الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1231

(2008/04)

السلسلة X: شبكات البيانات والاتصال بين الأنظمة المفتوحة والأمن

أمن الاتصالات

الاستراتيجيات التقنية لمكافحة الرسائل الاقتحامية

التوصيـــة ITU-T X.1231

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

الشبكات العمومية للبيانات	
الخدمات والمرافق	X.19–X.1
السطوح البينية	X.49–X.20
الإرسال والتشوير والتبديل	X.89–X.50
جوانب 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
تعاريف الخدمات	X.219–X.210
مواصفات البروتوكول بأسلوب التوصيل	X.229–X.220
مواصفات البروتوكول بأسلوب غياب التوصيل	X.239–X.230
جداول إعلان المطابقة (PICS)	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.399–X.370
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التوصيل الشبكي في التوصيل البيني للأنظمة المفتوحة (OSI) وجوانب النظام	
التوصيل الشبكي	X.629–X.600
الفعالية	X.639–X.630
نوعية الخدمة	X.649–X.640
التسمية والعنونة والتسجيل	X.679–X.650
ترميز النظم المجرد 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 لترميز النظم المجرد واحد (ASN.1)	X.899–X.890
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.1231

الاستراتيجيات التقنية لمكافحة الرسائل الاقتحامية

ملخص

تؤكد التوصية ITU-T X.1231 على الاستراتيجيات التقنية لمكافحة الرسائل الاقتحامية، كما تضم الخصائص العامة للرسائل الاقتحامية والأهداف الرئيسية لمكافحة الرسائل الاقتحامية. وعلاوة على ذلك ومع الإقرار بعدم وجود حل وحيد لحل مشكلة الرسائل الاقتحامية، تقدم هذه التوصية أيضاً قائمة مرجعية لتقييم الأدوات الواعدة في مجال مكافحة الرسائل الاقتحامية.

المصدر

وافقت لجنة الدراسات 17 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 18 أبريل 2008 على التوصية ITU-T X.1231 طبقاً للإجراء الوارد بالقرار 1 للجمعية العالمية لتقييس الاتصالات.

الكلمات المفتاحية

مكافحة الرسائل الاقتحامية، الرسائل الاقتحامية، الاستراتيجيات التقنية.

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 2009

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 تعاريف 1

1.3 مصطلحات معرَّفة في مواضع أخرى 1

2.3 مصطلحات معرَّفة في هذه التوصية 2

4 مختصرات 2

5 اصطلاحات 3

6 جوانب عامة 3

7 الأهداف العمومية 5

8 الاستراتيجيات التقنية 6

1.8 استراتيجيات التجهيزات 7

2.8 استراتيجيات الشبكة 8

3.8 استراتيجيات الخدمة 9

4.8 استراتيجيات الترشيح 10

5.8 استراتيجيات المعلومات الرجعية 12

9 تقييم النظام 12

ثبت المراجع 13

مقدمـــة

أصبحت ظاهرة الرسائل الاقتحامية، بمسايرة تطور صناعة المعلومات، مشكلة واسعة الانتشار تتسبَّب في خسائر في الإيرادات لدى مشغِّلي الاتصالات وموردي الخدمات والمستعملين في دوائر الأعمال التجارية، فضلاً عن آثارها الضارة بين المستعملين عموماً. وقد تطوَّرت ظاهرة الرسائل الاقتحامية من مجرد مصدر إزعاج إلى آفة عالمية.

ولذلك من الضروري التوصل إلى أساليب فعَّالة وناجعة لمكافحة الرسائل الاقتحامية. وهنالك جوانب عديدة لمكافحة الرسائل الاقتحامية: من تشريع وتدريب وتعاون دولي وغير ذلك. وتركز هذه التوصية بالدرجة الرئيسية على الوسائل التقنية.

التوصيـــة ITU-T X.1231

الاستراتيجيات التقنية لمكافحة الرسائل الاقتحامية

1 مجال التطبيق

تؤكد هذه التوصية بالدرجة الرئيسية على الاستراتيجيات التقنية لمكافحة الرسائل الاقتحامية كما تشتمل على الخصائص العامة للرسائل الاقتحامية والأهداف الرئيسية لمكافحتها. وعلاوة على ذلك، وبما أن ليس هنالك من حل وحيد لمشكلة الاقتحام، فإن هذه التوصية توفر أيضاً قائمة مرجعية لتقييم الأدوات الواعدة التي من شأنها مكافحة الرسائل الاقتحامية.

وتتناول هذه التوصية بالوصف الاستراتيجيات التقنية بصفة عامة ولا تحدد الاستراتيجيات التقنية لأي نمط معين من أنماط الرسائل الاقتحامية. وبالإضافة إلى ذلك، توفر هذه التوصية نموذجاً تراتبياً للفئات العامة التي يمكن استهدافها لإقامة بنية تحتية تتسم بالكفاءة والفعالية في مجال مكافحة الرسائل الاقتحامية. ويشتمل النموذج على الأقسام التالية:

- استراتيجيات خاصة بالتجهيزات؛
- استراتيجيات خاصة بالشبكات؛
- استراتيجيات خاصة بالخدمات؛
- استراتيجيات خاصة بعملية الترشيح؛
- استراتيجيات خاصة بالمعلومات الرجعية.

ومن الناحية العملية، توفر هذه التوصية استراتيجيات تقنية لمكافحة مختلف أنماط الرسائل الاقتحامية التي تراها إدارة ما بأنها غير ملائمة من منظور تطابقها مع القوانين والسياسات الوطنية.

2 المراجع

لا يوجد.

3 تعاريف

1.3 مصطلحات معرَّفة في مواضع أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في مواضع أخرى:

1.1.3 الاستيقان [b-ITU-T X.811]: توفير التأكد من صحة الهوية التي يدعيها كيان ما.

2.1.3 هاتف بروتوكول الإنترنت [b-ITU-T Q-Sup.49]: يشير هاتف بروتوكول الإنترنت إلى مطراف (مثال ذلك مطراف مكرس للصوت أو حاسوب شخصي متعدد الأغراض) موصول مباشرة (عبر سطح بيني إثرنت مثلاً أو خط xDSL) بشبكة تقوم على أساس بروتوكول الإنترنت.

3.1.3 كيان رسالة قصيرة (SME) [b-ITU-T Q.1742.3]: الكيان الذي يؤلف ويفكك الرسائل القصيرة. وقد يكون كيان الرسالة القصيرة أو لا يكون جزءاً متأصلاً لا يتميَّز عن سجل موقع الأصل (HLR) أو مركز رسائل (MC) أو سجل موقع زائر (VLR) أو محطة متنقلة (MS) أو مركز تبديل متنقل (MSC).

2.3 مصطلحات معرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 التبادل اللحظي للرسائل (IM): يشير إلى نقل الرسائل بين المستعملين في شبه الوقت الفعلي، وتكون هذه الرسائل عادة، قصيرة، وإن كان يمكن أن تكون غير ذلك. ويستعمل هذا التبادل بأسلوب تقليدي، بمعنى أن نقل الرسائل يتم بين المشاركين بسرعة تكفي للاستمرار في إقامة محادثة تفاعلية.

2.2.3 رسائل اقتحامية متعددة الوسائط عبر بروتوكول الإنترنت: تشير إلى رسائل أو نداءات غير مطلوبة في تطبيقات متعددة الوسائط في الوقت الفعلي عبر بروتوكول الإنترنت. وخلافاً للرسائل الاقتحامية التقليدية عبر البريد الإلكتروني، فإن الرسائل الاقتحامية متعددة الوسائط عبر بروتوكول الإنترنت تشير إلى الرسائل الاقتحامية على طرائق الاتصالات الناشئة حديثاً عبر بروتوكول الإنترنت، مثل المراسلة الفورية وخدمة الحضور ونقل الصوت بواسطة بروتوكول الإنترنت (VoIP) وغير ذلك. والاقتحام على المهاتفة عبر شبكة الإنترنت (SPIT) والرسائل الاقتحامية الصوتية أو الرسائل الاقتحامية على نقل الصوت عبر بروتوكول الإنترنت (VAM) والرسائل الاقتحامية على التبادل الخطي للرسائل (SPIM) أسماء حالية خاصة ببروتوكول الإنترنت تحديداً.

3.2.3 الكيفية: يشير مصطلح الكيفية إلى تشفير المعلومات، وهي تشتمل على معلومات من الممكن للكائنات البشرية أن تدركها. مثال ذلك: تشتمل معلومات الكيفية على نص أو رسوم أو صوت أو فيديو أو بيانات لمسية تُستخدم في التفاعل بين الفرد والحاسوب. وقد تنطلق المعلومات متعددة الكيفية من أجهزة متعددة الكيفية، أو تستهدف هذه الأجهزة، مثل الميكروفون بالنسبة لإدخال الكلام/الصوت أو القلم لإدخال لمسي أو لوحة المفاتيح لإدخال نص أو الفأرة لإدخال حركة أو مجهار لإخراج صوت مركب أو الشاشة لإخراج رسوم/نص أو جهاز اهتزاز لرد فعل لمسي أو جهاز كتابة "برايل" للمعاقين بصرياً.

4.2.3 رسالة متعددة الكيفيات: تشير الرسالة متعددة الكيفيات إلى نوع من أنواع الرسائل متعددة الوسائط التي تحتوي معلومات مشفرة مختلفة من أجل التفاعل عن طريق تعدد الكيفيات.

5.2.3 خدمة تبادل الرسائل متعددة الوسائط (MMS): تشير خدمة تبادل الرسائل متعددة الوسائط إلى نوع من أنواع خدمة المراسلة بعد خدمة الرسائل القصيرة (SMS) والتي بإمكانها نقل مختلف الرسائل متعددة الوسائط، بما فيها النصوص والرسوم والصوت والفيديو وغير ذلك، من خلال شبكة متنقلة أو شبكة لا سلكية أو شبكة ثابتة.

6.2.3 خدمة الرسائل القصيرة (SMS): تشير خدمة الرسائل القصيرة إلى نوع من أنواع خدمات المراسلة التي تتيح للهواتف المتنقلة والهواتف الثابتة والكيانات الأخرى للرسائل القصيرة (SME) نقل واستلام رسائل نصية من خلال جهاز يدعى مركز الخدمة يقوم بتنفيذ الوظائف مثل عمليات الحفظ والتسليم.

7.2.3 المقتحم (Spammer): يشير هذا المصطلح إلى الكيان أو الشخص الذي يقوم بتوليد الرسالة الاقتحامية وإرسالها.

4 مختصرات

تستعمل هذه التوصية المختصرات التالية:

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

DoS منع الخدمة (*Denial of Service*)

E-mail بريد إلكتروني (*Electronic Mail*)

HLR سجل موقع الأصل (*Home Location Register*)

IM مراسلة فورية (*Instant Messaging*)

IP بروتوكول الإنترنت (*Internet Protocol*)

MC مركز مراسلة (*Message Centre*)

MMS خدمة مراسلة متعددة الوسائط (*Multimedia Messaging Service*)

MS محطة متنقلة (*Mobile Station*)

MSC مركز تبديل متنقل (*Mobile Switching Centre*)

PSTN شبكة مهاتفة عمومية تبديلية (*Public Switched Telephone Network*)

SME كيان رسائل قصيرة *(Short Message Entity)*

SMS خدمة الرسائل القصيرة (*Short Message Service*)

SMTP بروتوكول بسيط لنقل البريد (*Simple Mail Transfer Protocol*)

SPIM اقتحام على التبادل اللحظي للرسائل على الإنترنت (*Spam over Internet Messaging*)

SPIT اقتحام على مهاتفة الإنترنت (*Spam over Internet Telephony*)

VAM اقتحام صوتي أو اقتحام على نقل الصوت بواسطة بروتوكول الإنترنت (*Voice Spam or VoIP Spam*)

VLR سجل موقع الزائر (*Visitor Location Register*)

VoIP نقل الصوت بواسطة بروتوكول الإنترنت (*Voice over IP*)

5 اصطلاحات

لا يوجد.

6 جوانب عامة

الرسائل الاقتحامية عبارة عن معلومات إلكترونية تقدَّم من المرسِلين إلى المستقبلين بواسطة مطاريف، مثل الحواسيب والهواتف المتنقلة والهواتف الثابتة وغير ذلك، وهي عادة معلومات غير مطلوبة وغير مرغوبة وتعود بالضرر على المستقبلين. ويمكن حمل الرسائل الاقتحامية بواسطة البريد الإلكتروني والمراسلة المتنقلة (SMS وMMS وغير ذلك) وبروتوكول الإنترنت متعدد الوسائط وغير ذلك من الأشكال الإلكترونية. ويتوقف معنى كلمة "الاقتحام" في الواقع على أشكال إدراك معيَّنة تبعاً للبلدان أو المنظمات أو الأفراد. وعلى وجه التحديد، فإن معنى الكلمة يتطوَّر ويتسع بتطور تكنولوجيات اتصالات المعلومات التي توفر فرصاً جديدة للرسائل الاقتحامية. وتتسم هذه الرسائل عموماً بالخصائص المشتركة التالية:

إلكترونية: الرسائل الاقتحامية عبارة عن معلومات إلكترونية تُنقَل عادة عبر شبكة اتصالات مفتوحة، لا سيما الإنترنت، وهي تختلف كثيراً عن الطرائق التقليدية لاستعمال البريد أو الإعلانات الورقية أو التسويق المباشر. فالرسائل الاقتحامية رخيصة الثمن ميسورة وسهلة التمويه.

غير مطلوب: غالباً ما تضم الرسائل الاقتحامية إعلانات أو معلومات مزيفة أو فيروسات أو غير ذلك.

وعلاوة على ذلك، فإن الرسائل الاقتحامية تتسم عموماً بالخصائص التالية كلياً أو جزئياً:

الجملة والتكرار: تُرسَل الرسائل الاقتحامية والرسائل الاقتحامية الإلكترونية عادة بالجملة ودون تمييز، بينما تنطلق الاتصالات الاقتحامية في الوقت الفعلي دائماً بصورة تكرارية. غير أن المقتحم لا يعرف شيئاً سوى عنوان الاتصال بالمستقبل (مثل عنوان البريد الإلكتروني ورقم هاتف المستقبِل).

استخدام العناوين دون موافقة أصحابها: غالباً ما يستعمل المقتحمون عناوين اتصال تُجمَع دون موافقة أصحابها صراحةً لإرسال الرسائل الاقتحامية. ويمكن لبعض البرمجيات أن تجمع عادة عناوين الاتصال من شبكة الويب أو تستحدث العناوين تلقائياً.

مصادر الرسائل مخفية أو كاذبة: غالباً ما تُرسَل الرسائل الاقتحامية بطريقة تموِّه عن مصدرها باستخدام عنوان رسالة كاذب أو بإخفاء المصدر بكل بساطة. ويستخدم المقتحمون عادة مخدِّمات غير مرخَّص بها لأطراف ثالثة لا تتحقق من معلومات المصدر.

صعوبة المنع: من الصعب جداً كشف الرسائل الاقتحامية بسبب الكمية الهائلة من هذه الرسائل. وقد تكون محاولات منع الرسائل الاقتحامية صعبة وقد تؤدي، في بعض الأحيان، إلى حالات إيجابية كاذبة أو حالات سلبية كاذبة.

وينبغي أن تكون هذه الاستراتيجيات محايدة تكنولوجياً، ومع ذلك من المفيد تقييم عدد من العوامل: ما هي وسائط الاتصال تحديداً التي يساء استخدامها أو التي تتسبب في مشاكل ضمن الولاية القضائية، وأي وسائط اتصال تنطوي على احتمال قوي بأن يساء استخدامها في المستقبل، وما هي الوسائط التي من غير المحتمل أن يساء استخدامها. والخيارات الشائعة هي كما يلي:

البريد الإلكتروني

تعد الرسائل الاقتحامية عبر البريد الإلكتروني في الوقت الراهن هي النوع الأكثر تهديداً من بين مختلف أنماط الاقتحام، وذلك بسبب مواطن ضعف بروتوكول البريد الإلكتروني وثغرات الأمن في البنية التحتية الأساسية، أي شبكة الإنترنت، التي يُرسَل البريد الإلكتروني عبرها. والبروتوكول البسيط لنقل البريد (SMTP) هو أكثر البروتوكولات شيوعاً في ترحيل البريد الإلكتروني. ويحدد هذا البروتوكول غلافاً ورأسية لكل رسالة إلكترونية. ويحتوي الغلاف على عنوان المستقبل ولا يمكن أن يراه هذا الأخير. وهو يُستخدم كعنوان مقصد لنقل الرسائل من المرسِل إلى المستقبل. ومن الممكن عادة، أثناء النقل، نسخ عنوان المقصد في الغلاف ووضعه في رأسية الرسالة الإلكترونية التي يمكن للمستقبل أن يراها. ويستغل المقتحمون نوعين من مواطن الضعف في عملية استيقان البروتوكول البسيط لنقل البريد:

- الاستيقان غير مطلوب، ومن ثم يمكن للمستعملين إخفاء عناوينهم أو تزويرها.
- من الممكن تزوير معظم السجلات المدرجة في الغلاف وفي رأسية الرسالة الإلكترونية.

وعلاوة على ذلك، تعد تكاليف إرسال رسالة اقتحامية عبر البريد الإلكتروني ضئيلة جداً بينما تكون آثارها السلبية كبيرة جداً في الغالب.

خدمة المراسلة المتنقلة

إن المزايا المرموقة للاتصالات المتنقلة هي الراحة والكفاءة وانخفاض التكلفة وسهولة الاستعمال. ولكن يواجه المستعملون في هذه الأيام الرسائل الاقتحامية على المراسلة المتنقلة في الوقت الذي يتمتعون فيه بمزايا الاتصالات المتنقلة. وعبارة الرسائل الاقتحامية المتنقلة تُستعمَل عموماً للدلالة على الرسائل غير المطلوبة التي تُرسَل عبر الخدمة SMS أو MMS. وتتمثل حالياً الأنماط الرئيسية من الرسائل الاقتحامية القصيرة فيما يلي:

- خداع باسم الاشتراك في الخدمة؛
- معلومات إعلانات؛
- غش مخالف للقانون؛
- معلومات خلاعية.

وتكون هذه الأنواع من الرسائل عموماً خدّاعة أو تزويرية، وتُعرَف أيضاً باسم رسائل احتيالية.

ومن الجدير بالملاحظة أنه أصبح الآن من الشائع استلام بريد إلكتروني على الأجهزة المتنقلة، وذلك مع تقدم البريد الإلكتروني المتنقل وهو ما يسهل استخدامه بواسطة المقتحمين.

الوسائط المتعددة القائمة على بروتوكول الإنترنت

إزاء تطور الوسائط المتعددة القائمة على بروتوكول الإنترنت، بدأ مفهوم الاقتحام يُستعمَل على نطاق واسع بالنسبة لهذه الوسائط، مثال ذلك اقتحام التبادل اللحظي للرسائل واقتحام المهاتفة على الإنترنت واقتحام الحضور واقتحام المراسلة على الويب واقتحام مجموعة أنباء استعمال الشبكة واقتحام تبادل الألعاب على الخط، وغير ذلك. وهنالك في بعض الحالات مصطلحات مختلفة للرسائل الاقتحامية التي تُوزَّع في أنماط معيَّنة من الوسائط، مثل الاقتحام على التبادل اللحظي للرسائل على الإنترنت (SPIM)، والاقتحام على المهاتفة على الإنترنت (SPIT)، وغيرها. وعلاوة على ذلك، فإن التفاعلات متعددة الكيفيات، كأنماط جديدة للوسائط المتعددة، تتأثر هي الأخرى بظاهرة الاقتحام حيث من الممكن أن يكون "الاقتحام" متعدد الوسائط وحيد ذو مظاهر متعددة بالنسبة للسطوح البينية للمستعمِل. فقد تؤدي رسالة "اقتحام" على الشبكة مثلاً إلى تشغيل تسجيل سمعي "اقتحامي"، وإلى عرض رسالة نصية "اقتحامية" وإلى عرض نص رسالة "اقتحامي" على الشاشة، وقد يكون المحتوى مماثلاً أو مختلفاً فيها جميعاً. ومن هذا المنطلق، فإن تعدد الأساليب يزيد من التعرض "للاقتحام" متعدد الوسائط، وبالتالي فإن من المرتقب أن تتفاقم مشكلة "الاقتحام" متعدد الأساليب عندما تزداد انتشاراً التفاعلات متعددة الأساليب.

الاقتحام على التبادل اللحظي للرسائل على الإنترنت (SPIM): التبادل اللحظي للرسالة هو نوع من طرائق الاتصال المريحة والرخيصة في الوقت الفعلي على شبكة الإنترنت وهي طريقة تتطوَّر بسرعة، وتُستخدم بالدرجة الرئيسية في الاتصالات الخاصة. وفي الوقت ذاته، يزداد استعمال تطبيقات التبادل اللحظي للرسائل في المؤسسات التجارية. ولكن لسوء الحظ، يجري توزيع المزيد والمزيد من المعلومات غير القانونية، مثل الفيروسات والشفرات المؤذية وغيرها، بواسطة التبادل اللحظي للرسائل الذي يعرف على نحو شائع بمختصر SPIM. وعلى الرغم من أن هذا الاقتحام يمثل نسبة مئوية صغيرة من جميع أشكال الاقتحام فإنها تزداد بسرعة.

الاقتحام على المهاتفة عبر الإنترنت (SPIT): تشمل بعض المشكلات الخاصة بالاقتحام والتي تم تحديدها حتى الآن تلك المشكلات المرتبطة عادةً بشبكات بروتوكول الإنترنت، بالإضافة إلى تهديد آخر أكثر تعقيداً، مثل التمثيل الكاذب والتنصت وهجمات منع الخدمة الخاصة بنقل الصوت عبر بروتوكول الإنترنت، وعمليات دس الرزم والرسائل غير المطلوبة (الاقتحام على نقل الصوت بواسطة بروتوكول الإنترنت (VoIP) أو الاقتحام على المهاتفة عبر الإنترنت (SPIT)). ومردّ هذا النوع الأخير بالدرجة الرئيسية الإمكانية التي توفرها تقنية VoIP لنقل الرسائل الصوتية بتكلفة منخفضة جداً، مما قد يؤدي إلى حالة مماثلة للحالة المشهودة الآن بخصوص الرسائل الاقتحامية عبر البريد الإلكتروني: أي إمكانية إرسال أعداد كبيرة من رسائل البريد الصوتي غير المطلوبة عبر العالم في عدة ثوان.

تطور الاقتحام

لا يقتصر الاقتحام على الخيارات المذكورة أعلاه. فمع إدخال المزيد والمزيد من تكنولوجيات وتطبيقات اتصالات المعلومات، فإن الرسائل الاقتحامية ستتطور بشكل شامل. وعلاوة على ذلك، يمكن لأي تكنولوجيا أو تطبيق من تكنولوجيات وتطبيقات الاتصالات أن تكون وسطاً للاقتحام إذا لم تكن حلول مكافحة الاقتحام ناجعة.

7 الأهداف العمومية

يرمي هذا القسم إلى وصف الأهداف الأساسية لمكافحة الاقتحام. ومحاور التركيز هو ما ينبغي تحقيقه وليس تحديد خطوات التنفيذ العملية.

وتتمثل الأهداف من مكافحة الاقتحام فيما يلي:

- التحقق من صلاحية من حيث ما إذا كان لديها امتيازات إرسال الرسائل أو استهلال الاتصالات بعد عملية الاستيقان و/أو بوجود الترخيص.
- حماية العنوان و/أو المعلومات الهامة الأخرى المتعلقة بالرسائل أو الاتصالات التي ترسلها كيانات مشروعة من العمل على إخفائها أو تمويهها.

- حماية الخصوصية أثناء إرسال المعلومات.
- مسؤولية جميع الكيانات عن تصرفاتها الخاصة بها فيما يتعلق بإرسال المعلومات أو ترحيلها.
- حماية شبكات الاتصالات من النفاذ أو التشغيل غير المرخَّص به وذلك حرصاً على ضمان إمكانية النفاذ على نحو يتسم بالفعالية والكفاءة.
- توفير المعلومات الضرورية بخصوص المصدر من أجل التعقب مستقبلاً.
- حماية تجهيزات الخدمة من الفيروسات ومن النفاذ غير المرخَّص به وذلك حرصاً على إمكانية التيسُّر.
- ترشيح الرسائل الاقتحامية وإذا اقتضى الأمر تخزينها في تجهيزات معيَّنة لأغراض التعقب والتحليل القضائي.
- توفير منصات للمعلومات الرجعية، والتي لا تشجع الإبلاغ الدقيق والفعال للمعلومات فحسب وإنما تدعم أيضاً التعاون الدولي والتشريعات، وغير ذلك.
- استعمال بروتوكولات دولية معروفة جيداً من أجل تبادل المعلومات على النحو الملائم وتعميمها فيما يتعلق بمكافحة الاقتحام.

وعلاوة على ذلك، فإن تحقيق الأهداف المدرجة أعلاه ينبغي أن يقوم على أساس البيئة المحدَّدة في كل حالة.

8 الاستراتيجيات التقنية

من الضروري، لمكافحة الاقتحام، اتباع نهج متعدد الجوانب يشمل الملامح التالية: تكنولوجيا تحركها الصناعة، وانضباط ذاتي من دوائر الصناعة، وتعاون دولي، وتشريعات، ومعلومات رجعية، وتدريب. ومن بين هذه الجوانب تعد التكنولوجيا ضرورية لضمان تنفيذ الجوانب الأخرى. وتركز هذه التوصية بالدرجة الأولى على الاستراتيجيات التقنية العامة لمكافحة الاقتحام.

وتيسيراً لعملية التحليل من الأفضل تصنيف الخدمات أولاً. ومن الممكن، تبعاً لطريقة الإرسال، تصنيف الخدمات إلى صنفين: صنف التخزين والإرسال، وصنف الاتصال في الوقت الفعلي. ويشمل صنف التخزين والإرسال خدمات البريد الإلكتروني وخدمات المراسلة المتنقلة وخدمات تبادل الرسائل متعددة الوسائط، وغير ذلك. أما صنف الاتصال في الوقت الفعلي فيشمل المهاتفة القائمة على بروتوكول الإنترنت والفاكس القائم على بروتوكول الإنترنت والتبادل اللحظي للرسائل، وغير ذلك. وتختلف طرائق مكافحة الرسائل الاقتحامية باختلاف الخدمات. ولذلك يحتاج الأمر إلى تحليل مفصَّل لخدمة معيَّنة إزاء الاستراتيجيات التقنية العامة.

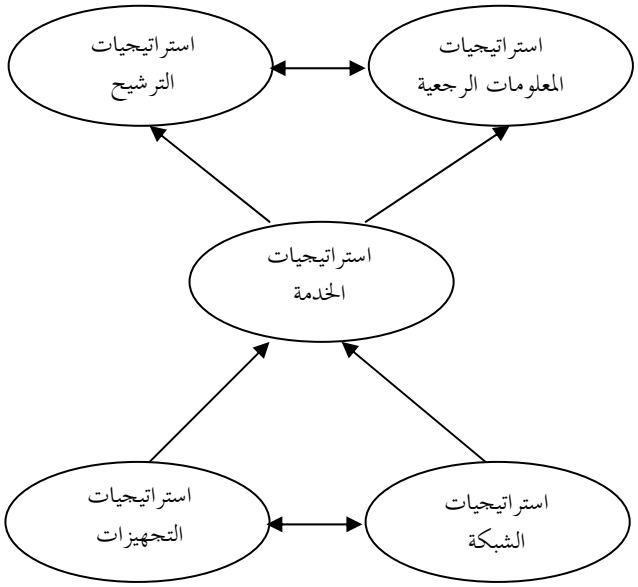
ومن الموصى به، لمكافحة الاقتحام بصورة فعَّالة، تنفيذ نموذج تراتبي مختلف الأجزاء. أضف إلى ذلك، أن فعالية النموذج تزداد بزيادة الأجزاء التي يتألف منها. ويبيِّن الشكل 1 نموذج تراتبي لمكافحة الاقتحام حيث يوصف على النحو التالي:

استراتيجيات المعلومات الرجعية	استراتيجيات الترشيح
استراتيجيات الخدمة	
استراتيجيات الشبكة	استراتيجيات التجهيزات

الشكل 1 – نموذج تراتبي لمكافحة الاقتحام

وتُقسم الأجزاء الخمسة في هذا النموذج التراتبي إلى ثلاثة مستويات: مستوى البنية التحتية ومستوى الخدمة ومستوى التطبيق. ويقوم النموذج التراتبي على أساس استراتيجيات التجهيزات واستراتيجيات الشبكة التي تنتمي إلى مستوى البنية التحتية. ويمثل تحقيق هذه الاستراتجيات حجر القاعدة المأمون والمكين بالنسبة إلى الاستراتيجيات التقنية في الطبقات الأعلى. وتجدر الإشارة إلى أن استراتيجيات التجهيزات واستراتيجيات الشبكة تؤثر كل منها على الأخرى. كما أن الشبكة المأمونة تحتاج إلى تجهيزات مأمونة بينما تحتاج التجهيزات المأمونة إلى شبكات مناسبة. واستراتيجيات الخدمة، التي تنتمي إلى مستوى الخدمة، هي أهم جزء من الأجزاء الخمسة لأن هذه الطبقة مسؤولة مباشرة عن توفير الخدمة. وأخيراً، تنتمي كلتا متطلبات

الترشيح ومتطلبات المعلومات الرجعية إلى مستوى التطبيق وهي أقرب إلى المستعملين من أجل مكافحة الاقتحام. بيد أنها تتفاعل فيما بينها. ويبيِّن الشكل 2 العلاقة القائمة بين مختلف الأجزاء:



الشكل 2 – العلاقة بين مختلف الأجزاء

وإضافة إلى ذلك، يوصى باستعمال بروتوكولات دولية معروفة جيداً للوفاء بهذه الاستراتيجيات التقنية. ولكن في حال الوفاء بكل الاستراتيجيات التقنية، فقد تكون التكلفة عالية جداً مقارنة بقيمة الخدمات الجاري حمايتها. ومن ثم فمن المهم إلى حد كبير تكييف الاستراتيجيات التقنية طبقاً لسيناريوهات التطبيق. كما ينبغي توفير طرائق مكافحة الرسائل الاقتحامية بحيث تسمح بهذا التكييف. ونتيجة للأعداد الكبيرة من التوليفات المحتملة من الاستراتيجيات التقنية، يفضل وجود نماذج تغطي نطاق واسع من الخدمات. ويمكن للتقييس عبر المنظمات الصناعية ومنظمات البحوث الرائدة أن يسهل من إعادة استعمال الحلول والمنتجات. وفي نفس الوقت، يمكن نشر حلول مكافحة الرسائل الاقتحامية بسرعة أكبر أو بتكلفة أقل.

1.8 استراتيجيات التجهيزات

التجهيزات هي حجر القاعدة في البنية التحتية لمكافحة الرسائل الاقتحامية. لذلك فإن حماية التجهيزات مسألة أساسية في مكافحة الرسائل الاقتحامية.

1.1.8 تحسين أمن البرمجيات في التجهيزات ذات الصلة

يقوم المقتحمون بتوزيع رسائلهم باستخدام موارد الحواسيب وموارد الشبكات التي تملكها أطراف ثالثة بمجرد أن تنم هذه الموارد عن مواطن ضعف واضحة. وتصبح هذه الموارد بمثابة ضحايا، وتُطلَق عليها أسماء شبكات مُسيَّرة (botnet) أو حواسيب مأمورة (zombie). وبذلك يستطيع المقتحمون التحكم بالضحايا عن بُعد لإرسال الرسائل الاقتحامية. ومن الحلول الناجعة تركيب نظام تشغيل مأمون وبرمجية تطبيق مأمونة وتحديث برمجيات مكافحة الفيروسات في الوقت المناسب لحماية التجهيزات ذات الصلة من الفيروسات.

2.1.8 توفير أدوار إدارة مختلفة

نظراً لأهمية أنظمة الخدمات، فإن الأمر يستدعي توفير أدوار إدارة مختلفة. وينبغي على الأقل أن تشتمل على دور إدارة المستعملين ودور إدارة النظام ودور إدارة التدقيق. ويُستخدم دور إدارة المستعملين لإدارة تشكيلة المديرين والمشغِّلين والمدققين. ويُستخدم دور إدارة النظام للحفاظ على التجهيزات وتشغيلها. أما دور إدارة التدقيق فيُستخدم لتدقيق سجلات التشغيل وسجلات النظام. وعلاوة على ذلك، قد تحتاج بعض الخدمات المحددة إلى بعض أدوار الإدارة المعيَّنة.

3.1.8 توفير سجل التشغيل وسجل النظام

يتعيَّن على النظام أن يوفر سجلات تشغيل وسجلات نظام لضمان التشغيل المنتظم للنظام وللحفاظ عليه في حالة التشغيل الاعتيادي.

وتُستخدم سجلات التشغيل لتتبع الأحداث. وينبغي لها أن تسجل جميع أحداث الدخول والتشغيل. وينبغي أن تتضمن سجلات التشغيل الحقول التالية، على أقل تقدير: اسم المشغِّل ووقت التشغيل وأمر التشغيل ونتيجة التشغيل.

بإمكان سجلات النظام أن توفر تاريخ حالة عمل النظام. وهي تشمل بالدرجة الأولى معلومات الأداء ومعلومات الخلل، وغير ذلك. وقد تختلف سجلات الأنظمة باختلاف الأنظمة وباختلاف الخدمات.

غير أن سجلات التشغيل وسجلات الأنظمة لا تقتصر على الحفاظ على النظام فحسب، بل يمكن أن تساعد المديرين أيضاً في ضمان الإجراءات التشغيلية دون أنشطة تخريبية.

4.1.8 تحسين أمن المطاريف ومرونتها

إن المطاريف هي أهم تجهيزات المستعمل النهائي وهي دوماً الضحايا المباشرة لعملية الاقتحام. وبما أن الوظائف تختلف دوماً باختلاف أنماط المطاريف، فلا بد من أن يقتصر الأمر على استراتيجيات عامة. وهي تشتمل على الاستراتيجيات التالية دون أن تقتصر عليها:

- دعم عمليات الاستيقان والترخيص، خصوصاً من أجل المطاريف الذكية؛
- دعم الاحتفاظ بقائمة سوداء وقائمة بيضاء؛
- توفير برمجية لمكافحة الفيروسات، خصوصاً من أجل المطاريف الذكية.

2.8 استراتيجيات الشبكة

إن أمن الشبكة، على غرار متطلبات التجهيزات، هو كذلك الأساس في مكافحة الاقتحام. إذ من الممكن تخفيض الاقتحام إلى حد كبير من خلال التصميم الملائم لطبولوجيا الشبكة ونشر مختلف تجهيزات الأمن، مثل جدران الوقاية والمسيِّرات المأمونة والبوابات المأمونة، وغير ذلك.

1.2.8 حماية شبكة الخدمات من الإنترنت

تواجه شتى خدمات الشبكات تهديدات من الإنترنت لأن معظم هذه الخدمات تعتمد على تكنولوجيا بروتوكول الإنترنت ذات المعايير المفتوحة.

ومن المطلوب توفر الوظائف التالية:

- حماية شبكات الخدمات من هجمات الإنترنت، مثل هجمات منع الخدمة (DoS) وهجمات منع الخدمة الموزعة (DDoS). وشبكات الخدمة هامة جداً ويتحكم فيها مديرو الشبكات عادة عن بُعد. وبما أن شبكة الإنترنت مفتوحة أمام الجميع، فإن من الضروري أن تتمكن شبكات الخدمات من مقاومة استغلال مواطن الضعف في الإنترنت. وتُستعمل جدران الوقاية وغيرها من تجهيزات الأمن عادة لحماية شبكات الخدمة من مواطن الضعف هذه.
- حماية إشارات البروتوكولات في مستوي التحكم لمنع عمليات الاقتحام غير المشروعة. وهي تتسم بأهمية خاصة بالنسبة لنقل الصوت بواسطة بروتوكول الإنترنت (VoIP). وتكون الشبكة الهاتفية العمومية التبديلية (PSTN) مأمونة ومكينة دائماً أما الإنترنت فإنها غير مأمونة وغير مكينة. ولذلك ينبغي لبوابات نقل الصوت بواسطة بروتوكول الإنترنت (VoIP) أن تتمكن من منع إشارات البروتوكولات غير المشروعة وذلك لتحقيق نفس مستوى الأمن الذي تتمتع به الشبكة الهاتفية العمومية التبديلية (PSTN).

2.2.8 توفير آلية إطناب وآلية احتياط للحفاظ على استقرار شبكة الخدمات

نظراً للأهمية البالغة التي تتسم بها تجهيزات الخدمة وشبكات الخدمة فإنها تتطلب توفر تجهيزات إطناب ومسيّرات احتياطية. وعلاوة على ذلك، ينبغي أن تكون آلية الإطناب والاحتياط آلية عملية وفعَّالة وتتسم بالكفاءة من حيث التكلفة.

3.8 استراتيجيات الخدمة

تعتبر استراتيجيات الخدمة أكثر الأجزاء أهمية في النموذج التراتبي لأن الخدمات تلبي متطلبات المستعملين بشكل مباشر. ولكن هناك الكثير والكثير من أنواع الخدمات التي تختلف وظائفها ومواطن الضعف فيها. ولذلك، فإن استراتيجيات الخدمة الخاصة بمكافحة الرسائل الاقتحامية تختلف في الخدمات المختلفة عن بعضها البعض. بيد أن الخدمات المختلفة لها نفس استراتيجيات الخدمة العامة الخاصة بمكافحة الرسائل الاقتحامية والتي يرد ذكرها كالتالي.

1.3.8 دعم الاستيقان

عندما تقوم الكيانات (المستعملون أو التجهيزات) بالنفاذ إلى الخدمات، ينبغي أن تدعم أنظمة الخدمات الاستيقان الصارم. فمن جهة أولى، بإمكان الاستيقان الصارم أن يحول دون قيام كيان غير صحيح من النفاذ إلى الخدمات. ومن جهة أخرى، يمكن استعمال سجلات الاستيقان الدقيقة في عملية التعقب.

وفي الوقت الحاضر، حققت بعض البلدان الكثير من الإنجازات في مجال الشبكات المتنقلة نتيجة لتطبيق الاستيقان وآليات الوقت الفعلي.

2.3.8 دعم عنوان الترحيل القابل للتشكيل

ينبغي غلق الترحيل المفتوح وأن يعتمد الترحيل المحدود في تجهيزات الخدمة. وينبغي أن تدعم تجهيزات الخدمة قوائم عناوين ترحيل قابلة للتشكيل. فهي لا تقوم بترحيل الرسائل إلا من العناوين المسموح بها. وعلى النقيض من ذلك، تُحجب الرسائل الواردة من عناوين أخرى.

3.3.8 دعم نسق رسائل صارم

ينبغي بالنسبة لبعض الرسائل، خصوصاً الرسائل التجارية، تحديد نسق الرسالة على نحو صارم. وبذلك يستطيع نظام الخدمة أن يحصل على معلومات كافية للتعامل مع الرسائل.

4.3.8 التوافق مع المعايير الدولية

يجب أن تكون بروتوكولات الاتصالات للخدمات متوافقة مع المعايير الدولية، وذلك حرصاً على تعزيز مقدرة التوصيل البيني والتشغيل البيني.

5.3.8 تحسين إمكانية تعقب الرسائل الاقتحامية

ينبغي من جهة أولى، أن تتمكن أنظمة الخدمات من تحديد هوية الكيانات (مستعملون أو تجهيزات) إبان نفاذها إلى أنظمة الخدمات والاستيقان منها وأن تحصل على معلومات دقيقة عن مصدر الكيانات، وعندئذٍ تدوِّن المعلومات الملائمة في قواعد البيانات. وينبغي من جهة أخرى، أن توفر أنظمة الخدمات وظائف التدقيق من أجل عملية التعقب استناداً إلى السجلات المدرجة بقواعد البيانات.

6.3.8 دعم التحكم في التدفق

بإمكان مديري الأنظمة الحد من عرض نطاق الاتصال أو عدد الرسائل المرسَلة في كل فاصل زمني معيَّن.

7.3.8 توفير وظائف الإحصاءات

تبيِّن المعلومات الإحصائية لمديري الأنظمة الحالة الراهنة للنظام، من قبيل حجم الحركة ومعلومات الزوار.

4.8 استراتيجيات الترشيح

إن عملية الترشيح من أكثر التكنولوجيات شيوعاً في مجال مكافحة الرسائل الاقتحامية. وتكمن الميزة الرئيسية لعملية الترشيح في البساطة ومرونة التنفيذ.

1.4.8 دعم ترشيح الرسائل الاقتحامية

هنالك عموماً نمطان من الترشيح: ترشيح يعتمد على العنوان وترشيح يعتمد على المحتوى (بما في ذلك الترشيح القائم على أساس الكلمات الرئيسية).

ومن الممكن استعمال الترشيح القائم على أساس العنوان في كل من خدمات التخزين والإرسال وخدمات الوقت الفعلي. ففي خدمات التخزين والإرسال، يُستعمَل الترشيح القائم على العنوان لفرز الرسائل والبريد الإلكتروني تبعاً لعنوان مصدرها. وهو فعَّال في الحيلولة دون قيام أنظمة الخدمة بإرسال أو ترحيل رسائل اقتحامية وبريد إلكتروني اقتحامي. وبالنسبة لخدمات الوقت الفعلي، يُستخدم الترشيح القائم على أساس العنوان لمنع النداءات تبعاً لرقم الهاتف أو عنوان المنادي. والترشيح القائم على العنوان فعَّال جداً ومريح جداً في مكافحة الاقتحام، بوجه عام.

ومن الممكن أيضاً استعمال الترشيح القائم على المحتوى في كل من خدمات التخزين والإرسال وخدمات الوقت الفعلي. فبالنسبة لخدمات التخزين والإرسال، يُستعمل الترشيح القائم على المحتوى لفرز الرسائل والبريد الإلكتروني اعتماداً على المحتوى أو الكلمات المفتاحية. وبالنسبة لخدمات الوقت الفعلي، يُستعمل الترشيح القائم على المحتوى لقطع الاتصالات اعتماداً على محتواها. والترشيح القائم على المحتوى معقول أكثر نظرياً بالمقارنة مع الترشيح القائم على أساس العنوان. ولكن الترشيح القائم على المحتوى يستهلك الكثير من الموارد دائماً وترتبط دقته ارتباطاً وثيقاً بخوارزميات التحليل.

وليس بمقدور أي من طريقتي الترشيح التمكن من ترشيح كل الرسائل الاقتحامية. ومن ثم يفضل استخدام الطريقتين في آن واحد. وعلاوة على ذلك، ينبغي لتجهيزات الخدمة أن تدعم ترشيح الفيروسات.

2.4.8 توفير آلية احتياط/تسجيل لترشيح البريد الاقتحامي

فيما يتعلق بخدمات التخزين والإرسال، ينبغي لتجهيزات الخدمة أن تخزن نسخة احتياطية من الرسائل الاقتحامية أوتوماتياً. وفيما يتعلق بخدمات الوقت الفعلي، ينبغي لتجهيزات الخدمة أن تسجل ملخصات للرسائل الاقتحامية أوتوماتياً. ويتم تخزين النسخة الاحتياطية والملخصات لأي استفسار في المستقبل.

3.4.8 متطلبات الأداء من أجل ترشيح الرسائل الاقتحامية

إن الأداء عملية هامة جداً من أجل ترشيح الرسائل الاقتحامية. ومعدلات الردود الإيجابية الكاذبة والردود السلبية الكاذبة من أهم العوامل في تقييم أداء ترشيح الرسائل الاقتحامية. ويشير مصطلح "الردود الإيجابية الكاذبة" إلى الكشف عن حالات سلبية عندما لا تكون هنالك حالات سلبية، أما مصطلح الردود "السلبية الكاذبة" فيشير إلى عدم الكشف عن حالات سلبية عندما تكون هنالك حالات سلبية بالفعل. لذلك فإن معدل الردود الإيجابية الكاذبة هو نسبة الحالات السلبية التي أُبلِغ عنها خطأ بأنها حالات إيجابية، ومعدل الردود السلبية الكاذبة هو نسبة الحالات الإيجابية التي أُبلِغ عنها خطأ بأنها حالات سلبية. ويبيِّن الجدول 1 نتيجة ترشيح الرسائل الاقتحامية.

الجدول 1 – نتيجة ترشيح الرسائل الاقتحامية

		الحالة الفعلية	
		الحالات الإيجابية	الحالات السلبية
نتيجة الاختبار	الحالات الإيجابية المكتشفة	A	B
	الحالات السلبية المكتشفة	C	D
ملاحظة – تمثل الحالة الإيجابية حالة اقتحام، وتمثل الحالة السلبية عدم اقتحام.			

يُرمَز إلى مجموع عدد حالات الاختبار بالحرف T.

$$D + C + B + A = T$$

عدد الردود الإيجابية الكاذبة يساوي B.

عدد الردود السلبية الكاذبة يساوي C.

معدل الردود الإيجابية الكاذبة = $B / (B + D)$.

معدل الردود السلبية الكاذبة = $C / (A + C)$.

وثمة علاقة ارتباط وثيقة بين معدل الردود الإيجابية الكاذبة ومعدل الردود السلبية الكاذبة. فعادة، كلما كان معدل الردود الإيجابية الكاذبة مرتفعاً، كان معدل الردود السلبية الكاذبة منخفضاً. ولكن الأهمية النسبية لأي من المعدلين تعتمد على البيئة العملية. ففي الممارسات التجارية مثلاً، من الأفضل زيادة معدل الردود السلبية الكاذبة بدلاً من زيادة معدل الردود الإيجابية الكاذبة.

4.4.8 توفير تشكيل سهل ومرن لعملية الترشيح

في مواجهة تعدد الرسائل الاقتحامية وتنوعها، ينبغي توفير تشكيل ترشيح سهل ومرن، من قبيل السطوح البينية الميسورة وطرائق التشكيل الانتقائية وغير ذلك. وبالإضافة إلى ذلك، يمكن تصنيف قواعد الترشيح العامة بتقسيمها إلى فئات ترشيح مختلفة توضع في قواعد البيانات أو ملفات الإيداع. وعند الضرورة، يمكن انتقاء هذه الفئات من الترشيح واستعمالها بسهولة.

5.4.8 تخفيض تكاليف الترشيح إلى أدنى حد ممكن

من الأفضل ترشيح الرسائل الاقتحامية في أول فرصة ممكنة، وليس بعد أن يحتل قدراً كبيراً من الموارد. ولذلك ينبغي ترشيح الرسائل الاقتحامية عند بداية الإرسال وينبغي ألا يُترَك لتجهيزات الخدمة اللاحقة.

6.4.8 دعم القوائم السوداء والقوائم البيضاء

هنالك نمطان من الترشيح القائم على أساس العنوان: قوائم بيضاء بأسماء المرسلين المقبولين وقوائم سوداء بأسماء المقتحمين المشتبه بهم.

وتعتمد القوائم السوداء على إدراج أسماء مصادر الرسائل الاقتحامية. وقد تشتمل هذه القائمة على أسماء الأجهزة وعناوين بروتوكول الإنترنت وعناوين MAC أو غيرها من أنواع العناوين الإلكترونية. وبإمكان نظام الترشيح ترشيح الرسائل أو منع الاتصالات وذلك تبعاً للقوائم السوداء.

وتقوم القوائم البيضاء على إدراج أسماء المصادر المقبولة. وآلية العمل مماثلة لآلية القوائم السوداء سوى أن القوائم البيضاء عبارة عن قائمة بالعناوين المقبولة.

وفي واقع الحال، يعتبر نهج القوائم البيضاء/القوائم السوداء نهجاً بدائياً جداً إلى حد كبير بحيث لا يكون مقبولاً لدى غالبية المستعملين. ومع ذلك، فإن هذه النُّهج بسيطة جداً ولا تتطلب الكثير من الموارد. وزيادة في كفاءة عملية الترشيح، ينبغي أن تدعم المرشحات القوائم السوداء والقوائم البيضاء، ولا سيما القوائم السوداء من أجل مكافحة الرسائل الاقتحامية.

7.4.8 دعم ترشيح الرسائل متعددة الأساليب

بالنسبة للرسائل متعددة الأساليب، فإن المطلوب:

- دعم إمكانية منع بعض الرسائل متعددة الأساليب منعاً تاماً.
- دعم إمكانية إزالة بعض مرفقات الرسائل متعددة الأساليب أو إزالة جزء من المحتوى متعدد الأساليب داخل رسالة متعددة الوسائط.
- دعم إمكانية ترشيح الرسائل متعددة الأساليب الواردة (المتلقاة) و/أو الصادرة (المرسَلة).

5.8 استراتيجيات المعلومات الرجعية

المستعملون النهائيون هم الذين يستقبلون الرسائل الاقتحامية في نهاية المطاف، وهم الضحايا المحتملين للفيروسات أو عمليات الاحتيال. ولذلك، فإن مشاركة المستعملين النهائيين مفيدة في مكافحة الرسائل الاقتحامية مكافحة تتسم بالفعالية والكفاءة. ولذلك ينبغي أن تؤخذ المعلومات المرتجعة من المستعملين النهائيين في الحسبان عند وضع حلول مكافحة الرسائل الاقتحامية. بيد أن مشاركة المستعملين النهائيين في آلية المعلومات الرجعية يجب أن تكون على أساس طوعي.

1.5.8 توفير منصة للمعلومات الرجعية بشأن الرسائل الاقتحامية

ينبغي توفير إمكانية الشكوى للأفراد الذين يتأثرون بالرسائل الاقتحامية الضارة. كما يتعيَّن حماية حقوق الأشخاص الفعليين الذين يتلقون هذه الرسائل وذلك بواسطة التشريعات الملائمة. ولذا يحتاج الأمر إلى إتاحة سبل التظلم. ويتعيَّن إقامة آليات دعماً لهذا الهدف، بما في ذلك سبل التبليغ عن مخالفات الاقتحام إلى سلطة ملائمة. وينبغي أن تكون إجراءات تناول هذه المعلومات شفافة تتسم بالكفاءة والفعالية. ومن الممكن لمنصة معلومات رجعية أن تقوم بمثل هذا الدور.

2.5.8 توفير أنساق معيارية لتبادل المعلومات الرجعية

من الضروري لمنصة المعلومات الرجعية أن تعتمد نسق تسجيل معياري لتسجيل هذه المعلومات. وبالتالي، يمكن لمختلف المشغِّلين والكيانات تبادل المعلومات الرجعية. وانطلاقاً من هذه المعلومات الرجعية المتبادلة، يمكن الحصول على العناوين الرئيسية للمقتحمين، والتي يمكن إدراجها في القوائم السوداء.

9 تقييم النظام

ينبغي من أجل تقييم كفاءة وفعالية التكنولوجيات والأنظمة إزاء مكافحة الرسائل الاقتحامية أن تؤخذ الجوانب التالية بعين الاعتبار:

- معدل الردود الإيجابية الكاذبة.
- معدل الردود السلبية الكاذبة.
- التكاليف: ينبغي لطرائق مكافحة الرسائل الاقتحامية أن تكون مرنة لتوفير حلول تلائم كل الأحوال. ونظراً لكبر عدد التوليفات الممكنة من الاستراتيجيات، من المستصوب توفر عدد من النماذج التي تغطي طائفة واسعة من الخدمات.
- إمكانية التشغيل البيني للأنظمة الحالية: إن الشرط المسبق لمكافحة الرسائل الاقتحامية هو ضمان عمليات التشغيل الاعتيادي للأنظمة الحالية. بعبارة أخرى، لا يمكننا تعطيل الأنظمة الحالية بتنفيذ حلول لمكافحة الرسائل الاقتحامية.
- الاتفاق مع المعايير الدولية: من المفضل أن تقوم الحلول التقنية على أساس معايير دولية وذلك لتحقيق إمكانية التوصيل البيني والتوسع عالمياً. وعلاوة على ذلك، فإن عملية التقييس من شأنها تيسير إعادة استعمال الحلول والمكونات. ومن شأن ذلك أن يساعد في مجال الأخذ بحلول وتقنيات مكافحة الرسائل الاقتحامية الجديدة على وجه السرعة وبتكلفة منخفضة.

والجوانب المدرجة أعلاه عبارة عن معايير عامة لتقييم تدابير مكافحة الرسائل الاقتحامية. يحتاج الأمر، في شبكة الخدمة العملية، إلى النظر في جوانب محددة أخرى.

ثبت المراجع

[b-ITU-T Q.1742.3] Recommendation ITU-T Q.1742.3 (2004), *IMT-2000 references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network*.

[b-ITU-T Q-Sup.49] Recommendation ITU-T Q-series Recommendations – Supplement 49 (2004), *Technical Report TRQ.2840: Signalling requirements to support IP telephony*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*. <http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication*. <http://www.ietf.org/rfc/rfc2554.txt>

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*. <http://www.ietf.org/rfc/rfc2635.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*. <http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*. <http://www.ietf.org/rfc/rfc3685.txt>

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، 2009