الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1233

(2021/09)

السلسلة X: شبكات البيانات والاتصالات،
بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – مكافحة الرسائل الاقتحامية

مبادئ توجيهية بشأن مكافحة الرسائل الاقتحامية عبر المراسلة الفورية

التوصية ITU-T X.1233

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
الخصائص البيومترية	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 الويب	X.1140–X.1149
أمن البروتوكولات (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.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1399
أمن سجل الحسابات الموزع (DLT)	X.1400–X.1429
أمن سجل الحسابات الموزع (DLT)	X.1430–X.1449
أمن البروتوكولات (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل 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
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
المولد الكمومي للأعداد العشوائية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية (QKDN)	X.1710–X.1711
التصميم الأمني للشبكات QKDN	X.1712–X.1719
التقنيات الأمنية للشبكات QKDN	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن 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.1233

مبادئ توجيهية بشأن مكافحة الرسائل الاقتحامية عبر المراسلة الفورية

ملخص

تحدد التوصية ITU-T X.1233 مبادئ توجيهية لمقدمي ومستعملي خدمة المراسلة الفورية (IM) لمكافحة الرسائل الاقتحامية عبر المراسلة الفورية (SPIM) والحد من انتشار الرسائل الاقتحامية عبر المراسلة الفورية في الفضاء السيبراني وتحسين تجربة مستعملي الرسائل الفورية.

وتتضمن هذه التوصية تحليل سيناريوهات استحداث الرسائل الاقتحامية في المراسلات الفورية، وتحدد تدابير وآليات تقنية لمكافحة هذه الرسائل موجهة لمقدمي خدمة المراسلة الفورية كما تقدم توصيات لمستعملي المراسلة الفورية من أجل مكافحة هذه الرسائل.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1233	2021-09-03	17	11.1002/1000/14773

مصطلحات أساسية

مكافحة الرسائل الاقتحامية عبر المراسلة الفورية، مبادئ توجيهية، مقدم خدمة المراسلة الفورية، مستعمل المراسلة الفورية.

* 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 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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

أدت شعبية تطبيقات المراسلة الفورية (IM) إلى أن تصبح هذه التطبيقات وسيلة مهمة لنشر الرسائل الاقتحامية، إلى جانب الصوت وخدمة الرسائل القصيرة (SMS) والبريد الإلكتروني. ومن خلال إرسال الرسائل في الوقت الفعلي بكفاءة، تتيح المراسلة الفورية راحة كبيرة في الاتصالات الاجتماعية. ومع ذلك، فإنها تفتح الباب أيضاً للمقتحمين لإرسال رسائل اقتحامية عبر المراسلة الفورية (SPIM). ويتزايد حجم الإعلانات الاقتحامية والمواد الإباحية وغيرها من المعلومات غير القانونية مثل معلومات التصيد الاحتيالي والفيروسات وديدان طروادة وبرامج التجسس التي يتم إرسالها عن عبر المراسلة الفورية بشكلٍ كبير. ولا يتسبب ذلك في المضايقات أو حتى الخسائر الاقتصادية للاستعمالات فحسب، ولكنه يؤثر أيضاً بشكل خطير علىً أمن الفضاء السيبراني. وقد أصبحت مكافحة هذه الرسائل عنصراً مهماً في مكافحة الرسائل الاقتحامية.

بيد أنه لا يزال هناك نقص في التوجيهات المتاحة لمقدمي الخدمات (SP) والمستعملين الذين يرغبون في مواجهة الرسائل SPIM أثناء تشغيل أو استخدام المراسلة الفورية. وهذا يعني أن الجهود المبذولة لمكافحة هذه الرسائل لا تتم إدارتها بشكل فعال. لذلك من الضروري وضع معايير مناسبة لتوجيه مشغلي ومستعملي المراسلة الفورية من خلال تقنيات وتدابير إدارية من شأنها أن تمنع هذه الرسائل.

التوصية ITU-T X.1233

مبادئ توجيهية بشأن مكافحة الرسائل الاقتحامية عبر المراسلة الفورية

1 مجال التطبيق

تحدد هذه التوصية مبادئ توجيهية لمقدمي ومستعملي خدمة المراسلة الفورية (IM) لمكافحة الرسائل الاقتحامية عبر المراسلة الفورية (SPIM). وتتناول هذه التوصية سيناريوهات الرسائل الاقتحامية الفورية، وتدابير وآليات تقنية لمكافحة هذه الرسائل موجهة لمقدمي خدمة المراسلة الفورية كما تقدم لمستعملي المراسلة الفورية تدابير استجابة عاجلة من أجل مكافحة الرسائل الاقتحامية عبر المراسلة الفورية.

2 المراجع

لا يوجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مواضع أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مواضع أخرى:

1.1.3 رسائل اقتحامية عبر المراسلة الفورية (SPIM) [b-ITU-T X.1244]: رسالة اقتحامية تستهدف مستعملي خدمة المراسلة الفورية.

ملاحظة – لأغراض هذه التوصية، لا يعرف مصطلح "الرسائل الاقتحامية".

2.1.3 المقتحِم [b-ITU-T X.1244]: مُرسِل الرسائل الاقتحامية عبر المراسلة الفورية (SPIM).

2.3 مصطلحات معرفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 المراسلة الفورية (IM): تبادل محتوى بين مجموعة من المشاركين في وقت قريب من الوقت الفعلي. وعادةً يكون المحتوى رسائل نصية قصيرة، وإن لم تكن مقصورة على هذا الشكل.

ملاحظة – استناداً إلى المعيار [b-IETF RFC 3428].

4 المختصرات والأسماء المختصرة

IM المراسلة الفورية *(Instant Messaging)*

IP بروتوكول الإنترنت *(Internet Protocol)*

NE مشغل شبكة *(Network operator)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SPIM رسائل اقتحامية عبر المراسلة الفورية *(Spam over Instant Messaging)*

SP مقدم خدمة *(Service Provider)*

5 اصطلاحات

تدل الصيغة "يجب" على متطلَّب يجب التقيّد به من أجل الامتثال لهذه التوصية

وتدل الصيغتان "ينبغي" و"ينبغي ألا" على أنه، من بين عدة احتمالات، يوصى باستخدام واحد منها على أنه مناسب بشكل خاص، دون ذكر أو استبعاد الاحتمالات الأخرى؛ أو أن هناك مسار عمل معين مفضل ولكنه ليس مطلوباً بالضرورة؛ أو أنه (في الجانب السلبي) تم إغفال احتمال معين أو مسار عمل معين دون حظرهما.

وتدل صيغة الفعل "يمكن" على مطلب اختياري مسموح به. ولا ينطوي هذا المصطلح على ضرورة أن تتضمن عملية التنفيذ هذا الخيار.

6 سيناريوهات الرسائل الاقتحامية عبر المراسلة الفورية

أصبحت الرسائل الاقتحامية عبر المراسلة الفورية (SPIM) تحدياً رئيسياً لخدمات المراسلة الفورية (IM). وتؤثر الرسائل SPIM على أداء أنظمة المراسلة الفورية بطرق مختلفة، مثل إهدار الموارد بما في ذلك الذاكرة ووحدة المعالجة المركزية ومساحة التخزين وموارد عرض النطاق وما إلى ذلك، وقد تتسبب في مشاكل كبيرة مثل انتشار الديدان وهجمات رفض الخدمة، وغيرها. وتتضمن سيناريوهات الرسائل SPIM على سبيل المثال لا الحصر ما يلي:

- استخدام الوسائل الأوتوماتية لتسجيل عدد كبير من الحسابات لأغراض خبيثة، مثل نشر الرسائل SPIM.
- استخدام الحساب بدون تصريح من مالك الحساب لإنشاء توصيلة دورة مع المستعمل المستهدف لنشر الرسائل SPIM.
- يؤدي الافتقار إلى آليات الأمن المدمجة، مثل عدم وجود آلية تحقق عند إضافة الأصدقاء، إلى توفير بيئة يمكن أن تنتشر فيها الرسائل SPIM بسرعة.
- الكشف عن الرسائل عبر قناة تسليم غير مأمونة. ويمكن للقراصنة التلاعب في الرسائل الفورية أثناء إرسالها. ويمكن دمج الإعلانات أو الشفرات الضارة ضمن أي رسالة وتحويلها إلى رسالة SPIM.
- تدفع شركات التصنيع التي تتصرف بشكل غير قانوني باشتراكات الرسائل SPIM للمستعملين من أجل منافع تجارية.

7 مبادئ توجيهية لمقدمي خدمة المراسلة الفورية لمكافحة الرسائل الاقتحامية عبر المراسلة الفورية

1.7 تشكيلة وظائف مكافحة الرسائل الاقتحامية عبر المراسلة الفورية

يجب أن يوفر مقدم خدمة المراسلة الفورية وظائف مكافحة الرسائل SPIM أثناء تقديم خدمة المراسلة الفورية. وينبغي أن تتضمن وظائف مكافحة الرسائل SPIM على سبيل المثال لا الحصر ما يلي:

- الكشف عن تسجيل المستعمل والتحكم فيه أوتوماتياً؛
- التحكم في التخويل عند إضافة الأصدقاء؛
- كشف معدل إرسال الرسائل وتقييده؛
- ترشيح الرسائل على أساس القوائم السوداء؛
- منصة شكاوى للمستعملين تضم، من بين وظائف أخرى، آلية ردود فعل بسيطة لتنبيه مقدم خدمة المراسلة الفورية بالرسائل SPIM المستلمة.

وفي الوقت نفسه، يجب أن يرعى مقدم خدمة المراسلة الفورية وظائف مكافحة الرسائل SPIM أثناء التشغيل. وينبغي أن تشمل السيناريوهات على سبيل المثال لا الحصر ما يلي:

- رعاية قواعد بيانات مكافحة الرسائل SPIM، مثل قوائم الأصدقاء والقوائم السوداء وما إلى ذلك، بحيث تكون متاحة ومستقرة؛
- رعاية معلومات شكاوى المستعملين لتحسين دقة هذه المعلومات؛

- ضبط العتبات المستخدمة في وظائف مكافحة الرسائل SPIM، مثل عتبات تقييد معدل إرسال الرسائل، وعدد الشكاوى التي يمكن أن يتلقاها الحساب قبل إضافته إلى القائمة السوداء.

2.7 مراقبة السلوك والتحكم فيه

يجب أن يتخذ مقدم خدمة المراسلة الفورية تدابير لمراقبة السلوكيات التالية، وأن يولد تنبيهات عند اكتشاف انحرافات. وتشمل السلوكيات التي ينبغي مراقبتها على السبيل الذكر وليس الحصر:

- سلوك فشل الاستيقان: فعلى سبيل المثال، يُرسل عدد من طلبات الاستيقان من عنوان بروتوكول الإنترنت نفسه. فإذا كان هناك الكثير من مثل هذه السلوكيات، فقد يكون هناك قرصان يقوم بسرقة الحسابات لإرسال الرسائل SPIM. وينبغي أن يطلق هذا الأمر إنذاراً وينبغي إسقاط طلبات الاستيقان اللاحقة الصادرة من العنوان IP هذا.
- سلوك الشكاوى الكيدية: فعلى سبيل المثال، يقدم حساب ما عدداً كبيراً من الشكاوى في فترة زمنية معينة، سواء كانت الشكاوى تتعلق بحسابات مختلفة أو نفس الحساب، فإذا تجاوز عدد الشكاوى حداً معيناً، فينبغي أن يُطلق إنذار وينبغي إغفال الشكاوى الواردة من هذا الحساب، وبالتالي تحسين دقة الشكاوى.
- السلوك الكيدي المتمثل في إضافة حسابات إلى القوائم السوداء: فعلى سبيل المثال، إذا أضافت بعض الحسابات حساباً معيناً إلى قائمة سوداء، فينبغي اكتشاف ما إذا كانت هذه الحسابات في قائمة حسابات مشبوهة أم لا. وإذا كان معظمها في قائمة حسابات مشبوهة، فينبغي إطلاق إنذار. وينبغي ألا تُؤخذ بعين الاعتبار هذه المحاولات لإدراج الحساب المحدد في القائمة السوداء عند حساب عدد المرات التي تمت فيها إضافة الحساب المحدد إلى القائمة السوداء، وبالتالي تحسين دقة القائمة السوداء.

3.7 التدقيق والتسجيل

يجب أن يتبنى مقدمو خدمات IM تدابير تقنية لتدقيق وتسجيل سلوكيات المستعملين وحوادث الأمن السيبراني لمكافحة الرسائل SPIM. وتشمل السجلات التي ينبغي أن تقوم خدمة المراسلة الفورية بتدقيقها على سبيل المثال لا الحصر ما يلي:

- سجلات سلوك المستعملين، وتتضمن معلومات سلوك التسجيل، ومعلومات استيقان المستعمل، وما إلى ذلك. فعلى سبيل المثال، ينبغي لمقدم خدمة المراسلة الفورية تسجيل التصرفات التاريخية للمستعمل (على سبيل المثال، تجاوز سلوكيات إرسال الرسائل عتبة حدود معدل إرسال الرسائل، وسلوكيات الشكاوى الكيدية). وينبغي أن تتضمن سجلات سلوك إرسال الرسائل، على سبيل المثال لا الحصر، المعلومات التالية: معلومات حساب المرسل (على سبيل المثال، العنوان IP، واسم المستعمل، وما إذا كان المرسل مدرجاً في قائمة مشبوهة/قائمة سوداء أم لا)، ومعلومات حساب المستلم، ونوع العلاقة بين المرسل والمستلم (على سبيل المثال، أصدقاء، غير أصدقاء، أصدقاء أعضاء في مجموعة، أصدقاء غير أعضاء في مجموعة، أصدقاء أنظمة مراسلة فورية أخرى، جهات اتصال هاتفية). وينبغي لمقدم خدمة المراسلة الفورية دمج تحليل هذه المعلومات لتحديد الأنشطة المشبوهة أو الخبيثة. وينبغي أن تتضمن سجلات سلوك الشكاوى الكيدية المعلومات التالية على سبيل المثال لا الحصر: معلومات حساب مقدم الشكوى (على سبيل المثال، العنوان IP واسم المستعمل، وما إذا كان المرسل مدرجاً في قائمة مشبوهة/قائمة سوداء أم لا)، ومعلومات الحساب الذي يتم تقديم شكوى بشأنه، وعدد الشكاوى في فترة زمنية معينة. فإذا تجاوز عدد الشكاوى عتبة ما، يتم تجاهل الشكاوى الواردة من حساب مقدم الشكوى، وبالتالي تحسين دقة منصة الشكاوى.
- سجل تصفية الرسائل SPIM، والذي يتضمن سلوكيات تصفية الرسائل SPIM والرسائل التي تمت تصفيتها. وينبغي أن يشتمل سجل سلوك تصفية الرسائل SPIM على المعلومات التالية على سبيل المثال لا الحصر: الحساب مرسل الرسائل التي تمت تصفيتها (على سبيل المثال، العنوان IP واسم المستعمل، وما إذا كان المرسل مدرجاً في قائمة مشبوهة/قائمة سوداء أم لا)، وما هي تدابير التصفية المستخدمة (على سبيل المثال، هل تمت التصفية بناءً على القوائم السوداء أو التحكم في معدل الإرسال أو التحكم في التخويل). وينبغي تسجيل الرسائل التي تمت تصفيتها بحيث يمكن إعادة إرسالها في حالة تصفيتها عن طريق الخطأ.

4.7 الاستجابة للطوارئ

ينبغي لمقدم خدمة المراسلة الفورية صياغة خطة استجابة للطوارئ لأحداث الرسائل SPIM الرئيسية.

وينبغي تغطية أحداث الرسائل SPIM الرئيسية من خلال خطة الاستجابة للطوارئ، التي ينبغي أن تشمل هذه الأحداث على سبيل المثال لا الحصر ما يلي:

- تعديل قاعدة بيانات مكافحة الرسائل SPIM لمخدم الرسائل الفورية أو اقتحامها أو التحكم فيها؛
- تعديل منصة الشكاوى ضد الرسائل SPIM أو اقتحامها أو التحكم فيها؛
- تعديل عتبة وظيفة التسجيل الأوتوماتي بشكل غير قانوني؛
- وجود شكاوى واسعة النطاق ضد الرسائل SPIM في فترة زمنية معينة.

وينبغي لمقدم خدمة IM تحديد نوع ومستوى كل حدث من أحداث الرسائل SPIM هذه وفقاً للوضع الفعلي، وصياغة عملية الاستجابة للطوارئ والمبادئ التوجيهية لعمليات الطوارئ لكل نوع وكل مستوى من أحداث الرسائل SPIM.

وينبغي لمقدم خدمة IM إنشاء آلية مراقبة وتحذير بشأن أحداث الرسائل SPIM الرئيسية، واكتشاف هذه الأحداث وإخطار الموظفين المعنيين في الوقت المناسب.

وينبغي لمقدم خدمة IM أيضاً تلخيص أسباب أحداث الرسائل SPIM الرئيسية بعد الاستجابة للطوارئ، وتقييم فعالية تدابير الاستجابة للطوارئ، وحل المشكلة في الوقت المناسب.

5.7 إدارة تقييم المخاطر

ينبغي لمقدمي خدمة المراسلة الفورية تقييم المخاطر المتعلقة باحتمالية وخطورة أحداث الرسائل SPIM. وينبغي دمج إدارة المخاطر في أنشطة التشغيل الأساسية، بدءاً من التقييم الإداري، وصولاً إلى التقييم الأمني والتقييم الوظيفي. يجب أن تشمل إدارة تقييم المخاطر على سبيل المثال لا الحصر ما يلي:

- ينبغي لمقدم خدمة IM إجراء تقييم إداري والذي ينبغي أن يشمل، على سبيل المثال، وضع سياسة لمكافحة الرسائل SPIM ومراقبة ما إذا كانت عمليات واستراتيجيات الامتثال الأمني مطبقة للتخفيف من مخاطر الرسائل SPIM، وبالإضافة إلى ذلك، ينبغي أن تسهل تنفيذ السياسة. وينبغي لمورد خدمة IM أيضاً مراجعة وتحديث سياسة وإجراءات تقييم المخاطر الحالية وفقاً للوتيرة المحددة من قبل المنظمة أو كلما كانت هناك تغييرات كبيرة في نظام IM أو بيئة التشغيل.
- ينبغي لمقدم خدمة IM إجراء تقييم أمني، والذي ينبغي أن يتضمن، على سبيل المثال، أتمتة عملية إدارة مواطن الضعف باستخدام المعايير (على سبيل المثال، تعديد عيوب التطبيق والتشكيلات غير السليمة؛ تنسيق القوائم المرجعية وإجراءات الاختبار) لتحديد السبب الأكثر احتمالية للرسائل SPIM (على سبيل المثال، نقاط ضعف في كلمات المرور، وإعدادات جدر الحماية غير الآمنة، وديدان طروادة)، وقياس الظروف المهيئة لأحداث الرسائل SPIM الرئيسية.
- ينبغي لمقدم خدمة IM إجراء تقييم وظيفي، والذي ينبغي أن يشمل، على سبيل المثال، اكتشاف المعالجة غير المنطقية والأخطاء المتتالية التي يمكن أن تقع ضمن شفرة نظام IM (على سبيل المثال، التسجيل الأوتوماتي للمستعمل، معدل إرسال غير محدود لمستعمل ما خلال فترة زمنية معينة، نقص آليات الأمن المدمجة، والكشف عن الرسائل عبر قناة تسليم غير مأمونة) عند عمليات تحديث النظام IM.
- ينبغي لمقدم خدمة IM إجراء تقييم للمخاطر بانتظام أو مراجعة وتحديث سياسة تقييم المخاطر الخاصة به عند الضرورة. وينبغي أن يشتمل تقييم المخاطر على ثلاثة مكونات مترابطة: التقييم الإداري والتقييم الأمني والتقييم الوظيفي. فعلى سبيل المثال، ينبغي إجراء التقييم الإداري والتقييم الأمني جنباً إلى جنب مع التقييم العام للمخاطر، وينبغي إجراء التقييم الوظيفي قبل ترقية نظام IM، أو أثناء ترقيته، أو كليهما. وفي الوقت نفسه، ينبغي لمقدم خدمة IM إما معالجة العيوب المشروعة في أوقات الاستجابة المحددة من قبل المنظمة أو تنفيذ الضوابط اللازمة لمنع القرصان من استغلال موطن الضعف.

6.7 تدابير الحماية الأمنية

ينبغي لمورد خدمة IM اتخاذ إجراءات حماية أمنية لمكافحة الرسائل SPIM. وينبغي أن تشمل تدابير الحماية الأمنية على سبيل المثال لا الحصر ما يلي:

- ينبغي لمورد خدمة IM اتخاذ تدابير لمكافحة هجمات رفض الخدمة الموزع لحماية مكتبة القوائم السوداء ومنصة الشكاوى ومراقبة الأمن وطرق التدقيق، ولتحسين تيسر وظائف مكافحة الرسائل SPIM.
- ينبغي لمورد خدمة IM اتخاذ تدابير لمكافحة الفيروسات، ومكافحة أحصنة طروادة، ومكافحة الفيروسات لمنع إصابة المخدم والسيطرة عليه من قبل القراصنة الذين يقومون بتعديل تشكيلات مكافحة الرسائل SPIM أو تعطيل وظائف مكافحة الرسائل SPIM ثم إرسال الرسائل SPIM.
- ينبغي لمورد خدمة IM تنفيذ طرق للتحكم في النفاذ المتعدد داخل حدود الشبكة وأنظمة وتطبيقات نظام IM، لمنع النفاذ غير المصرح به من قبل القراصنة الذين يقومون بتعديل تشكيلات مكافحة الرسائل SPIM أو تعطيل وظائف مكافحة الرسائل SPIM ثم إرسال الرسائل SPIM.
- ينبغي لمورد خدمة IM نشر أساليب كشف الاقتحام والحماية منه لاكتشاف هجمات الشبكة ومنع اقتحام نظام IM من قبل القراصنة الذين يقومون بتعديل تشكيلات مكافحة الرسائل SPIM أو تعطيل وظائف مكافحة الرسائل SPIM ثم إرسال الرسائل SPIM.

8 وظائف مستعملي الخدمة IM لدعم مكافحة الرسائل SPIM

ينبغي أن يكون لدى مستعمل خدمة المراسلة الفورية إمكانية تشكيل عميل المراسلة الفورية للحماية من الرسائل SPIM عند استخدام نظام المراسلة الفورية. وينبغي أن تتضمن التشكيلة ما يلي على سبيل الذكر لا الحصر. وينبغي أن يكون لدى مستعمل خدمة المراسلة الفورية إمكانية القيام بما يلي:

- استخدام آلية تأكيد التحقق، بما في ذلك تأكيد طلب الاستيقان وتأكيد إضافات إلى المجموعة، لضمان موافقة المستعمل على جميع الإجراءات.
- تشكيل الإعدادات بحيث لا يسمح باستلام الرسائل أو الملفات من مستعملين غير مخولين.
- تشكيل القائمة السوداء في الوقت المناسب، وعدم السماح باستلام الرسائل أو الملفات من الحسابات المشبوهة.
- استخدام كلمة مرور قوية وتغييرها بانتظام لمنع سرقة حسابه واستخدامه لإرسال الرسائل SPIM.
- مراقبة تنفيذ الوظائف المميزة وتعطيل الإعدادات المنفذة وتغييرها لأنها قد تتسبب في رسائل SPIM (على سبيل المثال، قبول طلب استيقان شخص غريب).

9 مبادئ توجيهية لمقدمي الخدمات/مشغلي الشبكات لمكافحة الرسائل SPIM

يمكن لمقدمي الخدمات/مشغلي الشبكات (SP/NE) المساعدة في مكافحة الرسائل SPIM بوسائل مثل بناء منصة شكاوى موحدة ضد الرسائل SPIM، وإنشاء قاعدة بيانات موحدة للقوائم السوداء لمنع الرسائل SPIM، واختبار وظائف مكافحة الرسائل SPIM لنظام المراسلة الفورية والتحقق منها، وتوفير خدمات الكشف عن الرسائل SPIM لمقدمي خدمة المراسلة الفورية. ويشمل ذلك على سبيل الذكر لا الحصر ما يلي:

- ينبغي لمقدمي الخدمات/مشغلي الشبكات بناء منصة موحدة للشكاوى لخدمات المراسلة الفورية المتعددة. ويمكن لمنصة الشكاوى قبول الشكاوى من المستعملين بشأن أحد حسابات إرسال الرسائل SPIM، وتصنيف الشكاوى وفقاً لخدمات المراسلة الفورية المختلفة. وعندما يصل عدد المستعملين الشاكين ضد حساب IM ما إلى عدد معين من المرات، يتم إرسال تفاصيل الحساب IM هذا إلى قاعدة بيانات القوائم السوداء لخدمة المراسلة الفورية المقابلة.

- ينبغي لمقدمي الخدمات/مشغلي الشبكات إنشاء قاعدة بيانات موحدة للقوائم السوداء لخدمات المراسلة الفورية المتعددة. وتتم مزامنة قاعدة بيانات القوائم السوداء مع قاعدة بيانات القوائم السوداء لكل خدمة مراسلة فورية في الشبكة. وهناك نوعان من مصادر القوائم السوداء، والحسابان المدرجان في قاعدة البيانات هما:
  - موضوع الشكاوى من خلال منصة الشكاوى أعلاه؛
  - مرسل الرسائل SPIM الذي تم اكتشافه من خلال خدمة الكشف عن السائل SPIM.
- ينبغي لمقدمي الخدمات/مشغلي الشبكات توفير خدمة منتظمة للتحقق من اختبار المهاتفة لمقدمي خدمة المراسلة الفورية، والحيلولة دون إبطال وظائف مكافحة الرسائل SPIM في نظام المراسلة الفورية والذي قد ينتج عن هجمات للقراصنة. وإذا لم يتم تشغيل الوظيفة المقابلة بعد التحقق، يمكن لمقدمي الخدمات/مشغلي الشبكات إرسال إنذار إلى مقدم خدمة IM. وتتضمن وظائف التحقق من اختبار المهاتفة على سبيل الذكر لا الحصر محاكاة ما يلي:
  - سلوك التسجيل الأوتوماتي، والتحقق مما إذا كان نظام المراسلة الفورية يمكنه تحديد التسجيل الأوتوماتي ومنعه؛
  - حساب إرسال رسائل متعددة في وحدة زمنية (يتجاوز عدد الرسائل العتبة المحددة في نظام المراسلة الفورية)، والتحقق مما إذا كان بوسع نظام المراسلة الفورية اكتشاف الرسائل المرسلة من هذا الحساب وإغفالها لاحقاً؛
  - حساب مدرج في قائمة سوداء لإرسال رسالة والتحقق مما إذا كان بوسع نظام المراسلة الفورية إغفال الرسائل المرسلة بواسطة هذا الحساب؛
  - حاكاة الشكاوى الكيدية والتحقق مما إذا كان بوسع نظام المراسلة الفورية التعرف عليها وإغفالها.
- يمكن لمقدمي الخدمات/مشغلي الشبكات توفير خدمة لاكتشاف الرسائل SPIM لمقدم خدمة المراسلة الفورية. وينبغي أن يقوموا بالتوقيع على اتفاق مستوى الخدمة (SLA) مع كل مقدم خدمة IM، على أن يتضمن هذا الاتفاق شروط السرية، لحماية خصوصية المستعملين. تتمثل عملية الكشف عن الرسائل SPEM لدى مقدمي الخدمات/مشغلي الشبكات فيما يلي:
  - نشر أنظمة الكشف في العقد الرئيسية في الشبكة، واكتشاف رأسية رزم الرسائل IM بموجب ترخيص من مقدم خدمة IM؛
  - تحليل سلوك إرسال رسائل IM متعددة بواسطة حساب IM. فإذا تجاوز عدد الرسائل المرسلة بواسطة حساب IM خلال نطاق زمني معين عتبة معينة، هنا يجوز تحديد أن الحساب يرسل رسائل SPIM؛
  - إغفال الرسائل IM المرسلة من الحساب المذكور سابقاً مباشرة؛
  - إدراج الحساب المذكور سابقاً في قاعدة بيانات القوائم السوداء.

ويمكن، من خلال خدمة الكشف عن الرسائل SPIM المقدمة من مقدمي الخدمات/مشغلي الشبكات، اكتشاف الرسائل SPIM ونبذها عند الحافة القريبة، وهو الأمر الذي لا يمكِّن من توفير عرض النطاق للشبكة فحسب، ولكن يحول أيضاً دون استهلاك موارد مخدم المراسلة الفورية.

بيبليوغرافيا

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session initiation protocol (SIP) extension for instant messaging*. Available [viewed 2021-10-09] at: https://tools.ietf.org/html/rfc3428

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، 2022