات	X.629–X.600
الفعالية	X.639–X.630
نوعية الخدمة	X.649–X.640
التسمية والعنونة والتسجيل	X.679–X.650
ترميز نحو مجرد واحد (ASN.1)	X.699–X.680
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	
الإطار والهيكل المعماري لإدارة الأنظمة	X.709–X.700
خدمة اتصالات الإدارة وبروتوكولاتها	X.719–X.710
هيكل معلومات الإدارة	X.729–X.720
وظائف الإدارة ووظائف الهيكل المعماري للإدارة الموزعة المفتوحة	X.799–X.730
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	
الالتزام والتلازم والاستعادة	X.859–X.850
معالجة المعاملات	X.879–X.860
العمليات البُعدية	X.889–X.880
التطبيقات التنوعية للترميز نحو مجرد واحد (ASN.1)	X.890-X.899
المعالجة الموزعة المفتوحة	X.999–X.900
أمن الاتصالات	**X.1000–**

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

التوصيـــة ITU-T X.1207

مبادئ توجيهية لموردي خدمات الاتصالات للتصدي لمخاطر برمجيات التجسس والبرمجيات المحتملة غير المطلوبة

ملخص

يرد في هذه التوصية مبادئ توجيهية لموردي خدمات الاتصالات للتصدي لمخاطر برمجيات التجسس والبرمجيات المحتملة غير المطلوبة. وتشجع التوصية اتباع أفضل الممارسات حول المبادئ المتعلقة بإصدار إخطارات واضحة والحصول على موافقة المستعمل على خدمات الاستضافة على الويب لموردي خدمات الاتصالات (TSP) وتحكمهم فيها. وتضع التوصية وتشجع أفضل الممارسات للمستعملين فيما يخص أمن الحواسيب الشخصية (PC)، بما في ذلك استعمال برمجيات مكافحة تكنولوجيات التجسس، ومكافحة الفيروسات، واستعمال جدران الحماية الشخصية، وبرمجيات تحديث أمن أنظمة العميل.

المصدر

وافقت لجنة الدراسات 17 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 18 أبريل 2008 على التوصية ITU-T X.1207 بموجب الإجراء الذي ينص عليه القرار 1 للجمعية العالمية لتقييس الاتصالات.

عبارات مفتاحية

برمجيات مضللة، السلامة على الإنترنت، برمجيات محتملة غير مطلوبة، برمجيات تجسس.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. 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/.

© ITU 2008

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

المحتـــويات

الصفحة

1 مجال التطبيق 1

2 المراجع 1

3 التعاريف 1

4 المختصرات والصيغ المقتضبة 1

5 الاصطلاحات 2

6 نظرة عامة 2

7 الأهداف 3

8 البرمجيات المضللة وبرمجيات التجسس 3

9 لماذا تعتبر البرمجيات المضللة وبرمجيات التجسس مهمة 3

10 التوصيات 4

11 توجيهات لموردي خدمات الاتصالات (TSP) 4

1.11 إدارة المخاطر المتعلقة بأمن المعلومات في المشروع التجاري 4

2.11 متطلبات السلامة والأمن المتعلقة بخدمات الاستضافة على الويب 6

3.11 إرشادات بشأن سلامة المستعملين النهائيين وأمنهم 8

التذييـــل I – موارد إضافية 10

1.I المراجع المباشرة على الإنترنت المتعلقة بالأمن ومكافحة برمجيات التجسس 10

2.I قائمة نموذجية بجهات الاتصال المعنية بتصاعد الأحداث الأمنية 12

ثبت المراجع 12

مبادئ توجيهية لموردي خدمات الاتصالات للتصدي لمخاطر برمجيات التجسس والبرمجيات المحتملة غير المطلوبة

1 مجال التطبيق

تشكل هذه التوصية جزءاً من مجموعة توجيهات وضعها قطاع تقييس الاتصالات لتحسين حالة الأمن السيبراني. وهي تغطي متطلبات خط الأساس لممارسات السلامة والأمن التي يتبعها موردو خدمات الاتصالات (TSP) والمستعملون النهائيون، مع التركيز على معالجة مسألة برمجيات التجسس وغيرها من البرمجيات المحتملة غير المطلوبة، والضارة و/أو المضللة. ويشير تعبير موردي خدمات الاتصالات (TSP) في سياق هذه التوصية، إلى موردي خدمات الاتصالات الذين يقدمون خدمات ذات صلة بشبكة الإنترنت، وخصوصاً خدمات الاستضافة على الويب المقدمة لدوائر الأعمال، وخدمات النفاذ إلى الإنترنت للمستعملين النهائيين.

2 المراجع

لا يوجد.

3 التعاريف

يُستعمل تعبير برمجيات التجسس بصورة عامة ليشمل عدة أشكال من البرمجيات التي تظهر سلوكيات معينة تنطوي على التطفل على خصوصية المستعمل النهائي دون مبرر. وضماناً لاستعمال التعبير على نحو متسق ومفهوم بشكل عام، يرد فيما يلي تعريف عملي لبرمجيات التجسس وما يتصل بها من برمجيات مضللة.

1.3 البرمجيات المضللة: برمجيات تؤدي أنشطة في حاسوب مستعمل ما دون أن تقوم بما يلي: 1) إخطاره أولاً بما ستفعله بالضبط في حاسوبه؛ أو 2) تطلب منه ما إذا كان موافقاً على قيامها بذلك. وتشمل أمثلة البرمجيات المضللة، البرامج التي تختطف تشكيلات المستعمل، أو البرامج التي تتسبب في ظهور نوافذ فجائية للإعلانات لا نهاية لها يتعذر على المستعمل إغلاقها بسهولة.

2.3 البرمجيات المحتملة غير المطلوبة: يشير التعبير إلى عدة أشكال من البرمجيات المضللة، تشمل البرمجيات الضارة كالفيروسات، والديدان (worms)، وأحصنة طروادة (Trojans)، والبرمجيات غير الضارة التي لها خصائص البرمجيات المضللة وبرمجيات التجسس.

3.3 برمجيات التجسس: تعرف هذه التوصية برمجيات التجسس باعتبارها نوعاً معيناً من البرمجيات المضللة التي تجمع معلومات شخصية من حاسوب مستعمل ما. ويمكن أن تشمل هذه المعلومات الشخصية مسائل كمواقع الويب التي كثيراً ما يزورها المستعمل أو معلومات أكثر حساسية ككلمات السر.

4 المختصرات والصيغ المقتضبة

تستعمل هذه التوصية المختصرات والصيغ المقتضبة التالية:

CERT فريق الاستجابة لحالات الطوارئ المتعلقة بالحاسوب *(Computer Emergency Response Team)*

CIRT فريق الاستجابة للأحداث المتعلقة بالحاسوب *(Computer Incident Response Team)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

ISMS نظام إدارة أمن المعلومات *(Information Security Management System)*

ISMS-T نظام إدارة أمن المعلومات – متطلبات الاتصالات
(Information Security Management System – Requirements for Telecommunications)

ISV بائع مستقل للبرمجيات *(Independent Software Vendor)*

SQL لغة الاستفسار المركبة *(Structured Query Language)*

TSP مورد خدمات الاتصالات *(Telecommunication Service Provider)*

URI معرف المورد الموحد *(Uniform Resource Identifier)*

5 الاصطلاحات

لا يوجد.

6 نظرة عامة

أتاح انتشار شبكة الإنترنت ظهور مشاريع أعمال جديدة وحقق للمستهلك فوائد كثيرة في المنـــزل وفي مكان العمل. وقد أدى الانفتاح الملازم للإنترنت، والتوصيل البيني والنفاذ السريع اللذين توفرهما، إلى نموها أيضاً لتصبح أداة فعالة للاتصالات لدوائر الأعمال والمستهلكين، فضلاً عن استخدامها في أغراض التسويق التجاري على نطاق كبير. واستُغِل في السنوات الأخيرة هذا الانفتاح وسهولة الاتصال والتوصيلية استغلالاً مطرداً من جانب المجرمين السيبرانيين ومروجي أعمال الاحتيال من خلال استعمال مختلف أشكال البرمجيات الضارة من أجل تحقيق مكاسب مالية وتحقيق أغراض إجرامية أخرى.

وبرمجيات التجسس والبرمجيات المضللة واحدة من تحديات السلامة والأمن التي تزداد دلالة، وهي قادرة على تعريض معلومات المستعمل النهائي الشخصية للخطر، وإلحاق خسائر فادحة بإنتاجيته، وتقويض ثقته وتعويله على الاضطلاع بأعمال مشروعة على الإنترنت.

وتتجه غالباً أطراف عديدة إلى موردي خدمات الاتصالات (TSP)، وخاصة الهيئات التنظيمية وعملاء المنشآت، من أجل توفير خدمات مأمونة ومضمونة للمستعملين النهائيين (بمن فيهم المستهلكين وعملاء المنشآت). وعندما تستضيف شبكة موردي TSP مواقع شبكة الويب، ويكتشف استضافتها لمحتويات ضارة، تشمل برمجيات تجسس وبرمجيات مضللة تؤثر على سلامة وأمن أنظمة حاسوب المستعملين النهائيين، كثيراً ما يلجأ إلى موردي TSP طلباً للمساعدة في معالجة هذه المسائل، ومن شأن استمرار هذه الأحداث وتواتر حدوثها مراراً أن يؤثر على الثقة والطمأنينة في موردي خدمات الإنترنت في توفير خدمات آمنة ومضمونة. ومن شأن هذا الأمر أن يؤدي إلى عدم ارتياح المستهلك للخدمة وإلى نزوحه إلى مورد خدمة آخر.

ومن منظور تنظيمي، تطالب هيئات تنظيمية في بلدان كثيرة موردي خدمات الاتصالات بتقديم ضمانات بشأن تدابير الأمن والسلامة التي تتخذها، ويطلبون من الموردين أن يفعلوا المزيد لمساعدة المستهلكين والمستعملين النهائيين على الاضطلاع بأنشطة حوسبة مأمونة ومضمونة عبر الإنترنت.

ونظراً لهذه التغيرات التي طرأت على ساحة السلامة والأمن على الإنترنت، فإنه من الضروري أن يعتمد موردو خدمات الاتصالات مجموعة من المعايير تتعلق بأفضل الممارسات التي يمكن الاعتراف بها في الصناعة ككل باعتبارها أدنى خط أساس[1] من شأنه أن يكفل تقديماً مأموناً ومضموناً لخدمات الإنترنت التي تستضيفها شبكات موردي خدمات الاتصالات، وأن يعزز أيضاً الممارسات ذات الصلة التي يتبعها المستعملون النهائيون المشتركون في شبكات الموردين. كما سيسمح تطبيق معيار خط الأساس لموردي خدمات الاتصالات لكي يبيِّنوا للهيئات التنظيمية وللمستعملين النهائيين مطابقة المعيار لأفضل الممارسات المتبعة في الصناعة، ويعززوا ثقة وطمأنينة الهيئات التنظيمية، إن لم يصونوها، وتعويلهم على سلامة وأمن شبكات الموردين وخدماتهم.

[1] لا يوجد حالياً خط أساس من هذا القبيل، وتعتبر هذه التوصية خطوة نحو رسم هذا الخط الأساس الأدنى.

7 الأهداف

ترمي أهداف هذه التوصية إلى ما يلي:

1) تشجيع اتباع أفضل الممارسات حول المبادئ المتعلقة بإصدار إخطارات واضحة، والحصول على موافقة المستعمل على خدمات الاستضافة في الشبكة، وضوابطها؛

2) وتشجيع (موردي خدمات الاتصالات) على اتباع أفضل الممارسات الأمنية للمستعملين في المنازل بشأن الاستعمال المأمون والمضمون للحواسيب الشخصية والإنترنت، بما في ذلك استعمال برمجيات مكافحة الفيروسات، وبرمجيات مكافحة التجسس، واستعمال جدران الحماية الشخصية، والتحديثات الأمنية الأوتوماتية.

8 البرمجيات المضللة وبرمجيات التجسس

والعنصر المشترك، الذي تتقاسمه جميع البرمجيات المضللة (بما فيها برمجيات التجسس) الذي يميزها عن التطبيقات المشروعة، هو عدم إخطارها المستعمل ومنحه حق الاختيار. والأهم من ذلك، أن من الملاحظ عموماً أن الكثير من المهام البرمجية التي تؤديها البرمجيات المضللة/برمجيات التجسس يمكن أن توفر فوائد للمستعمل، إذا كشفت عن هويتها، وحصلت على ترخيص من المستعمل وتحكمه فيها. فيمكن مثلاً أن تسهل هذه البرامج من إضفاء الطابع الشخصي، وتمكن من إجراء تغييرات التشكيلة بموافقة المستعمل وتقدم إعلانات معتمدة يمكن بدورها أن تدعم مالياً تكلفة خدمة عالية القيمة كخدمة البريد الإلكتروني. وخلاصة القول، فإن البرمجيات المضللة ليست مشكلة تكنولوجية عموماً، ولكنها مشكلة تنشأ غالباً عن سلوك البرمجيات التضليلي أو التدليسي.

وأصبحت البرمجيات المضللة وبرمجيات التجسس على الصعيدين العالمي والمحلي على حد سواء، على قمة المسائل التي تتناولها الحكومات والصناعة والمستهلكون على أعلى مستوى، وهي تمضي أبعد من معلمات إحدى المسائل المتعلقة "بسياسات تكنولوجيا المعلومات". وإن كانت البرمجيات المضللة تستعمل بوضوح الإنترنت والحاسوب كوسيط لها، فإن سلوكها التضليلي يسبب أساساً مشكلة تتعلق بحماية المستهلك.

9 لماذا تعتبر البرمجيات المضللة وبرمجيات التجسس مهمة

تسبب هذه البرمجيات على صعيد المستهلك انحطاطاً لحوسبة المستعمل و/أو تجربته مع الإنترنت (إلى المدى الذي تجعل فيه الحاسوب غير قابل للاستعمال في بعض الأحيان) وتخلق شعوراً بالإحباط لدى المستعمل وتولد لديه تصوراً أن الأمر "خرج عن سيطرته". وليس من قبيل المبالغة الإشارة على مستوى المستهلك في المنـــزل، إلى أن هناك نسبة كبيرة من المستعملين تهددهم البرمجيات المضللة بتقويض كافة المنافع الاستثنائية التي تتيحها لهم الإنترنت والحوسبة في حد ذاتهما.

ومع أن البرمجيات المضللة تؤثر بوضوح تأثيراً كبيراً على المستهلكين، فإنها تمثل أيضاً مشكلة رئيسية للكثير من الشركات المعنية بتكنولوجيا المعلومات والاتصالات (ICT). فمن جهة، يعزو خطأً الكثير من العملاء سبب مشاكل تشغيل حواسيبهم إلى الجهات المصنعة للبرمجيات والمطورة لها، مما يلحق الضرر بسمعتها ويخلق تصورات خاطئة لدى العملاء عن منتجاتها. ومن الواضح أن المشاكل الناشئة عن البرمجيات المضللة تؤدي أيضاً إلى إنفاق ملايين الدولارات على نداءات لا داعي لها للحصول على الدعم في قطاعي البرمجيات والعتاد على حد سواء.

وكما لوحظ في الفقرة 6 أعلاه، فإن موردي خدمات الاتصالات ليسوا بمنأى عن التصدي للتحديات الناشئة عن برمجيات التجسس والبرمجيات المضللة، نتيجة استضافتهم لمواقع على شبكة الويب قد يستعملها مباشرة مروجو أعمال الاحتيال والمجرمون السيبرانيون لاستضافتهم فيها مباشرة، ومن ثم تقع الآثار السلبية لذلك مباشرة على المشتركين لدى موردي خدمات الاتصالات، الأمر الذي يدفعهم إلى الاتصال بالموردين طلباً للدعم والمساعدة. وفوق كل ذلك، تتوقع عادةً الهيئات التنظيمية والمستعملون النهائيون أن يطبق موردو خدمات الاتصالات تدابير مناسبة في مجال السلامة والأمن للتصدي لهذه المشاكل. وعندما يتخلى موردو خدمات الاتصالات عن مسؤوليتهم في معالجة هذه التحديات، فإن من شأن ذلك أن يقوض بطبيعة الحال سمعتهم وثقة المستعمل النهائي فيهم واطمئنانه إليهم.

10 التوصيات

من المرجح أن ينطوي أكثر السبل فعالية لمكافحة برمجيات التجسس على توليفة تجمع بين عدة استراتيجيات، تشمل مختلف أصحاب المصلحة، وذلك على النحو التالي:

- اتباع أفضل الممارسات السائدة في الصناعة، بتعاون جميع الأطراف الفاعلة الرئيسية من أجل تحديد برمجيات التجسس وغيرها من البرمجيات غير المطلوبة والتصدي لها؛
- تثقيف العميل عموماً، وتزويده بمورد موثوق للسبل الكفيلة بإزالة وتجنب برمجيات التجسس وغيرها من البرمجيات غير المطلوبة؛
- إيجاد حلول تكنولوجية ابتكارية للمساعدة في حماية المستعملين من برمجيات التجسس والبرمجيات المحتملة غير المطلوبة، والوقوف بحزم في وجه الاستغلال؛
- سن الحكومات لتشريعات وإنفاذها بمساعدة قطاع الصناعة لتثبيط استحداث البرمجيات المضللة وبرمجيات التجسس.

ويركز هذا المبدأ التوجيهي على توفير أفضل الممارسات السائدة في الصناعة وعلى تثقيف العميل بشكل عام بغية مساعدة مورد خدمات الاتصالات على أداء دور نشط في التصدي للبرمجيات المضللة وبرمجيات التجسس.

11 توجيهات لموردي خدمات الاتصالات (TSP)

سعياً إلى تقديم المساعدة في معالجة المسائل المتعلقة بالبرمجيات المضللة وبرمجيات التجسس، يركز هذا المبدأ التوجيهي على ثلاثة مجالات رئيسية، هي، الإدارة الداخلية لأمن منظومة موردي خدمات الاتصالات في حد ذاتها؛ ومتطلبات الأمن التي ينبغي أن يحددها الموردون لعملائهم المستضافين على شبكة الويب من أجل تطبيقها؛ والتوجيهات الأمنية المفيدة للمستعملين النهائيين (أو المشتركين) في خدمات النفاذ إلى الإنترنت. ويتكون هيكل التوصيات من ثلاثة أقسام فرعية خاصة كما يلي:

أ) إدارة المخاطر المتعلقة بأمن المعلومات في المشروع التجاري.

ب) متطلبات السلامة والأمن المتعلقة بخدمات الاستضافة على شبكة الويب.

ج) توجيهات بشأن سلامة المستعملين النهائيين وأمنهم.

1.11 إدارة المخاطر المتعلقة بأمن المعلومات في المشروع التجاري

1.1.11 نظام إدارة أمن المعلومات

ينبغي على مستوى المنشأة، تطبيق نظام رسمي لإدارة أمن المعلومات من أجل تحديد المخاطر المتعلقة بأمن المعلومات في دوائر الأعمال وإدارتها. وتوفر التوصية [b-ITU-T X.1051] التوجيهات وأفضل الممارسات لتطبيق هذا النظام.

وثمة اعتبار رئيسي يتعين أن يراعيه موردو خدمات الاتصالات في تنفيذهم توصيات النظام ISMS-T، يتمثل في ضمان أن يكون لدى مورد خدمة اتصالات، بوصفه منشأة منظمة، نظام يواصل تحديد المخاطر المتعلقة بأمن المعلومات وتقييمها ومعالجتها وإدارتها، فيما يتصل بتقديم المورد للخدمات عبر الإنترنت بصورة مباشرة إلى المستعملين النهائيين/المشتركين، وبصورة غير مباشرة عبر عملاء الخدمات المستضافين على شبكة الويب.

وسيتكون لدى موردي خدمات الاتصالات، من خلال الاضطلاع باستمرار بعمليات إدارة المخاطر بواسطة نظام ISMS-T، رؤية واضحة عن ملامح المخاطر، وسيتمكنون من تبيان سلامة شبكاتهم وخدماتهم للهيئات التنظيمية وسائر الأطراف المهتمة.

ويمكن أيضاً أن ينظر موردو خدمات الاتصالات في إصدار شهادات رسمية بشأن تقيدهم بتنفيذ توصيات ISMS-T، وذلك بموجب مخطط إصدار الشهادات ISO/IEC 27001.

وكجزء من تنفيذ توصيات ISMS-T، أو نظام إدارة أمن المعلومات المعني، ينبغي أيضاً أن ينشئ موردو خدمات الاتصالات قدرة لمراقبة الأحداث الأمنية والاستجابة لها، وأن ينسقوا أنشطة الاستجابة لهذه الأحداث مع المنظمات الخارجية العاملة في البلد والمعنية بأفرقة الاستجابة للأحداث المتعلقة بالحاسوب (CIRT) أو أفرقة الاستجابة لحالات الطوارئ المتعلقة بالحاسوب (CERT). وينبغي أن تشمل الاستجابة للأحداث مراقبة وتقييم الحالة الأمنية للمستعملين النهائيين والمواقع المُستضافة لشبكة الويب عبر شبكات موردي TSP، وتقدم توجيهات لمساعدة الأطراف المتأثرة في مجال الاستجابة بفعالية للأحداث الأمنية.

2.1.11 توفير منتجات آمنة ومضمونة

يمكن أن يستحدث[2] بعض موردي TSP ويطلق أشرطة أدوات لتصفح شبكة الويب، أو برمجيات مهاتفة، أو شفرات بصرف النظر عن نوعها، لتزويد المستعملين النهائيين بخدمات ذات قيمة مضافة، أو تسهيل سبل نفاذهم إلى خدمات الإنترنت. وينبغي في هذه الحالة إبرام اتفاق مناسب مع المستعمل النهائي يبين بلغة وعبارات واضحة سياسة التشفير التي يتبعها مورد خدمات الاتصالات، وسياسة الخصوصية، والوسائل التي يتمكن المستعملون بواسطتها من تغيير قبولهم لاحقاً أو تصعيد جميع المسائل التي قد يطرحونها فيما يخص السياسات والممارسات المُتبعة. وعند إبرام هذا الاتفاق، ينبغي أن يتأكد مورد خدمات الاتصالات من توقيع المستعمل النهائي للاتفاق كما ينبغي وحصوله على نسخة منه.

كما ينبغي أن يوثّق مورد خدمات الاتصالات سلوك الشفرة ويجري تقييماً لما إذا كان سلوكه يدخل في نطاق أية مجالات محتملة يمكن اعتبارها برمجيات تجسس أو برمجيات مضللة. وعلى المورد في الحالة الأخيرة أن يكلف بعدئذ جهة تقييم مؤهلة بما فيه الكفاية لتقييم مسألة ما إذا كانت الشفرة يمكن أن تدخل في نطاق أية معايير موضوعية يحددها بائع برمجيات مكافحة برامج التجسس والتقيد بأفضل الممارسات، لكي لا توسم أداة البرمجية التي يوفرها مورد خدمات الاتصالات للمستعمل النهائي باعتبارها برمجية تجسس/برمجية نشر التحذيرات. وينشر بائعون كثيرون لبرمجيات مكافحة برامج التجسس المعايير التي يستندون إليها في تقييم البرمجيات.[3]

وينبغي أن يطبق مورد خدمات الاتصالات توقيعاً بالشفرة الرقمية لرموزه الثنائية ليتسنى لبائعي برمجيات مكافحة برمجيات التجسس أن يحددوا بسهولة صاحب الملف، ويتسنى تصنيف البرمجيات التي تقوم الجهات المستقلة لبيع البرمجيات (ISV) على إنتاجها باتباع أفضل الممارسات، على اعتبارها مأمونة حتى قبل تحليلها.

وإذا اكتشف مورد خدمات الاتصالات تقنيات برمجية مفيدة يمكن أن تساعد في تخفيف مشكلة برمجيات التجسس، ينبغي أن ينظر المورد في إمكانية إقامة شراكة مع البائع والعمل معه من أجل إتاحتها على نطاق واسع.

3.1.11 مراقبة الشبكة والاستجابة

مراقبة الشبكات أمر شائع بين موردي خدمات الاتصالات ضماناً لموثوقية ونوعية الخدمات المقدمة على شبكاتهم. ويمكن في الوقت نفسه تعزيز هذه القدرة للبحث عن الحالات الاستثنائية للحركة في الشبكة والكشف عن الأنشطة الضارة التي تظهر على الشبكة. وينبغي عموماً أن يقوم مورد خدمات الاتصالات بما يلي:

- فهم الحركة على الشبكة – ما هي الحركة العادية، وما هي الحركة غير العادية.
- استعمال أدوات إدارة الشبكة لتحديد هوية التغييرات في الحركة، والحركة/المنافذ "غير العادية" وضمان إتاحة الأدوات اللازمة لتحديد الأسباب والاستجابة لها.
- اختبار قدرات الاستجابة قبل أن تكون هناك حاجة إليها في أحد الأحداث الفعلية. وتطوير تقنيات الاستجابة وعملياتها وأدواتها استناداً إلى نتائج التدريبات المنتظمة.

---

[2] إما داخلياً أو من خلال مورد طرف ثالث.

[3] يوجد أيضاً لدى التحالف المعني بمكافحة برمجيات التجسس، الذي يمثل عدة أطراف صناعية فاعلة، مجموعة تعاريف ومعايير تُنشر في موقعه على شبكة الويب. وللحصول على المزيد من المعلومات، انظر التذييل I.

- فهم المكونات الأساسية على أساس فردي – إذا بدأ فجأة أحد المستعملين غير النشطين عادة، باستعمال نسبة 100 في المائة من عرض النطاق المتيسر له، ربما يكون من الضروري عزله لحين اكتشاف الأسباب. ويمكن أن يمنع عزله عن الشبكة انتشار البرمجيات الضارة (البرمجيات المؤذية)، رغم أن بعض حالات التنفيذ قد تتطلب الحصول على موافقة المستعمل أو على تحديث شروط تقديم الخدمة.

4.1.11 الدعم والتصاعد

عادة ما يكون لدى مورد خدمات الاتصالات خدمة دعم للإجابة على استفسارات العملاء وتقديم المساعدة والدعم التقنيين اللازمين لمعالجة مشاكل المستعملين النهائيين. ومع تصاعد البرمجيات المؤذية عبر الإنترنت، يتلقى مورد خدمات الاتصالات تقارير تتعلق بحالات عدوى بهذه البرمجيات وبرمجيات التجسس وبمسائل في هذا الشأن. وهذه المعلومات مهمة ومفيدة للبائعين المعنيين لتقييم خطورة حالة البرمجيات المؤذية، وتقديم تحديثات للأدوات اللازمة لضمان إمكانية التخلص من جميع البرمجيات المؤذية وبرمجيات التجسس الجديدة التي يُكشف عنها أو وقفها بفعالية. وينبغي في هذا الصدد أن يتصل مورد خدمات الاتصالات ببائعي الخدمات الأمنية ويقدم إليها التقارير ذات الصلة وعينات من البرمجيات المؤذية من أجل متابعتها – وخصوصاً، إذا اتضح أن هناك حالة إقفال سائدة. ويحتفظ معظم البائعين بقائمة بريد إلكتروني لتلقي هذه التقارير/العينات من أجل تحليلها ومتابعتها. انظر مثلاً الجدول I.1.

5.1.11 مواكبة التطورات الأخيرة

ينبغي أن يقوم مورد خدمات الاتصالات، كجزء من تنفيذ توصيات ISMS-T المتعلقة بإدارة مخاطر أمن معلومات في المنشأة، وضماناً أيضاً لمواصلة المورد على متابعة أفضل الممارسات الصناعية ومواكبة آخر حالات التعرض للهجمات وحالات الاستغلال/الهجمات، بالمشاركة في المحافل المجتمعية أو الصناعية ذات الصلة لتقاسم أفضل الممارسات المتبعة والتعلم من زملائه الموردين.

ملاحظة – لمزيد من المعلومات، انظر التذييل I.

2.11 متطلبات السلامة والأمن المتعلقة بخدمات الاستضافة على الويب

يوفر معظم موردي خدمات الاتصالات خدمات استضافة على شبكة الويب عبر شبكاتهم ومراكز بياناتهم كجزء من خدمات الأعمال التي يقدمونها. وتصل هذه الخدمات إلى المستعملين النهائيين/المستهلكين و/أو مشاريع الأعمال الصغيرة، عندما يعيد المشتركون المستضيفون على الويب ترزيمها وبيعها مجدداً إلى المستعملين النهائيين. وفي حال أنشأ المشتركون المستضيفون على شبكة الويب مخدماً غير آمن، أو في حالة استضافة محتوى ضار في مواقعهم على شبكة الويب، يؤدي ذلك آثاراً سلبية على سلامة المستعملين النهائيين وأمنهم. وبناءً على ذلك، فإن من الضروري أن يحدد مورد خدمات الاتصالات معياراً أدنى لأفضل الممارسات المتبعة بشأن السلامة والأمن يتقيد به المشتركون المستضيفون على الويب كجزء من شروط الاتفاق المُبرم.

وينبغي أن تشمل شروط الاتفاق ما يلي:

أ) إخطارات واضحة، تصف ممارسات الأمن والخصوصية لمواقع الويب، وممارسات جمع البيانات، وسلوك أي شفرة (آلية المساعدة على التصفح)، التي يمكن أن يوزعها موقع الويب ويطبقها على الحاسوب الشخصي للمستعمل النهائي أو بيئة متصفح الويب.

ب) قبول المستعمل، الذي يسهل موافقته أو رفضه شروط الخدمات التي تصفها الإخطارات. ومن شأن ذلك أن يسمح للمستعملين بالتمييز والبت فيما إذا كان بإمكانهم قبول شروط الخدمة على هذا الأساس.

ج) ضوابط المستعمل، التي تسهل على المستعمل تغيير السياقات المحيطية أو إنهاء قبوله بهذا الشكل أو ذاك في أي وقت في المستقبل بعد إبرام الاتفاق الأولي.

والشروط ضرورية لضمان وضوح سلوك موقع الويب وممارساته أمام المستعملين النهائيين فيما يخص سلامتهم، وخصوصيتهم وأمنهم. وينبغي وضع الشروط بمساعدة أحد المهنيين القانونيين لضمان حماية مورد خدمات الاتصالات بموجبها أيضاً من التهم القانونية التي يُحتمل أن يوجهها إليه المستعلمون النهائيون بسبب الخسائر أو أضرار معينة تلحق بهم من جراء نشر محتويات ضارة على موقع الويب أو اتباع سياسات وممارسات غير واضحة على الموقع.

وعلاوة على الأحكام المتعلقة بحماية البيانات والخصوصية الشخصية وأحكام السلامة على موقع الويب، ينبغي أن يطالب مورد خدمات الاتصالات مواقع الويب المُستضافة على شبكته بتنفيذ مجموعة تدابير أمنية لأفضل الممارسات على مستوى التطبيق قبل التمكن من بثها مباشرة. وينبغي أن يشمل ذلك، على سبيل المثال لا الحصر، ما يلي:

أ) إرشادات بشأن ممارسات التطوير الآمن لمواقع شبكة الويب وتشفير صفحات الشبكة، تشمل ما يلي:

i) عرض إخطارات قصيرة عن الخصوصية تقدم موجزاً واضحاً ومقتضباً مكوناً من صفحة واحدة (بلغة الأشخاص العاديين) عن الممارسات الأساسية التي تتبعها الشركة فيما يتعلق بالخصوصية على الإنترنت، الأمر الذي يُمكن المستعملين من التوصل إلى خيارات أكثر وعياً بشأن تقاسم معلوماتهم على الإنترنت. وينبغي أن تكون الإخطارات القصيرة مطابقة لجميع المتطلبات التنظيمية وأن توفر وصلات إلى تصريحات قانونية كاملة ومعلومات أخرى ذات صلة، لكي يتسنى للعملاء الذين يرغبون في الحصول على المزيد من التفاصيل، أن ينقروا بسهولة على الوصلات لقراءة صيغة أطول من التفاصيل. وبإصدار إخطار واحد، يمكن أن يحصل العملاء على خبرة أكثر اتساقاً عن جميع خصائص الشركة، مصحوبة بمعايير وتوقعات الخصوصية نفسها الممتدة إلى مواقع كثيرة.

ii) والمناولة الآمنة للبصمات (Cookies).

iii) والتحقق الآمن من الدخل ومناولته بأمان منعاً للهجمات الشائعة من قبيل حقن SQL. ونظراً لاستعمال مواقع الإنترنت التي تجري زيارتها بشكل متزايد، لتوزيع الشفرات الضارة، يجب التحقق من الدخل والخرج بواسطة المحتوى النشيط والمحتوى الديناميي.

iv) والإعداد الآمن لنصوص صفحات الويب منعاً للهجمات الشائعة مثل التعرض لهجمات تجسس تطبيقات الويب على مواقع الغير (Cross-site Scripting).

v) واستعراض واختبار أمن الشفرة.

وكجزء من البنية الأساسية لاستضافة شبكة ويب لمورد خدمات الاتصالات، ينبغي أيضاً اتخاذ التدابير الأمنية الواردة أدناه لحماية مخدمات الويب من النفاذ غير المرخص إليها وتعريضها لخطر المحتويات الضارة المضيفة، مثل البرمجيات المضللة وبرمجيات التجسس، وذلك كما يلي:

ب) تشكيل مخدم الويب، بما في ذلك أنظمة التشغيل الأساسية وفقاً لدليل خط الأساس لتشكيلة الأمن. وينبغي أن يشمل ذلك أيضاً تعريفاً مناسباً لمستعمل مخدم الويب إزاء الجهة القائمة على إدارته، ويعزز ضوابط النفاذ إلى البرامج وأدلة الأنظمة والملفات، وتخويل قنوات التدقيق، وخصوصاً فيما يتعلق بأحداث أمن النظام والأعطال الأخرى للنظام؛ ويوصى أيضاً بتركيب نظام أدنى في المخدم من أجل تقويض قوة الهجمات.

ج) تطبيق نظام لاختبار ونشر التحديثات الأمنية، وضمان إنشاء أنظمة لتشغيل مخدم الويب والتعجيل بتحديث التطبيقات عندما تتوفر تحديثات أمنية جديدة.

د) مراقبة جودة الأداء الأمني لمخدم الويب من خلال الانتظام في استعراض قنوات التدقيق.

هـ) تشغيل برمجيات مكافحة الفيروسات وبرمجيات مكافحة برامج التجسس على حد سواء على المخدم.

و) إجراء مسح دقيق بانتظام لجميع المحتويات المُستضافة والمُحملة باستعمال تعاريف حديثة. والتسليم بأن أي ملف قد يكون أيضاً من ملفات برمجيات التجسس أو البرمجيات المؤذية، حتى إن لم تكشف عنه هذه التعاريف بسبب القيود المتعلقة بالمعلومات المنقوصة.

ز) إجراء اختبار منتظم لاختراق الحاجز الأمني لمواقع الويب لضمان صيانة أمنها كما ينبغي والتأكد من عدم تعرضها لمرتكبي هذه الانتهاكات.

وللسماح بإنفاذ هذه التدابير الأمنية، وخصوصاً المتعلقة منها بأمن موقع الويب، ينبغي أن ينظر مورد خدمات الاتصالات في إدراج هذه الأحكام في شروط اتفاق الخدمات.

3.11 إرشادات بشأن سلامة المستعملين النهائيين وأمنهم

1.3.11 إرشاد المستعمل وتثقيفه

يتعين تقديم إرشادات إلى المستعمل بشأن كيفية بقائه آمناً على الخط. وبإمكان مورد خدمات الاتصالات أن يضع الإرشادات مباشرة، أو يحيل المستعملين إلى المواقع الإرشادية المتاحة التي يمكن أن تزودهم بمحتوياتها. ومن الضروري تثقيف المستعملين النهائيين بالسبل الكفيلة بإسهامهم في تصفح الإنترنت بطريقة آمنة. ويمكن أن تشمل حملات وضع الإرشادات أو الأنشطة المتعلقة بوضعها ما يلي:

أ) إصدار رسائل إخبارية أمنية بشكل دوري (شهرياً مثلاً) لإسداء المشورة بشأن تقنيات أمنية محددة (عن كيفية انتقاء كلمة سر صالحة على سبيل المثال)؛ وتقديم تحديثات عن الاتجاهات الأمنية؛ وإصدار إخطارات بشأن النشرات الإخبارية الأمنية، وغيرها من إصدارات الفيديو المقدمة عند الطلب، والنشرات الإذاعية الإخبارية، والمعلومات الأمنية التي يُحصل عليها من بوابة ويب مورد خدمات الاتصالات أو من موردين آخرين للمحتوى الأمني؛

ب) إصدار نشرات إذاعية مباشرة عن إصدارات الفيديو المقدمة عند الطلب بشأن التثقيف بالجوانب الأمنية و/أو النشرات الإخبارية التي تشمل طائفة من المواضيع الأمنية الرامية إلى تحسين الممارسات الأمنية التي يتبعها المستعملون النهائيون ورفع مستوى وعيهم؛

ج) إدراج عمود معني بالجوانب الأمنية في النسخة المطبوعة من رسالة مورد خدمات الاتصالات الإخبارية التي تُرسل إلى مكان إقامة المستعمل النهائي أو إلى عنوان عمله لإبراز الأحداث أو المحتويات الأمنية الرئيسية؛

د) تنظيم حلقات دراسية أو عروض في الشارع على أساس سنوي أو على أساس دوري آخر، ويمكن تنظيمها بالاشتراك مع سائر الأطراف الصناعية الفاعلة، والبائعين، والحكومات.

2.3.11 التدابير الأمنية التقنية الخاصة بالمستعمل النهائي

ينبغي أن يقوم مورد خدمات الاتصالات، كجزء من تثقيف وإرشاد المستعمل النهائي أمنياً لحمايته من البرمجيات المضللة وبرمجيات التجسس، بإسداء المشورة إلى المستعمل بشأن اللجوء إلى ما هو مناسب من التدابير الأمنية التقنية الرامية إلى حماية نظامه من حالات الاستغلال والهجمات المعروفة. وينبغي أن تشمل تدابير الحماية الدنيا ما يلي:

أ) استعمال أحدث أنظمة التشغيل التي تُركب فيها أحدث تصحيحات البرامج الأمنية؛

ب) استعمال أدوات مكافحة الفيروسات وبرمجيات التجسس. وينبغي، إن أمكن، أن يشارك مورد خدمات الاتصالات مع بائعي الأدوات الأمنية الموثوقة[4] لعرض منتجاتهم كجزء من مجموعة الاشتراك في خدمة المورد ليتسنى إتاحة التدابير الأمنية عند توقيع عقد الاشتراك أو تجديده؛

ج) تخويل مصد النوافذ الفجائية. وهذه الإمكانية مدمجة الآن في أشرطة الأدوات الشائعة لمتصفح الويب والمتصفحات، وهي تمنع مواقع الويب الضارة من عرض النوافذ الحاوية على برمجيات تجسس أو برمجيات مضللة يمكن أن تستغل مواطن ضعف النظام أو المتصفح أو تلجأ إلى الهندسة الاجتماعية لخداع المستعمل بتنزيل هذه البرمجيات وتركيبها على نظامه. وينبغي تجميع قائمة بالأدوات المقترحة لمصدات النوافذ الفجائية، والتوصية باتباعها، ولا بد من تشجيع

[4] يمكن أن تكون الجهات البائعة الأمنية الموثوقة شريكة لمورد خدمات الاتصالات في أعماله، و/أو جهات توفر منتجات وتقدم خدمات تُقيم على أساس استيفاء سياسات مورد خدمات الاتصالات ومتطلباته الأمنية.

استعمالها مع تقديم إرشادات عن تخويلها وعن كيفية السماح للنوافذ الفجائية الوافدة من مواقع الويب التي يسمح لها المستعمل بالظهور؛

د) تخويل جدار الحماية الشخصي. هذا الجدار أداة مهمة أخرى للتحكم في خدمات الشبكة التي تنفذ إلى أنظمة المستعملين، والعكس بالعكس. وتدرج جدران الحماية في عدد من أنظمة التشغيل الحديثة. وإن كانت جدران الحماية مخولة بالتغيب، فقد يعطلها المستعملون أو أي تطبيقات أخرى، مما يؤدي إلى تعرض أمن الشبكة لحالات غير مطلوبة. وينبغي أن يشجع موردو خدمات الاتصالات المستعمل على استعمال وظائف جدار الحماية، و/أو يقترحوا منتجات أخرى تقدمها أطراف ثالثة لتوفير جدار حماية شخصي يقيّمه الموردون على أنه موثوق، وأن يعلم الموردون المستعمل ويساعدوه في تخويل أمن الشبكة الأساسي على مستوى نظام المستعمل النهائي؛

هـ) تخويل التحديثات الأوتوماتية. وإن كانت التدابير الأمنية التقنية المذكورة أعلاه قادرة على التعامل مع معظم البرمجيات الضارة على مستوى التشغيل، فإنها ليست فعالة للغاية ضد استغلال مواطن الضعف الموجودة في أنظمة التشغيل ومنتجات التطبيقات. ومنعاً لهذا الاستغلال، ينبغي تخويل وظائف التحديث المتاحة في نظام التشغيل، والمتاحة أيضاً في التطبيقات الموثوقة للمستعمل (كالمنتجات التي تقيّمها أطراف ثالثة على أنها موثوقة لمكافحة برمجيات التجسس ومكافحة الفيروسات) تخويلاً يستند إلى إجراء تحديثات أوتوماتية. ومن شأن ذلك أن يكفل عندئذ تحديث النظام بآخر ما استجد من تصحيحات البرامج الأمنية، كلما توفرت، لتسد بذلك الفجوة الزمنية للاستغلال المقرر وقوعه.

ويرد في التذييل I قائمة بمراجع وموارد متاحة على الخط يمكن استعمالها لدعم تنفيذ التوصيات المبينة أعلاه.

التذييـــل I

موارد إضافية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I المراجع المباشرة على الإنترنت المتعلقة بالأمن ومكافحة برمجيات التجسس

يوجد عدد من مواقع الويب التي يمكن الرجوع إليها والاستعانة بها في الحصول على المزيد من المعلومات عن السلامة والأمن على الإنترنت، وتشمل ما يلي:

- **تحالف مكافحة برمجيات التجسس (ASC)** وعنوانه (http://www.antispywarecoalition.org/) – مجموعة مكرسة للتوصل إلى توافق في الآراء بشأن التعاريف وأفضل الممارسات المتبعة في المناقشات الدائرة حول تكنولوجيات برمجيات التجسس وغيرها من التكنولوجيات التي يمكن أن تكون غير مطلوبة. ويسعى هذا التحالف (ASC) المكون من شركات لإنتاج برمجيات مكافحة تكنولوجيات التجسس، وأوساط أكاديمية، ومجموعات المستهلكين، إلى جمع طائفة متنوعة من التصورات عن مشكلة التحكم في تكنولوجيات برمجيات التجسس وغيرها من التكنولوجيات التي يمكن أن تكون غير مطلوبة.
- **برنامج احذر شبكة الويب (Be Web Aware)** وعنوانه (http://www.bewebaware.ca) – برنامج وطني بلغتين لتعليم الجمهور بشأن السلامة على الإنترنت، الغرض منه ضمان استفادة الشباب الكنديين من الإنترنت، والعمل في الوقت نفسه على تأمين سلامتهم وتحميلهم مسؤولية أنشطتهم على الإنترنت.
- **مركز استعمال الإنترنت بأمان ومسؤولية** وعنوانه (http://csriu.org) – منظمة تقدم خدمات توعية تعالج المسائل المتعلقة باستعمال الإنترنت بأمان ومسؤولية.
- **شبكة الطفل الدولية (Childnet International)** وعنوانها (http://www.childnet-int.org) – هي منظمة غير هادفة للربح تعمل بالشراكة مع جهات أخرى حول العالم من أجل المساعدة على جعل الإنترنت مكاناً رائعاً وآمناً للأطفال.
- **شبكة ECPAT** وعنوانها (http://www.ecpat.net) – شبكة من المنظمات والأفراد العاملين معاً من أجل القضاء عل الاستغلال الجنسي للأطفال لأغراض تجارية.
- **خدمة GetNetWise** وعنوانها (http://www.getnetwise.org) – خدمة عامة يقدمها تحالف يُعنى بشركات صناعة الإنترنت والمنظمات المعنية بالمصلحة العامة، تريد أن يكون المستعمل على بعد "نقرة واحدة" فقط من الموارد التي يحتاجها لاتخاذ قرارات مستنيرة بشأن استعماله للإنترنت واستعمال أسرته لها.
- **التحالف الأساسي العالمي لسلامة الإنترنت (GIAIS)** وعنوانه (http://www.microsoft.com/security/msra/default.mspx) – تحالف مكون من موردي الخدمات، نُظّم تعزيزاً للأمن والسلامة على شبكة الويب، ويقوم بانتظام بإدارة التهديدات على نطاق واسع، وتحديد أوجه التعرض للخطر القائمة وتخفيفها.
- **رابطة INHOPE** وعنوانها (http://www.inhope.org) – رابطة دولية تدعم الخطوط المباشرة للإنترنت الرامية إلى الاستجابة للتقارير المقدمة عن المحتويات غير القانونية على الإنترنت سعياً إلى تحقيق قدر أكبر من الأمان على الإنترنت.
- **مجموعة السلامة على الإنترنت (ISG)** وعنوانها (www.netsafe.org.nz) – موقع على شبكة الويب يمثل المقر المباشر لمجموعة السلامة على الإنترنت في نيوزيلندا (ISG) ولمجموعة هيكتور الحامي (Hector the Protector).
- **المركز الدولي المعني بالأطفال المفقودين والمستغلين** وعنوانه (http://www.icmec.org) – وكالة عالمية تروج لتحقيق سلامة الأطفال ورفاههم من خلال النشاط في هذا المجال ووضع السياسات والتنسيق المتعدد الجنسيات.

- **المنظمة الدولية للشرطة (الإنتربول)** وعنوانها (http://www.interpol.int) – تسهل المنظمة الدولية للشرطة تعاون رجال الشرطة عبر الحدود، وتدعم وتساعد جميع المنظمات، والسلطات، والدوائر التي تضطلع بمهمة منع الجريمة الدولية ومكافحتها.
- **موقع iSafe** وعنوانه (http://www.isafe.org) – موقع عالمي رائد في مجال التثقيف بجوانب السلامة على الإنترنت؛ ويضم مناهج دراسية تقترن بتوعية المجتمع ديناميا لتمكين الطلبة، والمدرسين، والوالدين، والمكلفين بإنفاذ القانون، والمعنيين من البالغين، من جعل الإنترنت مكاناً أكثر أماناً.
- **موقع أمن مايكروسوفت في المنـــزل (Microsoft Security At Home)** وعنوانه (http://www.microsoft.com/protect) – موقع للمعلومات والموارد اللازمة لمساعدة الجمهور على حماية حواسيبه، ونفسه وأسرته.
- **المجلس القومي للأمومة والطفولة (NCCM)** وعنوانه (http://www.nccm.org.eg) – منظمة مصرية مكرسة لدعم الطفولة والأمومة باتباع نهج قائم على إعمال الحقوق.
- **خدمة Net Family News** وعنوانها (http://netfamilynews.org) – خدمة عامة غير هادفة للربح تمثل محفلاً وموقعاً "لأخبار التكنولوجيا الخاصة بالأطفال" للوالدين والمربين في أكثر من 50 بلداً.
- **منظمة NetAlert Limited** وعنوانها (http://www.netalert.gov.au) – منظمة مجتمعية غير هادفة للربح أنشأتها الحكومة الأسترالية لإسداء المشورة المستقلة إلى المجتمع وتثقيفه بشأن إدارة سبل النفاذ إلى محتويات الإنترنت.
- **موقع NetSmartzKids** وعنوانه (http://www.netsmartzkids.org) – NetSmartz عبارة عن مورد تفاعلي وتثقيفي معني بالسلامة على الإنترنت تابع للمركز الوطني المعني بالأطفال المفقودين والمستغلين (NCMEC) وأندية الفتيان والفتيات في أمريكا (BGCA) للأطفال الذين تتراوح أعمارهم بين 5 إلى 17 سنة، والوالدين، والأوصياء، والمربين، والمكلفين بإنفاذ القانون، يستعمل أنشطة ثلاثية الأبعاد ومناسبة للأطفال لتعليمهم كيفية البقاء آمنين على الإنترنت.
- **شبكة Safe Kids Worldwide** وعنوانها (http://www.safekids.org) – شبكة عالمية من المنظمات تضطلع بمهمة منع تعرض الأطفال للإصابات، وهي شبكة رائدة لمنع حوادث وفاة الأطفال الذين تتراوح أعمارهم بين 14 عاماً وما دون ذلك.
- **موقع SafeKids.com** وعنوانه (http://www.safekids.com) – موقع للموارد اللازمة لمساعدة الأسر على جعل الإنترنت والتكنولوجيا مجالين ممتعين، وآمنين، ومثمرين.
- **موقع StaySafe.org** وعنوانه (http://www.staysafe.org) – موقع تعليمي الغرض منه مساعدة المستهلكين على فهم كل من الجوانب الإيجابية للإنترنت، فضلاً عن السبل الكفيلة بإدارة طائفة من المسائل المطروحة على الإنترنت والمتعلقة بالسلامة والأمن.
- **منظمة الأمم المتحدة للطفولة (اليونيسيف)** وعنوانها (http://www.unicef.org) – منظمة عالمية تناصر حماية حقوق الأطفال، وتكرس نفسها لتقديم المساعدة الإنسانية والإنمائية الطويلة الأجل للأطفال والوالدين في البلدان النامية.
- **موقع WebSafe Crackerz** وعنوانه (http://www.websafecrackerz.com) – موقع للألعاب والألغاز التفاعلية مصمم لمساعدة المراهقين وتزويدهم باستراتيجيات التعامل مع مختلف الحالات على الإنترنت، بما في ذلك الوقاية من الرسائل الاقتحامية، والتدليس وعمليات الاحتيال.

2.I قائمة نموذجية بجهات الاتصال المعنية بتصاعد الأحداث الأمنية

يرد في الجدول 1.I أدناه قائمة لعينات بجهات الاتصال المعنية بتصعيد الأحداث المتعلقة بالسلامة والأمن على الإنترنت:

الجدول 1.I: قائمة نموذجية بالمعلومات المتعلقة بجهات الاتصال المعنية بتصعيد الأحداث الأمنية

المنظمات	جهة الاتصال
شركة Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
محفل أفرقة الاستجابة للأحداث المتعلقة بالحاسوب والأفرقة الأمنية (FIRST)	http://www.first.org/about/organization/teams/
شركة مايكروسوفت	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
شركة Telecom-ISAC Japan	https://www.telecom-isac.jp/contact/index.html

ثبت المراجع

[b-ITU-T X.1051] التوصية ITU-T X.1051، (2004) *نظام إدارة أمن المعلومات – متطلبات الاتصالات (ISMS-T)*.

[b-ISO/IEC 27001] المعيار ISO/IEC 27001:2005، تكنولوجيا المعلومات – *تقنيات الأمن – أنظمة إدارة أمن المعلومات – المتطلبات*. http://www.iso.org/iso/catalogue-detail?csnumber=42103

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، 2008