الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1240

(2008/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

أمن الاتصالات

التكنولوجيات الضالعة في مكافحة البريد الإلكتروني الاقتحامي

التوصيـــة ITU-T X.1240

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.1240

التكنولوجيات الضالعة في مكافحة البريد الإلكتروني الاقتحامي

ملخص

تحدد التوصية ITU-T X.1240 المفاهيم والخصائص والآثار الأساسية للبريد الإلكتروني الاقتحامي كما تحدد التكنولوجيات الضالعة في مكافحة البريد الإلكتروني الاقتحامي. وهي تعرض أيضاً الحلول التقنية الراهنة والأنشطة المرتبطة بها المتوفرة من مختلف منظمات وضع المعايير والمنظمات ذات الصلة لمكافحة البريد الإلكتروني الاقتحامي. وهي توفر مبادئ توجيهية ومعلومات إلى المستعملين الذين يعتزمون تطوير حلول تقنية لمكافحة البريد الإلكتروني الاقتحامي. وسوف تستخدم هذه التوصية كأساس للمضي في وضع توصيات تقنية بشأن مكافحة البريد الإلكتروني الاقتحامي.

المصدر

وافقت لجنة الدراسات 17 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 18 أبريل 2008 على التوصية ITU-T X.1240 بموجب الإجراء الذي ينص عليه القرار 1 للجمعية العالمية لتقييس الاتصالات.

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/.

المحتـــويات

الصفحة

مقدمـــة

تم الاضطلاع بعمل التقييس، عملاً بالقرار 52 الصادر عن الجمعية العالمية لتقييس الاتصالات (WTSA) لعام 2004 وعنوانه "مكافحة الرسائل الاقتحامية بالوسائل التقنية"، بهدف إعداد توصيات تساعد على مكافحة الرسائل الاقتحامية بالوسائل التقنية. وهذه التوصية واحدة في سلسلة من التوصيات الصادرة عن قطاع تقييس الاتصالات الخاصة بمكافحة البريد الإلكتروني الاقتحامي التي تضم مبادئ توجيهية ومتطلبات وإطاراً تقنياً واستراتيجيات تقنية. وسيتم إعداد توصيات أخرى بشأن مكافحة الرسائل الاقتحامية تتعلق بتطبيقات بروتوكول الإنترنت متعدد الوسائط، مثل المهاتفة باستعمال بروتوكول الإنترنت والمراسلة اللحظية والاتصالات المؤتمرية، في وثائق منفصلة.

التكنولوجيات الضالعة في مكافحة البريد الإلكتروني الاقتحامي

1 مجال التطبيق

تحدد هذه التوصية التقنيات المستخدمة في مكافحة البريد الإلكتروني الاقتحامي. فهي تعرض الحلول التقنية الراهنة والأنشطة المرتبطة بها والمتوفرة من مختلف منظمات وضع المعايير والمنظمات ذات الصلة لمكافحة البريد الإلكتروني الاقتحامي. والغرض من هذه التوصية توفير معلومات مفيدة للمستعملين الذين يعتزمون تطوير حلول تقنية لمكافحة البريد الإلكتروني الاقتحامي. وسوف تُستخدم هذه التوصية كأساس للمضي في وضع توصيات تقنية بشأن مكافحة البريد الإلكتروني الاقتحامي.

ملاحظة – لا يشير استعمال مصطلح "هوية" في هذه التوصية إلى المعنى المطلق للمصطلح. وهو لا يشكل تحديداً أي إشارة إيجابية.

2 المراجع

لا يوجد.

3 التعاريف

تعرف هذه التوصية المصطلحات التالية:

1.3 المنتحل (phisher): كيان أو شخص يشن هجمات انتحالية.

2.3 الانتحال (phishing): تستعمل هجمات الانتحال كلاً من وسائل التحايل على الناس والخدع التقنية من أجل سرقة معلومات الهوية الشخصية للفرد ومفاتيح حساباته المالية. وتستخدم خطط التحايل الرسائل الإلكترونية المضللة لاستدراج الفرد إلى مواقع مزيفة على الويب مصممة من أجل التغرير بالناس وجعلهم يكشفون عن بيانات مالية مثل أرقام بطاقات الائتمان وأسماء أصحاب الحسابات وكلمات السر وأرقام الضمان الاجتماعي. وغالباً ما ينجح المنتحلون، باختلاس الأسماء التجارية للمصارف وأصحاب تجارة التجزئة الإلكترونية وشركات بطاقات الائتمان، في إقناع مستلمي الرسائل الاقتحامية بالاستجابة. وفي الخدع التقنية تُزرع برمجيات الإجرام في الحواسيب الشخصية لاختلاس بيانات الائتمان مباشرة، وغالباً ما يكون ذلك باستخدام برمجية تجسس على غرار "حصان طروادة" لتعقب لمسات لوحة المفاتيح.

3.3 الاقتحام (spam): يتوقف معنى كلمة "اقتحام" على النظرة المحلية للخصوصية وعلى ما يمثله الاقتحام من المنظور الوطني التقني والاقتصادي والاجتماعي والعملي. ويتطور معنى الكلمة ويتسع خصوصاً مع تطور أنواع التكنولوجيا وتوفيرها فرصاً جديدة لإساءة استخدام الاتصالات الإلكترونية. وعلى الرغم من عدم وجود أي تعريف متفق عليه عالمياً للاقتحام، يُستعمل هذا المصطلح عموماً لوصف الرسائل الإلكترونية غير المطلوبة التي ترسَل بالجملة عبر البريد الإلكتروني أو بواسطة خدمة المراسلة المتنقلة لأغراض الترويج التجاري لمنتوجات أو خدمات ما.

4.3 المقتحم (spammer): كيان أو شخص يُعدّ رسائل اقتحامية ويرسلها.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

API السطح البيني لبرمجة التطبيق *(Application Programming Interface)*

DKIM البريد المعرف بمفاتيح الميادين *(DomainKeys Identified Mail)*

CSV إثبات صلاحية مخدم معتمد *(Certified Server Validation)*

DNS نظام أسماء الميادين *(Domain Name System)*

DSN تبليغ عن حالة التسليم *(Delivery Status Notification)*

HTML لغة وسم النصوص الفائقة *(HyperText Markup Language)*

IM مراسلة لحظية *(Instant Messaging)*

ISP مورد خدمة الإنترنت *(Internet Service Provider)*

META تعزيز الرسائل للحصول على ترخيص الإرسال *(Message Enhancements for Transmission Authorization)*

MMS خدمة الرسائل متعددة الوسائط *(Multimedia Message Service)*

MTA وكيل نقل البريد *(Mail Transfer Agent)*

OECD *منظمة التعاون والتنمية في الميدان الاقتصادي (Organization for Economic Co-Operation and Development)*

OPES خدمات الحافة القابلة للتوصيل المفتوحة *(Open Pluggable Edge Services)*

PGP مستوى خصوصية لا بأس به *(Pretty Good Privacy)*

PTR سجل المؤشر *(Pointer Record)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SMTP بروتوكول نقل البريد بأسلوب بسيط *(Simple Mail Transfer Protocol)*

SPF إطار سياسة المرسل *(Sender Policy Framework)*

TEOS معيار مفتوح للبريد الإلكتروني الموثوق *(Trusted Email Open Standard)*

5 الاصطلاحات

لا يوجد.

6 مدخل إلى مكافحة البريد الإلكتروني الاقتحامي

1.6 مفهوم الاقتحام وخصائصه

على الرغم من عدم وجود تعريف للاقتحام متفق عليه عالمياً، فإن هذه الكلمة تُستخدم عموماً لوصف الرسائل الإلكترونية غير المطلوبة عبر البريد الإلكتروني أو في المراسلات المتنقلة (SMS أو MMS) وخدمات المراسلة اللحظية وذلك عادة بهدف الترويج لمنتجات أو خدمات تجارية.

ومع أن الشكل المعروف والأكثر انتشاراً للاقتحام هو البريد الإلكتروني الاقتحامي، فإن المصطلح يُستخدم ليشمل انتهاكات مماثلة في وسائط أخرى مثل اقتحام المراسلة في الهاتف المتنقل واقتحام المهاتفة القائمة على بروتوكول الإنترنت واقتحام المراسلة اللحظية واقتحام حلقات المناقشة في الشبكة واقتحام محرك البحث في الويب واقتحام مدونات اليوميات في الشبكة. ويتراوح محتوى الرسائل الاقتحامية بين الإعلانات عن السلع والمواد الإباحية المستنكرة. وللرسائل الاقتحامية عبر البريد الإلكتروني آثار ضارة شتى على مستخدمي خدمة البريد الإلكتروني وموردي خدمة الإنترنت منها:

- اضطرار مستلمي الرسائل الاقتحامية ومزودي خدمة الإنترنت إلى هدر الكثير من الوقت والجهد والمال في التعرف على هذه الرسائل وغربلتها والتخلص منها.
- احتمال احتواء البريد الإلكتروني الاقتحامي على مواد مضللة خادعة أو على مواد إباحية مؤذية للصغار.
- معاناة مستعملي خدمات البريد الإلكتروني وموردي خدمة الإنترنت من هدر موارد الشبكات وحيّز التخزين.
- تعريض أمن الشبكة للخطر من جراء انتشار الفيروسات وبرمجيات التجسس.
- ضياع الرسائل الإلكترونية العادية والهامة في خضم الرسائل الاقتحامية.

وهناك ظاهرة جديدة ومتنامية تتمثل في استعمال الاقتحام لدعم الأنشطة الاحتيالية والإجرامية، بما فيها محاولات الاستيلاء على المعلومات المالية (مثل أرقام الحسابات وكلمات السر) من خلال تزوير الرسائل لتظهر وكأنها صادرة عن شركات موثوقة ("اختلاس الاسم التجاري" أو "الانتحال"). ويُستعمل الاقتحام أيضاً كوسيلة لنشر الفيروسات والديدان.

وتستخدم هجمات الانتحال وسائل التحايل على الناس والخدع التقنية في سرقة معلومات الهوية الشخصية للمستهلكين ومفاتيح الحسابات المالية. وتستعمل خطط التحايل الرسائل الإلكترونية 'المضللة' لاستدراج المستهلكين إلى مواقع مزيفة على الويب مصممة خصيصاً من أجل التغرير بالناس وجعلهم يكشفون عن بيانات مالية مثل أرقام بطاقات الائتمان وأسماء أصحاب الحسابات وكلمات السر وأرقام الضمان الاجتماعي. وغالباً ما ينجح المنتحلون، باختلاس الأسماء التجارية للمصارف وأصحاب تجارة التجزئة الإلكترونية وشركات بطاقات الائتمان، في إقناع مستلمي الرسائل الاقتحامية بالاستجابة. وفي الخدع التقنية تُزرع برمجيات الإجرام في الحواسيب الشخصية لاختلاس بيانات الائتمان مباشرة، وغالباً ما يكون ذلك باستخدام برمجية تجسس على غرار "حصان طروادة" لتعقب لمسات المفاتيح. وتعمد برمجيات الاختلاس الإجرامية إلى تضليل الفرد وتوجيهه إلى مواقع مزيفة أو مخدّمات بالوكالة، عموماً من خلال اختطاف نظام أسماء الميادين (DNS) أو التغرير به (تسميمه).

وقد أظهر المقتحمون أنهم على درجة عالية من الابتكار من أجل تفادي كشفهم بوسائل منها تزوير مصدر البريد الإلكتروني وخلط المحتوى عشوائياً كي يفلت من مراشيح الاقتحام. وقد تعاظم حجم المشكلة إلى درجة دعت إلى استعجال سن قوانين مكافحة الاقتحام في عدد من البلدان مع اختلاف الوسائل والحلول على الصعيد الوطني. وفي الوقت ذاته، يتعاظم الإقرار بأن مكافحة الرسائل الاقتحامية مسألة تتطلب تنسيقاً وتعاوناً دوليين.

2.6 طرق مكافحة البريد الإلكتروني الاقتحامي

نظراً للضرر الكبير الذي يلحقه البريد الإلكتروني الاقتحامي بمستعملي خدمة البريد الإلكتروني وبموردي خدمة الإنترنت وبمشغلي الشبكات، فقد تم تطوير التقنيات واعتماد التشريعات في العديد من البلدان من أجل المساعدة على مكافحة البريد الاقتحامي. غير أن من الصعب مكافحة البريد الاقتحامي مكافحة فعالة من خلال تدبير معين واحد مثل استعمال الترشيح أو إنزال عقوبة قانونية إذ إن مكافحة البريد الاقتحامي ليست مسألة بسيطة. ولهذا السبب، ينبغي من أجل مكافحة البريد الاقتحامي على نحو فعال استخدام عدة طرق مختلفة متزامنة:

- التشريع: ينبغي اعتماد تشريعات لمكافحة البريد الاقتحامي بهدف تسهيل الرد الملائم لمستعملي الخدمة على البريد الإلكتروني الاقتحامي وزيادة فعالية تقنيات مكافحة الاقتحام كالترشيح مثلاً. إضافة إلى ذلك، بإمكان التشريعات أن تساعد على حماية مستعملي الخدمة وموردي خدمة الإنترنت من البريد الاقتحامي غير القانوني.
- التقانات: تطوير تقانات مكافحة البريد الاقتحامي أمر أساسي من أجل مكافحة هذا الكم الهائل من البريد الإلكتروني الاقتحامي مكافحة فعالة. ومن الضروري تطوير أنواع مختلفة من التقنيات من أجل منع إرسال البريد الاقتحامي وللتعرف على هذا البريد وترشيحه على نحو فعال.
- الإجراءات الصناعية: يُستحسن أن يعمد المشاركون في مجال الصناعة، مثل موردي خدمة الإنترنت ومشغلي الشبكات، إلى تطوير وتركيب أشكال مختلفة لتقنيات مكافحة البريد الاقتحامي بما في ذلك وظائف القوائم السود أو القوائم البيض والترشيح. وبإمكان موردي خدمة الإنترنت أيضاً اعتماد سياسات لمكافحة البريد الإلكتروني الاقتحامي.
- التعاون الدولي: التعاون الدولي ضروري لأن شبكات الاتصالات لا تعرف الحدود ولأن توليد البريد الاقتحامي وأثره لا يقتصران على أي بلد. كما أن التعاون الدولي مفيد في مجال تبادل المعلومات عن اعتماد التشريعات الفعالة وتطوير تقنيات مكافحة البريد الاقتحامي وتوعية مستعملي الخدمة وموردييها.
- التوعية: توعية مستعملي الخدمة وموردي خدمة الإنترنت مسألة هامة من أجل التقليل من الضرر الناجم عن البريد الإلكتروني الاقتحامي إلى أبعد حد ممكن. ومن شأن توعية مستعملي البريد الإلكتروني أن يساعدهم على اتخاذ

الإجراءات المناسبة لمكافحة البريد الإلكتروني الاقتحامي وأن يساعد موردي خدمة الإنترنت على اعتماد سياسات مكافحة البريد الاقتحامي وتقنياتها.

ومن بين التدابير المختلفة المذكورة أعلاه لمكافحة البريد الاقتحامي، تركز هذه التوصية على الوسائل التقنية لمكافحة الاقتحام مثل تطوير تقنيات مكافحة الرسائل الاقتحامية وتطبيقاتها.

7 تقانات مكافحة الاقتحام

يقدم تقرير فريق مهام منظمة التعاون والتنمية في الميدان الاقتصادي بشأن الرسائل الاقتحامية [b-OECD TF] العديد من العناصر لمكافحة البريد الإلكتروني الاقتحامي ومنها النُهج التنظيمية وجوانب الإنفاذ والحلول التقنية. وتشير هذه التوصية في هذه الفقرة إلى جزء من التقرير هو (العنصر IV – تقانات مكافحة الرسائل الاقتحامية). ولا بد من الإشارة في هذا الصدد إلى أن مجموعة أدوات مكافحة الرسائل الاقتحامية صدرت في مايو 2006 و لم تُحدَّث منذ ذلك الحين.

وتشمل هذه الفقرة مناقشة مختلف تقانات مكافحة الرسائل الاقتحامية وقدراتها المتاحة حالياً، فضلاً عن الطرائق التي يجب استخدامها عند استلام رسائل اقتحامية. وتحتاج أي محاولة لمكافحة الرسائل الاقتحامية بفعالية إلى مراعاة الإدارة الواعية لعدد من هذه التقانات بانسجام. ولا توجد طريقة تضمن النجاح الكامل بمعزل عن الطرائق الأخرى. وعند استعمال عدد من تقانات مكافحة الرسائل الاقتحامية بتعاون فعال فيما بينها، فإن نتاج ذلك يمكن أن يتمثل في خفض كبير في مستوى تأثير الرسائل الاقتحامية على النظام.

1.7 لمحة عامة

تنطوي عملية الاقتحام على تحديات تقنية معقدة، ولذا فإن الحلول من أجل التخلص منها ينبغي أن تقوم على تدابير تقنية ملائمة. وإذا كانت إجراءات الحكومات وتشريعاتها مفيدة فإنها لا تكفي للتصدي للتحديات التي يفرضها الاقتحام. فالاقتحام في واقع الأمر مشكلة تقنية ناجمة أساساً عن خلل في البروتوكول SMTP (بروتوكول نقل البريد بأسلوب بسيط). والطبيعة التقنية للمشكلة تجعل مسألة التعرف على المقتحمين وبالتالي معاقبتهم مسألة بالغة الصعوبة بالنسبة للجهات القائمة على الإنفاذ.

وعلى الرغم من اختلاف تعاريف الرسائل الاقتحامية، فإن هناك تقانات وتقنيات يمكن استخدامها على حد سواء في المساعدة على الحد من مشكلة الرسائل الإلكترونية غير المطلوبة. والغرض من هذا القسم تقديم نظرة عامة محايدة لمختلف أنماط الأدوات والوسائل التكنولوجية فضلاً عن العوامل التي ينبغي مراعاتها قبل تطبيقها. ويتناول هذا الجزء الأدوات على وجه الخصوص أكثر مما يتناول الحلول. وإذا كانت التكنولوجيا قد صُممت لمعالجة الكثير من المشاكل التي يسببها البريد الاقتحامي وأنها قد تستطيع حقاً "حل" بعض المسائل المحددة المتعلقة بالبريد الاقتحامي، فإن الحل الشامل لهذا البريد لا يمكن تحقيقه إلا من خلال نهج متعدد الجوانب يضم التكنولوجيا والسياسات (بما فيها التشريعات حسب الاقتضاء) والممارسات والتوعية.

وتعمل أدوات مكافحة الاقتحام على مستويات عديدة، في نقطة المنشأ وفي الشبكة الأساسية وفي البوابة وفي حاسوب المتلقي، ويمكن استخدامها متفرقة أو مجتمعة. وأحدث المعلومات والموارد متاحة في موقع مجموعة الأدوات على شبكة الويب على العنوان www.oecd-antispam.org.

ويتوجه هذا القسم تحديداً إلى القائمين على إدارة مخدم البريد لتزويدهم بنظرة ثاقبة إلى نقاط القوة والضعف في كل تقنية ترشيح وتمكينهم من اختيار البرمجيات وفقاً للسياسة المتبعة في بريدهم الإلكتروني واحتياجاتهم وذلك تبعاً لمعمارية كل مخدّم. ويركز القسم على الممارسات في البريد الوارد، مع أن الممارسات الهادفة إلى تقليص الرسائل الاقتحامية الصادرة مفيدة أيضاً. وعلاوة على مشغلي مخدمات الاستقبال، فإن مشغلي مخدمات الإرسال لهم دورهم أيضاً: إذ بمقدورهم تطبيق تقنية الحد من معدل البريد الصادر وإغلاق المنفذ 25 واتباع تدابير أخرى من أجل الحد من كمية الرسائل الاقتحامية التي ترسَل من مخدماتهم.

ويتعيّن على الأدوات التي تعالج الرسائل الاقتحامية التركيز على البريد وعلى السلوك المحيط بالبريد على حد سواء. وفي ضوء هذه العوامل المتعددة تستند أجهزة وطرائق عديدة إلى مجموعات من القواعد أو الافتراضات التي تعمل متفرقة أو مجتمعة من أجل التعرف على الرسائل الإلكترونية المشبوهة. وقد تكاثرت الرسائل الاقتحامية مع الزمن لتضم مزيداً من الفيروسات والبرمجيات الضارة، مما يستدعي اعتماد تكنولوجيا دفاعية تتجاوز الأدوات القائمة على النصوص إلى الأدوات التي تحلل العوامل السلوكية والسياقية من أجل تحديد قبول رسالة ما أو رفضها أو حتى محاولات التوصيل. ونظراً للتهديد المتزايد للأمن الذي تنطوي عليه الرسائل الاقتحامية، فإننا نتوقع أن تحتوي تكنولوجيات مكافحة الاقتحام على مزيد من التقنيات المتطورة للأمن والاستيقان أو أن تحتاج إلى أن تعمل بالترافق معها.

2.7 أهمية سياق الأداة/التكنولوجيا

بعض الأدوات/التكنولوجيات المذكورة في هذا القسم مصممة خصيصاً للتطبيق عند المدخل إلى منصة البريد الإلكتروني بينما يكون تطبيق البعض الآخر منها أكثر فائدة بعد استقبال الرسائل ولكن قبل تسليمها إلى المستعمل النهائي. وجدير بالذكر أن بعض الأدوات يكمن أيضاً في حاسوب المتلقي. وفي كل مرحلة من مراحل الترشيح قد يكون الغرض من تطبيق قاعدة ما رفض الرسالة الإلكترونية أو مجرد وضع علامة عليها أو وضعها في صندوق المستعمل النهائي المخصص للرسائل الاقتحامية.

ولا يمكن بالتالي الحكم على أهمية أي قاعدة وفائدتها إلا في السياق الدقيق الذي تطبق فيه والمستوى الذي تنفذ عنده في عملية توزيع الرسائل وما تؤول إليه الرسالة في نهاية الأمر.

3.7 الجمع بين الاختبارات

ينبغي أن تشكل التكنولوجيا العمود الفقري لأي نهج يهدف إلى مكافحة الرسائل الاقتحامية. وينبغي أن ندرك أن أياً من التكنولوجيات المذكورة لاحقاً لن يكون بمثابة "حل سحري" أو الحل الوحيد الناجع للمشاكل التي تسببها الرسائل الاقتحامية. وفي الواقع، كل هذه التكنولوجيات متكاملة تبلغ ذروة فعاليتها عندما تُنفَّذ معاً. فالجمع بين عدد من التقنيات ضروري من أجل التخفيف من الأثر الضار للرسائل الاقتحامية على النظام.

ولا ينبغي أن تُستخدم الاختبارات بالضرورة بأسلوب "كل شيء أو لا شيء" بل، على العكس من ذلك، من الأفضل تجميع الاختبارات من أجل اعتراض أكبر عدد ممكن من الرسائل الاقتحامية وفي الوقت ذاته تقليل عدد الرسائل المشروعة المعترَضة أو المرفوضة عن غير قصد.

- رفض كل شيء أو لا شيء – هذا أحد الإجراءات الممكنة التي تعتمدها المخدمات التي تستعمل القائمة السوداء. حيث ترفض كل رسالة ترسب في الاختبار. غير أن حدوث الخطأ يتوقف على موقع القاعدة في عملية التوزيع.
- امتياز النفاذ – هذا أحد الإجراءات الممكنة التي تعتمدها المخدمات التي تستعمل القائمة البيضاء، حيث تُقبل كل رسالة تنجح في الاختبار. ولا يخشى أن تُرفض أي رسالة مشروعة لكن قد تكون هناك "سلبيات كاذبة". فعلى سبيل المثال ليس لقائمة بيضاء لأسماء ميادين قيمة حقيقية إذا لم يتم استيقان اسم ميدان المرسل (في إطار سياسات المرسِلين أو البريد المعرَّف بمفاتيح الميادين (DKIM)).
- تدّعي رسائل اقتحامية أو ديدان عديدة أنها صادرة باسم مؤسسات تجارية معروفة بغية الحصول على امتياز النفاذ.
- أسلوب العلامات – كيفية تجميع البرامج لاختباراتها. ويُنصح جداً باستعمال أسلوب العلامات لأنه يتجنب مساوئ أسلوب "كل شيء أو لا شيء" غير أنه باهظ التكاليف من حيث موارد الآلات وضرورة التحديث المستمر لعوامل تحديد العلامات من أجل زيادة نتائج الفرز إلى أبعد حد وفي الوقت ذاته تخفيض عدد "الإيجابيات الكاذبة" إلى أبعد حد.

والطريقة التقليدية هي إجراء عدة اختبارات "كل شيء أو لا شيء" ثم إعطاء علامات للرسائل التي يتم قبولها.

4.7 أنواع تقنيات مكافحة الاقتحام

1.4.7 استيقان البريد الإلكتروني

تقع طرائق استيقان البريد الإلكتروني في فئة القواعد التي تساعد على مكافحة الرسائل الاقتحامية دون أن تشكل بحد ذاتها تقنيات لمكافحة الرسائل الاقتحامية.

ويمكن توضيح ذلك بالتشبيه. فبطاقات الهوية ليست دليل ثقة لأن للمقتحمين أيضاً بطاقات هوية. لكن اشتراط الشفافية يعود بفائدة أكبر على المرسلين المشروعين منه على المقتحمين.

2.4.7 إطار سياسة المرسل (SPF) و/أو معرف هوية المرسل

من أسباب القوة الرئيسية التي تكمن وراء انتشار الرسائل الاقتحامية قدرة المقتحمين على إخفاء عنوان المرسِل الحقيقي للرسالة. ومعمارية البريد الإلكتروني لا تنطوي على افتراض اتصال مسبق بين المرسِل والمتلقي. وبالتالي، لا يمكن الاعتماد على الاستيقان المنهجي. وتثير المشكلة قلقاً متزايداً لأن العناوين المزيفة قد استُعملت في عمليات انتحال خادعة تستدرج متلقي الرسائل إلى الكشف عن أرقام بطاقات ائتمانهم وعن معلومات شخصية أخرى.

وما زال تطبيق هذه التكنولوجيا في بداياته ولذلك فإنه يفتقر إلى التقييس، لكن الاستيقان ممكن من خلال "تعليم" الرسائل الإلكترونية التي لا يمكن التحقق من مرسليها الحقيقيين. وبإمكان المخدم المستقبل أن يختار منع الرسائل غير المستيقنة لكن التكنولوجيا لا تلزمه بفعل ذلك. فهي تكتفي بتعليم الرسالة. والميزة الأساسية للاستيقان على مستوى الميدان هي أنه يخفض كثيراً من عدد "الإيجابيات الكاذبة" ويسمح بمزيد من الترشيح الموثوق القائم على السمعة. ويعوض ازدياد التكاليف بالنسبة للمرسلين ضمان تسليم الرسائل، بعد الاستيقان من مرسليها ومن استخدامهم للنظام بصورة مشروعة، أو احتمال التعرض لطائلة الملاحقة القانونية لإساءة استعمال العلامة التجارية. وتتغير خصائص عملية التحقق باختلاف النموذج المستعمل، وهناك حالياً عدة نماذج لاستيقان المخدمات، ومنها النموذجان الأكثر انتشاراً وهما إطار سياسة المرسل (SPF) ومعرف هوية المرسل.

وبالإمكان مناقشة هاتين التقنيتين معاً لأنهما تشتركان بعدة خصائص. أما مسألة الاختيار بينهما فهي ليست على نفس القدر من البساطة.

ويمكن استخدام التقنيتين SPF ومعرف هوية المرسل لاختبار ما إذا كان مخدم البريد الإلكتروني مخوَّلاً بإرسال بريد إلكتروني باسم ميدان معين. ويتم ذلك بنشر سجل في نظام أسماء الميادين (DNS) يعدد مخدمات البريد الإلكتروني المعتمدة لميدان ما. وتختلف التقنيتان مبدئياً في اختيار الهوية المختبرة. ففي التقنية SPF يختبر البند MAIL FROM في الغلاف [b-IETF RFC 2821] وفي تقنية معرف هوية المرسل تختبر الرأسيات [b-IETF RFC 2822].

ويتبع القائمون على إدارة المخدم نمطين من الإجراءات، إذ تنشر السجلات SPF في نظام أسماء الميادين وتختبرها عند الدخول. وبحسب تقرير (B-Lyris) حديث العهد، فإن استعمال سجل SPF غير صحيح يقلل إلى حد بعيد جداً من فرص إيصال رسالة ما.

ويساعد استيقان البريد الإلكتروني من خلال التحقق من عناوين مخدم المرسل في بروتوكول الإنترنت على الحد من الرسائل الاقتحامية والتحكم فيها مستقبلاً. وقد يستدعي ذلك استحداث خدمات فوق مستوى الاستيقان مثل القوائم البيض الخاصة وخدمات السمعة وخدمات الاعتماد.

3.4.7 البريد المعرّف بمفاتيح الميادين (DKIM) و/أو تعزيز الرسائل للحصول على ترخيص الإرسال (META)

يُستخدم أسلوب البريد DKIM وأسلوب تعزيز الرسائل META في استيقان ميدان المرسل بواسطة توقيع التجفير الذي يضيفه مخدم البريد الإلكتروني أوتوماتياً. ويساعد استيقان البريد من خلال مهر الرسالة بتوقيع مجفّر على الحد من الاقتحام والتحكم فيه مستقبلاً.

والأسلوب DKIM هو أكثر نماذج الاستيقان شهرة. وهو يعمل على أساس طلب توقيع رقمي، أو مفتاح خصوصي، على جميع الرسائل الصادرة. ويتم استيقان الرسائل الواردة على مستوى الميدان ومستوى مخدم البريد بالتأكد من التطابق بين الخصوصي والمفتاح العمومي الموجود على الملف. وتضمن هذه الطريقة أن الرسالة لا يمكن أن تأتي إلاَّ من مورد خدمة الإنترنت المصدر. ويفيد الأسلوب DKIM ميدان المرسل بضمان التسليم إلى موردي خدمة الإنترنت الذين يستخدمون خوارزمية DKIM. وقد حصل الأسلوب DKIM مؤخراً على اعتماد فريق مهام هندسة الإنترنت (IETF) له كمعيار RFC مما يجعله معيار فريق مهام هندسة الإنترنت.

5.7 وجود ميدان المرسل والتماس استجابة ما

يرسل كثير من المقتحمين بريداً بعنوان مرسل لا وجود له. ويمكن استعمال قاعدة لرفض هذه الرسائل، كإعطاء التوجيه reject_unknown_sender_domain في Postfix أو التوجيه j-chkmail في BadMX. وهناك طريقة أخرى وهي التحقق من صلاحية السجل المتعلق بمخدّم الرسائل الواردة (MX) بشأن الميدان الوارد في الحقل "from" في الرسالة. ويضع بعض المقتحمين سجلاً MX وهمياً من أجل تجنب الإجابات الغاضبة والمحتجة (حيث يذكر مثلاً أن السجل MX يعود إلى 127.0.0.1، مما يعني المرسل المحلي).

وتتطلب هذه القواعد قدراً بسيطاً من حركة النظام DNS، التي كانت تحدث في جميع الأحوال أثناء الإجابة، وهي قادرة أيضاً على رفض كمية لا بأس بها من الرسائل الاقتحامية.

6.7 وجود سجل مؤشر (PTR)

يستخدم السجل PTR في نظام أسماء الميادين في ترجمة العناوين IP لمخدم المرسل إلى اسم، دون التحقق بالضرورة من توافق هذا الاسم مع ميدان المرسل.

ولا تخضع إضافة سجلات من هذا القبيل دائماً لمراقبة ميدان المرسل (إن لم يكن هناك تفويض من بروتوكول الإنترنت خاص بالميدان addr.arpa على سبيل المثال) الذي قد لا يستطيع الوفاء بمهمته حتى لو كانت الإضافة مشروعة. ويمكن استعمال هذه السجلات من أجل تحديد مصدر الرسالة وما إذا كان موثوقاً به وإلى أي مدى. كما يمكن استعمالها أيضاً لتحديد ما إذا كانت الرسالة صادرة من عنوان IP مقيم أو لإعادة إرسال رسالة خطأ إلى المخدم الصحيح.

7.7 القوائم السود/القوائم البيض

يمكن أن يؤدي الترشيح التقليدي وتتّبع الشكاوى لدى جماعات المستعملين في نهاية المطاف إلى وضع قوائم بيض تضم المرسلين المقبولين وقوائم سود تضم المقتحمين المشبوهين. وغالباً ما يكون نهج القوائم البيض/السود حلاً أكثر تشدداً من أن يقبل به معظم المستعملين. فوضع القوائم البيض يستغرق وقتاً طويلاً ويتطلب تحديثاً مستمراً. كما تتطلب القوائم السود مراقبة مماثلة. وتحتاج جميع القوائم إلى آليات وإجراءات لتحديثها من أجل معالجة "الإيجابيات الكاذبة" والشكوى المغرضة من قائمة ما. وبإمكان عمليات الخداع والترحيل المفتوح أن تعطي انطباعاً بأن البريد صدر من مصدر ما.

وتستند القوائم السود إلى مبدأ إدراج مصادر الرسائل الاقتحامية في قائمة. وتضم هذه القائمة أسماء آلات أو عناوين IP أو عناوين إلكترونية. ويمكن وضعها في كيان للاستعمال المشترك أو إدخالها والحفاظ عليها في مخدم يستخدمها لمتطلباته الخاصة.

ويمكن إجراء هذا الاختبار باستعمال خدمة وكلاء نقل البريد (MTA) الحالية في دورة بروتوكول SMTP وينتج عن ذلك رفض الرسالة حتى قبل إرسالها. وتضم بعض القوائم عمليات ترحيل مفتوح لا ترسل الرسائل الاقتحامية وحدها. ويمكن للمنصات التي أرسلت إليها الرسائل معالجة تشكيلة الترحيل المفتوح على أنها سلوك غير مشروع.

وتختلف نوعية القوائم السود كثيراً باختلاف الكفاءة المهنية للجهة التي تضعها. فكثير من هذه القوائم تتم إدارتها بشكل سيء أو تهمَل أو يشك بسلامتها: فالأسماء تضاف بسرعة والمعايير المطبقة قد تكون غير واضحة وشطب اسم من القائمة مستحيل عملياً أو ممكن مقابل مبلغ من المال فقط. والسبب الرئيسي لهذه المشكلة هو عدم وجود مدونة سلوك أو أي نوع من القواعد الناظمة لضبط عمل القوائم السود والحد من تطبيقها. وإذا تم اختيار استخدام هذا الحل مستقبلاً سيكون من الضروري بذل

جهود تعاونية لوضع قائمة بالممارسات الجيدة تُوضَّح فيها الحالات التي يمكن فيها إدراج العناوين في القائمة السوداء والشروط التي يمكن بموجبها سحب العناوين من هذه القائمة حسب الاقتضاء.

ولا مناص من احتواء القوائم السود على بعض الأخطاء التي تمنع بعض الرسائل المشروعة من الوصول إلى المستهلك. وقد تسببت هذه المشكلة المعروفة باسم "الإيجابية الكاذبة" في نزاعات قانونية عندما اعتقد المرسلون الشرعيون أنهم أدرجوا خطأً في قائمة سوداء لدى مورد خدمة إنترنت. إضافةً إلى ذلك، فإن مشكلة "الإيجابية الكاذبة" لفرادى المستعملين يمكن أن تؤدي إلى عيب خطير يتمثل في الاعتماد بشكل حصري على تقنيات الترشيح التقليدية لوقف البريد الاقتحامي. غير أن رسائل "الإيجابيات الكاذبة" قد تنجم عن معظم تدابير مكافحة البريد الاقتحامي. وينبغي أن يحد الاستيقان على مستوى الميدان من "الإيجابيات الكاذبة".

وعلى الرغم من أن استخدام القوائم السود يثير شواغل كثيرة، فإنها ستبقى حلاً سريعاً لرفض الاتصال مع الآلات التي يمثل سلوكها خطراً على أمن الخدمات أو نوعيتها في المنصة التي يرسل إليها البريد أو لرفض الرسائل القادمة من بعض المرسلين.

8.7 اعتبار عنوان المخدم المرسِل عنواناً "دينامياً" أو "مقيماً"

هذا شكل خاص من أشكال القائمة السوداء يكون فيه معيار الإضافة إلى القائمة هو أن يقابل العنوان IP الممنوع مع آلة مشترك ما في خدمة مورد خدمات إنترنت وليس مع مخدم بريد منظمة ما. والفكرة هي أن مشتركاً عادياً لا يرسل الرسائل مباشرة في بروتوكول SMTP، بل يمر عبر تحليل التهديد العملي (PTA) لدى مورد الخدمة الخاص به. وذلك يعني عادة أن الآلة الممنوعة ترسل مباشرة رسائل اقتحامية من المقتحم أو على الأرجح أن الرسائل ترسل دون معرفة المالك (أي أن الآلة قد عبث بها وتحولت إلى "آلة منقادة" من أجل إرسال الرسائل).

وقوائم هذه العناوين ليست موثوقة دائماً نظراً إلى أن معظمها يُجمع بأساليب "حدسية" مثل وجود "adsl" في اسم الآلة. كما تستهلك إدارة هذه القوائم قدراً كبيراً من الموارد.

وعلى العكس من ذلك، يمكن استخدام بعض هذه القوائم، سيما تلك المجمعة من قبل الذي يستعملها، من أجل التمييز بين المخدمات المرخص لها في ميدان ما وبين القوائم المقيمة في المخدم. وعلاوة على ذلك، فإن بعض الميادين تنشر مدى كل من العناوين المقيمة لديها.

ويمكن اعتبار هذا الاختبار تمييز بين "المستهلكين الصرف" و"الموردين". ويعتبر هؤلاء أن السياسة التي تمكّن مالك الميدان من رفض توصيل مخدماته مع العناوين المقيمة سياسة مشروعة نظراً لأن هذه العناوين تمثل حالياً المصدر الرئيسي للرسائل الاقتحامية. غير أن المستهلكين يقولون إن الرسائل الاقتحامية موجودة ويجب حماية حرية استعمال البريد الإلكتروني.

9.7 الترشيح

الترشيح هو التقنية الأكثر انتشاراً لمكافحة الرسائل الاقتحامية. والفوائد الرئيسية للمراشيح هي سهولة تطبيقها والمرونة المتاحة للمستعملين في تحديد الرسائل التي ينبغي اعتبارها رسائل اقتحامية. ويتطلب استخدام المراشيح على أساس الحدس أن يضع المستعملون معايير، ككلمات سر أو عناوين مرسلين تدفع المرشاح إلى منع بعض الرسائل من بلوغ علبة بريد المستعمل. أما المقتحمون الذين يكتبون كلمات بأخطاء إملائية عن عمد أو يكتبونها بلغة أخرى فإنهم يتغلبون بسهولة على نهج كلمات السر. ومراشيح "بايز" تقوم على التجربة. فهي تستحدث إحصاءات للرسائل في جدول تعرّف ليكون لاحقاً مرجعاً لمختلف المستعملين يساعدهم على التمييز بين الرسائل الاقتحامية والرسائل المشروعة. ولا يسمح المرشاح بعد ذلك بالمرور إلا للرسائل التي تشبه الرسائل المشروعة التي تلقاها المستعمل. وقد بينت دراسة أجرتها لجنة التجارة الفدرالية الأمريكية في عام 2005 [b-FTC] أن المراشيح قادرة على منع 90% من الرسائل الاقتحامية.

1.9.7 المراشيح الحدسية

تستند هذه المراشيح إلى مبدأ الاختبار لتحري بعض العناصر الموجودة نمطياً في الرسائل الاقتحامية، مثل الاستخدام الحصري للغة HTML أو مواصفات المستهلك الذي ترسل إليه الرسائل. ويجري ترجيح الاختبار من خلال عملية تعلم تقوم على

مجموعة من الرسائل الاقتحامية المعروفة ومجموعة من الرسائل المعروف أنها مشروعة (ولذلك فإن العلامات غير محسوبة من قبل الإنسان حرصاً على الحد من العامل الذاتي).

وتنطوي هذه المراشيح على محذور تصنيف الرسائل التي تستعمل تقنيات المقتحمين، مثل أسلوب الرسائل المثيرة في اللغة HTML، ضمن فئة الرسائل الاقتحامية. زيادة على ذلك، جدير بالذكر أن المراشيح تستهلك كميات كبيرة من موارد الحاسوب.

وتستطيع هذه المراشيح كشف نسبة عالية من البريد الاقتحامي ولا تحتاج إلى تعليم أو تشكيل. ولكن بما أنها تستعمل عدداً كبيراً من الاختبارات ينبغي ألاّ يغرب عن البال إمكانية تغيير الاختبارات العاملة والعلامات المستعملة لتصنيف الرسائل ضمن فئة الرسائل الاقتحامية.

2.9.7 مراشيح الكلمات الرئيسية

هي مراشيح اثنينية تبحث عن كلمة رئيسية (مثل "فياغرا" ...). ومحذور "الإيجابيات الكاذبة" عال جداً وإمكانية تجنبها، من خلال الفراغات والسمات البديلة والأخطاء الإملائية المتعمدة، عالياً جداً أيضاً.

3.9.7 مراشيح الخلاصة أو القيمة المخلوطة

تستخلص هذه المراشيح قيمة مخلوطة من الرسالة المحالة إليها وتبين ما إذا سبق تعريفها كرسالة اقتحامية. وهناك الكثير من "السلبيات الكاذبة" لأن عدداً من أنواع البريد الاقتحامي لا يمكن تعريفه حتى عندما يجري لها المخدم مسحاً بهذه المراشيح. وعلاوة على ذلك، تختلف الرسالة أحياناً إلى درجة تكفي لتوليد قيمة مخلوطة مختلفة. ومن أحد الحلول لهذه المشكلة تأخير البريد (كما في أسلوب القوائم الرمادية). فهي تولد القليل من "الإيجابيات الكاذبة".

4.9.7 مراشيح بايز

المبدأ الذي يعمل بموجبه مرشاح بايز، هو شحن جهازه أولاً بفحص مجموعة من الرسائل الاقتحامية المعروفة ومجموعة من الرسائل المشروعة المعروفة، ثم بعد أن يتعلم المرشاح المفردات التي يستخدمها المقتحمون استناداً إلى هذه القائمة المعروفة يستعمل احتمالات بايز لمعرفة ما إذا كانت رسالة ما اقتحامية أم لا. وفي حالة مرشاح مجموعة تقوم إدارة النظام عادة بإجراء عملية التعلم.

ونظراً لأن هذه المراشيح تقوم على مفهوم مفردات الرسائل الاقتحامية، فإنها قد تسبب بعض المشاكل عند استخدامها على أساس التقاسم. وقد يكون ذلك مقبولاً على صعيد بيئة صغيرة على درجة عالية من التجانس (مثل شركة أو قسم في جامعة يعمل فيه الجميع في نفس الميدان ويستعملون مفردات متشابهة). لكن ذلك قد لا يكون صحيحاً في حالة مورد بريد إلكتروني كبير وخاصة إذا كان مورداً عمومياً ما لم توفر قاعدة المجموعة لكل مستعمل إمكانية تصميم المرشاح خصيصاً لصندوق بريده. غير أن المشكلة هي أن ما يعتبره بعض المستعملين مفردات مقبولة قد يطلق عمل المرشاح إذا كانت هذه المفردات قد اعتبرتها مجموعة أخرى من المستعملين مفردات اقتحام.

وعلى الرغم من احتمال نشوء بعض المشاكل على المستوى الجماعي، فإن هذه المراشيح عالية الفعالية عندما تُستعمل فردياً وهي واحدة من الحلول القليلة القادرة، عند استعمالها بمفردها، على ترشيح جميع الرسائل الاقتحامية تقريباً إذا ما جرى تدريبها بشكل مناسب.

5.9.7 مراشيح السلوك

يفحص هذا النمط من المراشيح سلوك المخدم البعيد من حيث عدد الرسائل المرسلة في وحدة زمنية مثلاً. والحد من المعدل هو مثال على هذا النوع من الترشيح. والفكرة وراء ذلك هي أن الرسائل العادية لا ترسَل إلا إفرادياً أو بأعداد صغيرة جداً بينما ترسَل الرسائل الاقتحامية بكميات هائلة.

وهذا النوع من المراشيح حساس جداً لأنه لا يمكن عادة التمييز بين مخدم رسائل اقتحامية ومخدم قوائم توزيع مشروعة مثل حلقات المناقشة.

وبحسب بعض الخبراء يحق لمنصة حاسوبية ما مع ذلك أن ترفض كميات معينة من البريد، أولاً بحكم حجمها أو بحكم وظيفتها لضمان أمن شبكاتها. ومن المشروع أيضاً الطلب إلى مرسلي البريد بالجملة مراعاة موارد المنصات البعيدة من خلال تحمل تكاليف توزيع رسائلهم دون محاولة إرسالها بسرعة زائدة بهدف التخلص من عبء التكاليف المترتبة على استعمال البريد الإلكتروني كقناة اتصال.

10.7 إثبات صلاحية المخدم المعتمد (HELO/CSV)

يعرِّف الحاسوب المرسل نفسه بالاسم إزاء الحاسوب المستقبِل في بداية كل معاملة في إطار بروتوكول نقل البريد بأسلوب بسيط (SMTP) باستعمال الأمر "EHLO" أو الأمر "HELO" في لغة البروتوكول SMTP.

وإثبات صلاحية المخدم المعتمد (CSV) خدمة توفر للمخدم المستقبل للبريد آلية تمكنه من تقييم المخدم المرسل للبريد. وهو ينطلق من ممارسة متَّبعة لدى مزودي الخدمة تعتمد الشبكات التي توصل منها الأنظمة المرسلة للبريد.

وتتحقق اختبارات HELO من أن وكيل نقل البريد (MTA) صحيح التشكيل، لكنها لا تكشف عما إذا كان مقتحماً أم لا. أما اختبارات الصلاحية CSV، فتضيف اختبار احتمالية إلى الاسم: هل يتوافق فعلاً مع ميدان ما؟ وعلى عكس إطار سياسة المرسل (SPF) أو البريد المعرّف بمفاتيح الميادين (DKIM)، فإن الخدمة CSV لا تستيقن الميدان المرسل للرسالة بل ميدان مخدم البريد الإلكتروني (الذي قد يكون مختلفاً على سبيل المثال في حالة مورد يخدم عدداً كبيراً من العملاء).

وتختبر توجيهات التشكيل، مثل التوجيه reject_invalid_hostname في Postfix، الاسم الذي يعلن عنه المخدم. ويؤدي استعمال اختبارات HELO التقليدية إلى رفض عدد كبير جداً من الرسائل المشروعة. غير أن مواقع قليلة جداً الآن تعرف كيفية تعديل خدمة HELO لكي تعمل على ما يرام. وسيؤول ذلك على الأرجح للتغيير مستقبلاً إذ أن عدداً متزايداً من المواقع ستختبر الخدمة HELO مولدةً بذلك حافزاً لتحسينها.

11.7 الإدراج في القوائم الرمادية

ينطوي ذلك على إرسال مقصود لشفرة الخطأ SMTP 4xx (خطأ مؤقت على عكس الشفرة 5xx التي تعني خطأ نهائياً، انظر المعيار [b-IETF RFC 2821]) عند مقابلة مرسل جديد. وإذا كان هذا المرسل وكيلاً MTA عادياً فإنه سيعيد الكرة بعد ذلك (عادةً بعد 15 دقيقة) وستقبل عندئذٍ رسالته. ومعظم برمجيات البريد الاقتحامي لا تقوم بمحاولات إرسال متعددة. وهذه التقنية عالية الفعالية وتمنع جميع الرسائل الاقتحامية غير المرسلة عبر مرحل مفتوح أو وكيل MTA لمورد خدمة. وتمنع هذه التقنية استقبال بعض الرسائل من مخدمات رديئة التشكيل واستعمالها ملائم خصوصاً بالترافق مع قائمة بيضاء.

12.7 العلامات/كلمات السر

هدف هذه التقنيات هو إدراج كلمة سر ضمن العنوان الذي يرسل إليه البريد الإلكتروني أو استعمال نظام أسئلة وإجابات مثل اختبار تورينغ (Turing). ولن تعرف برمجية المقتحم كلمة السر هذه ولن تكون قادرة على النجاح في الاختبار.

ولا ينجم عن هذه التقنيات "سلبيات كاذبة" – إلاَّ إذا قرر المقتحم أن يوظف آلاف الناس بأجور زهيدة ليقوموا بالعمل.

وسيرفض عدد من المستعملين المشروعين هذا الاختبار أو لن يتمكنوا من النجاح فيه. وسينتج بالتالي الكثير من "الإيجابيات الكاذبة". ولا تناسب هذه التقنيات إلاَّ المتلقين الذين يستلمون بالفعل كميات كبيرة من البريد بالجملة، بما فيها الرسائل المشروعة، أو أي متلقي يريد أن يقلص عدد الرسائل المستقبلة، مما يقع ضمن نطاق حرية الاتصالات. وينبغي ألاّ يغرب عن البال أن كل المرسلين لن يقبلوا بالاختبار المفروض. وقد تساعد توعية المستعملين بمزايا هذه التقنية والمرور بالاختبار على تخفيف معدل عدم القبول.

13.7 تقنيات متنوعة

يغطي هذا القسم تقنيات متنوعة معظمها تجريبـــي أو لم يُختبر بدرجة كافية.

1.13.7 اختبارات الغلاف (إثبات صحة وسم عنوان العودة (BATV)، ومرسل الغلاف الموقع (SES)

هذه التقنيات عبارة عن تطورات حديثة وغير منتشرة بشكل كاف لأخذها بعين الاعتبار.

2.13.7 الإشهاد بصحة البريد بالجملة – سمعة المرسل

على الرغم من أن استيقان المرسل على نحو فعال يعطي موردي خدمة الإنترنت مهمة أكثر وضوحاً عند معالجة البريد الاقتحامي، فإن الاستيقان ليس إلا خطوة تمهيدية نحو التخلص من الرسائل الاقتحامية. وبعد تحديد هوية المرسل، لا بد من الاعتماد على عوامل مثل السمعة والاعتماد من أجل تحديد ما إذا كان ينبغي تصنيف الرسالة في فئة الرسائل الاقتحامية قبل وصولها إلى المستعمل. وتقوم سلطات مستقلة بإدارة عملية الإشهاد ووضع المعايير لها. وثمة لجنة عليا تمثل مختلف القطاعات تشرف على سلطات الإشهاد.

ولهذه الغاية، استحدث فريق الخصوصية الإلكترونية المعيار المفتوح للبريد الإلكتروني الموثوق (TEOS). وقد انبثق المعيار TEOS من برنامج التنظيم الذاتي لدوائر الصناعة المهتمة بالخصوصية الإلكترونية وهو يهدف إلى فصل البريد الإلكتروني المشروع عن البريد الاقتحامي. والمعيار TEOS يتجاوز الاستيقان ويستحدث هوية موثوقة لمرسلي البريد الإلكتروني استناداً إلى توقيعات مدرجة في رأسيات الرسائل الإلكترونية. وخلافاً لتوقيعات استيقان أسلوب البريد المعرّف بمفاتيح الميادين (DKIM) فإن توقيعات TEOS عبارة عن أختام مرئية في الرسائل تشهد على استيفاء المرسِل للمعايير المحددة.

ومن أجل التخفيف من مشكلة البريد الإلكتروني بالجملة الذي تم ترشيحه خطأً كبريد اقتحامي، تواصل الصناعة مناقشة فعالية آلية الإشهاد للبريد بالجملة، إذ يمكن مثلاً تعريف هوية البريد المشروع بالجملة عند مستوى مورد خدمة الإنترنت بواسطة وسم يتعرف إليه المخدم، مما يزيد من موثوقية استعمال مراشيح البريد الإلكتروني. ويمكن استخدام عدة معايير في عملية الإشهاد مثل الالتزام بممارسات خصوصية صارمة. ففرنسا، على سبيل المثال، تعمل الآن مع وكالة حماية البيانات (CNIL) لديها من أجل الإشهاد للمرسلين الذين يبلغون عن الغرض من استعمال سجلات العملاء.

وسيحتفظ كل مورد من موردي خدمة الإنترنت بقائمة بيضاء للزبائن المعتمدين. ويتطلب الاقتراح اتفاقاً بين هؤلاء الموردين بشأن عملية الإشهاد ولا ينطوي على أي تدخل خارجي. غير أن الطريقة تتطلب كتلة حرجة من مشاركة موردي خدمة الإنترنت كيما تكون فعالة وهي تعتمد على الثقة المتبادلة بين الموردين، إذ أنه لا يوجد إشراف خارجي على عملية الإشهاد. وإضافة إلى ذلك، قد يكون تخصيص عدد ثابت لتحديد البريد بالجملة مسألة إشكالية. ويستطيع المقتحمون الدهاة أن يستعملوا عدة حسابات بريد إلكتروني مجانية لإرسال كميات كبيرة من الرسائل الاقتحامية، حيث يرسل في كل حساب عدد أدنى بقليل من العتبة المحددة مسبقاً لعدد رسائل البريد بالجملة.

3.13.7 التحقق من مخدم مرسل البريد؟

يحتاج إلى مزيد من الدراسة.

4.13.7 توقيعات مستوى خصوصية لا بأس به (PGP)

يحتاج إلى مزيد من الدراسة.

5.13.7 تشكيلة النظام

إن أفضل الممارسات في مجال الأمن في دوائر الصناعة وعلى المستوى الفردي، من حيث المنافذ وجدران الوقاية والشبكات والمسيِّرات وبرمجيات الوكالة والنفاذ وكلمات السر والحماية بمفاتيح السماح وتركيب البرمجيات، أمثلة لاستعمال تشكيلة النظام كتقنية لمكافحة الرسائل الاقتحامية. وبالإمكان، من خلال تشكيل النظام لمنع البريد غير المرغوب فيه، احتباس بعضه.

ولكن بما أن عدداً متزايداً من الأنظمة تركب هذه الآليات، فإن مخيلة المقتحمين ستتفتق ولا بد عن مزيد من العبقرية ولكن ستقل الرغبة في الاقتحام أكثر فأكثر بسبب المزيد من العوائق التي ينبغي تخطيها. فالناس الآن يبعثون البريد الاقتحامي لأن ذلك سهل وسريع وقليل التكاليف. وعندما يتغير ذلك، علماً بأن مئات الآلاف من إدارات الأنظمة تعمل حالياً على تغيير هذه الحالة، سيكون من الصعب النجاح في إرسال بريد اقتحامي.

6.13.7 أدوات مكافحة الفيروسات

إن أدوات مكافحة الفيروسات تكنولوجيا هامة للتخفيف من خطر الرسائل الإلكترونية الاقتحامية على الأنظمة الحاسوبية. وتحتوي عادة الرسائل الإلكترونية الاقتحامية الضارة على ملفات مرفقة قادرة على نشر الفيروسات. وتستطيع برمجيات مكافحة الفيروسات أن تمسح صناديق البريد وتمنع تفشي الفيروسات.

ويعمل بعض موردي خدمة الإنترنت على مراقبة السطح البيني لبرمجة التطبيقات (API) لمكافحة الفيروسات (VSAPI) وتحديثه باستمرار باستخدام مخدم التبادل. وتتيح هذه التكنولوجيا مسح صناديق بريد المستعملين ضد الفيروسات من أجل وضع عملية المسح على حافة الشبكة لإضعاف تأثير الرسائل المحتوية على فيروسات والملوثة بالفيروسات على البنى التحتية للشبكة. وبالإمكان أيضاً منع البريد الملوث من مغادرة منظمة ما من خلال مسح البريد الصادر إضافة إلى البريد الوارد.

14.7 كيفية استعمال التكنولوجيات المستعرضة والعوامل الواجب مراعاتها

تتوقف الفائدة من أي أداة (أدوات) على احتياجات مستعمل هذه الأداة وقدرته التقنية والبنية التحتية المتوفرة له. والغرض من الأدوات أن تُنشر في أجزاء مختلفة عبر النظام ولأغراض مختلفة. وعلى المستعملين دراسة احتياجاتهم واستراتيجيات الدفاع دراسة معمقة لدى اختيارهم أدوات مكافحة الرسائل الاقتحامية ونشرها. وتختلف الأدوات ذاتها من حيث النضج والفعالية والاعتمادية والانتشار. وبعض الأدوات أكثر عرضة من غيرها للإيجابيات الكاذبة وبعضها أكثر فعالية في مناطق محددة وبعضها يتميز بقدر أعلى من حيث التكاليف الثابتة والبنية التحتية وعرض النطاق/القدرة والخبرة التقنية الضرورية. وقد ورد ذكر عدد من هذه العوامل للنظر فيها لكن على المستعملين الحكم على جدوى الأدوات الموضوعة في السياق المحدد لتطبيقاتها المزمعة.

وقد صمم بعض الاختبارات المذكورة أعلاه لمكافحة الرسائل الاقتحامية بينما يهدف بعضها الآخر إلى منع أنماط معينة من السلوك التي تهدد الأمن ولا تحترم موارد المنصات الحاسوبية التي يرسَل إليها البريد أو أنها بكل بساطة لا تتقيد بالقواعد المتفق عليها في إرسال الرسائل الإلكترونية. وعندما تطبَّق قاعدة ما بعد استلام البيانات المكونة للرسالة التي ينبغي تسليمها يبقى أن تتقرر كيفية التعامل مع الرسالة. ويتوقف ذلك بالطبع على نتائج الاختبارات التي أجريت. وبعض الاختبارات موثوقة أكثر من بعضها الآخر ويمكنها بالتالي تبرير اللجوء إلى مزيد من التدابير المشددة. وعلاوة على ذلك، قد يتقرر إجراء اختبارات أخرى أكثر تكلفة على بعض الرسائل.

وفيما يلي عرض للخيارات المختلفة الخاصة بمعالجة رسالة ما حسب موقع القاعدة المطبقة.

15.7 النبذ في دورة بروتوكول نقل البريد بأسلوب بسيط (SMTP)

تكمن أهمية هذا النبذ في عدم تولي معالجة الرسالة الإلكترونية التي يبقى المخدم البعيد الذي جرى إخباره بالوضع مسؤولاً عن توزيعها. إضافة إلى ذلك، يوفر النبذ سعة عرض النطاق، أولاً بسبب عدم استقبال الرسالة، وثانياً لأن المخدم البعيد لن يضطر إلى إرسال تبليغ عن حالة التسليم (DSN)، وهي الرسالة التي تتولد رداً على النبذ (انظر [b-IETF RFC 3461]) الذي قد تولّده الرسالة. وتنتقل مهمة إصدار رسالة عدم التسليم هذه إلى المرسل.

غير أن هذا النوع من النبذ يعني أنه يتعذر الاحتفاظ بنسخة من الرسالة (وبالتالي استعادة رسالة مشروعة قد لا تكون حظيت بالقبول أو مجرد البحث عن أسباب النبذ).

علاوة على ذلك، ليست المخدمات SMTP جميعها قادرة حالياً على إجراء اختبارات معينة أثناء دورة البروتوكول SMTP. غير أن ذلك في طريقه إلى التغيّر نظراً لتزايد انتشار استعمال منتوجات جديدة وخصوصاً سطوحاً بينية مثل المخدمات

"milter" أو "مخدم السياسات" Postfix أو خدمات الحافة المضافة المفتوحة (OPES) المقبلة التي ستكون قادرة على وصل أي برنامج مع دورة SMPT.

16.7 النبذ الصامت

غالباً ما تربك هذه الطريقة المستعملين الذين يتوقعون تسليم رسائلهم الإلكترونية إلى مقاصدها أو على الأقل أن يبلغوا بنبذها. إذ إن خيار "التسليم أو التبليغ" مبدأ رئيسي في إرسال البريد الإلكتروني، ولكنه سوف يهمَل على الأرجح بسبب عدم مراعاة العدد الكبير من الرسائل الإلكترونية المزمع إرسالها من مرسل ما.

وينبغي مثالياً الاحتفاظ بسجل للرسائل الإلكترونية المتلفة بهذه الطريقة، بحيث يمكن استعمال تقنيات مثل تتبع الرسالة، من خلال نشر المعيار [b-IETF RFC 3885] مثلاً الذي يصف بروتوكول تتبع الرسائل، بحيث يمكن للمستعملين معرفة ما حدث لرسائلهم (على غرار أنظمة تتبع الطرود لمختلف شركات توزيع الطرود).

17.7 النبذ بإرسال تبليغ عن حالة التسليم (DSN) أو رسالة الارتجاع "bouncing"

هي الطريقة المستخدمة تقليدياً في البريد الإلكتروني. لكن نظراً لوجود رسائل الانتحال، هناك احتمال معاقبة مرسلين أبرياء، كما في حالة برامج مكافحة الفيروسات التي ترسِل خطأً رسائل DSN.

18.7 التسليم إلى صندوق رسائل اقتحامية

عند منع رسائل قليلة من الدخول إلى منصة حاسوبية، فإن صندوق الرسائل الاقتحامية قد يضم عدداً هائلاً من الرسائل مما يثني المستعملين عن قراءتها. فالرسالة لا يجري تدميرها وإنما تتاح للمستعمل فرصة علاج "الإيجابيات الكاذبة".

19.7 الوسم

لا يتخذ المخدم في هذه الحالة أي قرار وإنما يقتصر على وسم الرسالة. وتعطي هذه التقنية المستعمِل زمام التحكم لكنها ترغمه في نفس الوقت على تحميل البريد الاقتحامي.

وجدير بالذكر أن مورد خدمة البريد الإلكتروني يمكنه أن يوفر للمستعمل خيار وسم الرسالة فحسب أو إرسالها إلى صندوق الرسائل الاقتحامية، وهي عملية سهلة نسبياً.

التذييـــل I

أنشطة مكافحة البريد الإلكتروني الاقتحامي

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I مقدمة

يتناول هذا التذييل بعض الأنشطة المضطلَع بها مؤخراً في منظمات مختلفة منها قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات في مكافحة البريد الإلكتروني الاقتحامي وكذلك المواصفات التقنية والتحالفات والمبادرات في دوائر الصناعة في هذا الصدد. وقد كانت هذه المنظمات ناشطة في أعمال مكافحة البريد الإلكتروني الاقتحامي أثناء إعداد التوصية. وبالتالي، قد تتغير مستقبلاً طائفة المواصفات التقنية التي قدمتها المنظمات المذكورة وصلاحيتها ووضعها.

2.I الأنشطة الدولية بشأن مكافحة الرسائل الاقتحامية

1.2.I الاتحاد الدولي للاتصالات

في إعلان المبادئ الذي اعتمد في المرحلة الأولى للقمة العالمية لمجتمع المعلومات التي عُقدت في جنيف في ديسمبر 2003 [b-WSIS-2003]، تحدد البريد الاقتحامي على أنه خطر يهدد استعمال خدمات الإنترنت والبريد الإلكتروني بالكامل. وبناءً عليه أقرَّ المشاركون في القمة بأن الرسائل الاقتحامية تمثل "مشكلة هامة ومتزايدة للمستعملين والشبكات وللإنترنت برمتها" وأنه لا بد من أجل بناء الثقة والأمن في استعمال تكنولوجيات المعلومات والاتصالات من "اتخاذ الإجراءات المناسبة بشأن الرسائل الاقتحامية على المستويين الوطني والدولي".

وتم تسليط الضوء على اهتمام الدول الأعضاء في الاتحاد الدولي للاتصالات بالقضايا المتعلقة بالرسائل الاقتحامية أثناء الجمعية العالمية لتقييس الاتصالات التي عُقدت في فلوريانوبوليس بالبرازيل في أكتوبر 2004. ووافق أعضاء الاتحاد أثناء انعقاد الجمعية على قرارين يتعلقان بأنشطة الاتحاد المقبلة في مجال مكافحة الرسائل الاقتحامية.

ويكلف القرار الأول، وهو القرار 51 بشأن مكافحة الرسائل الاقتحامية، مديري القطاعات الثلاثة في الاتحاد والأمين العام للاتحاد بأن يقوموا على وجه السرعة بإعداد تقرير إلى المجلس في دورته لعام 2005 عن مبادرات الاتحاد وغيرها من المبادرات الدولية ذات الصلة لمكافحة الرسائل الاقتحامية وبالعمل، بمساهمة الدول الأعضاء وأعضاء القطاعات، على اقتراح إجراءات المتابعة الممكنة لكي ينظر فيها المجلس. كما يدعو القرار الدول الأعضاء إلى اتخاذ الخطوات الملائمة في إطار قوانينها الوطنية لضمان اتخاذ التدابير الملائمة والفعالة لمكافحة الرسائل الاقتحامية.

أما القرار الثاني، وهو القرار 52 بشأن مكافحة الرسائل الاقتحامية بالوسائل التقنية، فيؤكد "أن الرسائل الاقتحامية تخلق مشاكل أمنية لشبكات الاتصالات بما في ذلك استعمالها كقناة لنشر الفيروسات والديدان وغيرها". ويشير القرار أيضاً إلى وجود توصيات صادرة عن قطاع تقييس الاتصالات بشأن هذا الموضوع يمكنها أن توجه الخطى للتطوير المقبل في هذا الميدان، ويكلف بالتالي لجان الدراسات ذات الصلة في قطاع تقييس الاتصالات، بالتعاون مع فريق مهام هندسة الإنترنت (IETF) وغيره من الأفرقة ذات الصلة بأن تضع، على وجه الاستعجال، توصيات تقنية بشأن مكافحة الرسائل الاقتحامية حسب الاقتضاء، وأن تقدم تقارير منتظمة عن تقدم أعمالها إلى الفريق الاستشاري لتقييس الاتصالات. وينبغي دعم هذه الجهود بتقديم كل المساعدة اللازمة من مدير مكتب تقييس الاتصالات الذي سيقدم تقريراً عن هذا الموضوع إلى مجلس الاتحاد.

2.2.I منظمة التعاون والتنمية في الميدان الاقتصادي (OECD)

تؤثر الرسائل الاقتحامية سلباً على الاقتصاد الرقمي وتتسبب في خسائر اقتصادية واجتماعية جسيمة في بلدان المنظمة OECD وفي البلدان الأخرى. ونظراً لاحتمال ظهور مشاكل أخرى نتيجة لتقارب تكنولوجيات الاتصالات وتطور الاتصالات في آن واحد في كل مكان وكذلك الإنترنت المتنقلة، تواجه البلدان الأعضاء في المنظمة OECD ضرورة إيجاد

أساليب فعالة لمكافحة الرسائل الاقتحامية. ومن أجل التصدي لهذه المشاكل، نادت اللجنة المعنية بسياسات المعلومات والمعلوماتية والاتصالات (ICCP) التابعة للمنظمة OECD بالعمل بشأن هذا الموضوع الهام خلال اجتماع عقد في 3 و4 مارس 2003، وطالبت بأن يُعطى صفة الاستعجال مشيرةً إلى أن هذه المسألة مسألة عالمية. كما أبدت اللجنة المعنية بسياسة المستهلك (CCP) أيضاً اهتماماً بمواصلة عمل المنظمة OECD في هذا الموضوع. وتم الاضطلاع باستكشاف أولي للمسائل المتصلة بالرسائل الاقتحامية في وثيقة معلومات أساسية وفي ورشة عمل خُصصت للرسائل الاقتحامية في فبراير 2004 استضافتها المفوضية الأوروبية في بروكسل.

والرسائل الاقتحامية مسألة متشابكة تؤثر على استعمال الشبكات وجوانب الازدحام والشبكة القائمة على بروتوكول الإنترنت والخصوصية وأمن الشبكة وحماية المستهلك. وحرصاً على حُسن تنسيق العمل بشأن الرسائل الاقتحامية وبغية التوصل سريعاً إلى توافق الآراء بشأن إطار سياسة لمعالجة قضايا الرسائل الاقتحامية، وافق مجلس المنظمة OECD في يوليو 2004 على إنشاء "فريق مهام معني بالرسائل الاقتحامية". وطُلب من فريق المهام تقديم تقرير إلى اللجنتين CCP وICCP عن ذلك في موعد أقصاه يوليو 2006.

وكان الهدف الأساسي لفريق المهام جمع منسقين معنيين لسياسات مكافحة الرسائل الاقتحامية والتمهيد لإعداد فعال لمجموعة من الأدوات السياسية المطلوبة عاجلاً من أجل مكافحة الرسائل الاقتحامية ومعالجة المشكلة من منظور أوسع والاستفادة من الخبرات متعددة الاختصاصات المتوفرة لدى المنظمة OECD.

وطُلب من فريق المهام أن يدرس شتى استراتيجيات مكافحة الرسائل الاقتحامية القائمة والناشئة وأن يوثقها ويروج لها داخل جميع القطاعات. وإقراراً من الفريق بعدم وجود "حل سحري" لمعالجة الرسائل الاقتحامية وضع "مجموعة أدوات" لمكافحتها في أبريل 2006. وتنطلق مجموعة الأدوات من ضرورة الأخذ بعدد من العناصر المختلفة والمنسقة لتذليل مشكلة الرسائل الاقتحامية من أجل المساعدة على إعداد وتطوير استراتيجيات وحلول لمكافحة الرسائل الاقتحامية في المجالات التقنية والتنظيمية والإنفاذية وتسهيل التعاون الدولي. والغرض من مجموعة أدوات المنظمة OECD هو جمع مجموعة من مبادرات السياسة وغيرها من المبادرات (الإنفاذ مثلاً) المتساوقة والمتكاملة. وقد اعتمد إعداد مجموعة الأدوات وتنفيذها اعتماداً كبيراً على مساهمات من أصحاب المصلحة في مختلف المجالات المشمولة. وتتألف مجموعة الأدوات هذه من ثمانية عناصر مترابطة فيما بينها وهي:

- القواعد التنظيمية لمكافحة الرسائل الاقتحامية.
- التعاون الدولي في مجال الإنفاذ.
- الحلول التي تولّدها دوائر الصناعة لمكافحة الرسائل الاقتحامية.
- التكنولوجيات القائمة والناشئة لمكافحة الرسائل الاقتحامية.
- التثقيف والتوعية.
- الشراكات التعاونية لمكافحة الرسائل الاقتحامية.
- أدوات قياس الرسائل الاقتحامية.
- التعاون العالمي (الجهات الخارجية).

وقد أُعدت لفريق المهام تقارير معلومات أساسية عن عدة عناصر من مجموعة الأدوات. ويلخص هذا التذييل العمل الذي اضطلع به فريق المهام واستنتاجاته. ويكمل هذا التذييل توصية مجلس المنظمة OECD بشأن تعزيز التعاون عبر الحدود في مجال الإنفاذ لمكافحة الرسائل الاقتحامية وموقع المنظمة عن مكافحة البريد الاقتحامي على شبكة الويب: (www.oecd-antispam.org).

3.2.I مجلس التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC)

تناقش المسائل المتعلقة بالبريد الاقتحامي في مجلس التعاون الاقتصادي لآسيا والمحيط الهادئ ضمن فريق العمل المعني بالاتصالات والمعلومات (TEL WG). والفريق ملتزم بتحسين البنية التحتية للاتصالات والمعلومات في المنطقة وبتسهيل التعاون الفعال والتجارة الحرة والاستثمار والتنمية المستدامة.

وفي مجال أمن الشبكات والبنى التحتية، يتعاون الفريق مع منظمات أخرى بشأن المسائل الأمنية، ويعمل على تعزيز الأنشطة الرامية إلى خلق بيئة آمنة على الخط في مجتمع المعلومات، ويعالج قضايا مثل الرسائل الاقتحامية من أجل التصدي للتهديدات التي تواجه الشبكات بما في ذلك متابعة مبادئ العمل التي وضعها المجلس APEC بشأن إجراءات مكافحة الرسائل الاقتحامية والإرشادات التنفيذية التي وضعها المجلس APEC بشأن إجراءات مكافحة الرسائل الاقتحامية والتعاون مع المنظمات الدولية والإقليمية مثل الاتحاد الدولي للاتصالات والمنظمة OECD ورابطة أمم جنوب شرق آسيا (ASEAN). وتتاح المعلومات ذات الصلة على موقع الفريق التالي على شبكة الويب: (http://www.apectelwg.org).

3.I وضع المواصفات التقنية من أجل مكافحة الرسائل الاقتحامية

1.3.I قطاع تقييس الاتصالات في الاتحاد

كلّفت الجمعية العالمية لتقييس الاتصالات (فلوريانوبوليس، 2004) في قرارها رقم 52 لجان الدراسات ذات الصلة بأن تضع، بالتعاون مع فريق مهام هندسة الإنترنت (IETF) وغيره من الأفرقة ذات الصلة، توصيات تقنية تشمل، حسب الاقتضاء، التعاريف المطلوبة بشأن مكافحة الرسائل الاقتحامية، وأن تقدم تقارير منتظمة عن التقدم المحرز إلى الفريق الاستشاري لتقييس الاتصالات.

ولجنة الدراسات 17، باعتبارها لجنة الدراسات الرئيسية في مجال أمن الاتصالات ودعم الأنشطة التي تناولتها القرارات 50 و51 و52 الصادرة عن الجمعية العالمية لتقييس الاتصالات، في وضع يسمح لها بدراسة مختلف التدابير التقنية الممكنة لمكافحة الرسائل الاقتحامية بقدر ما تتعلق باستقرار شبكات الاتصالات ومتانتها. وقد أنشأت لجنة الدراسات 17 فريقاً مقرراً مكرساً للمسألة Q.17/17 مهمته إيجاد حلول تقنية لمكافحة الرسائل الاقتحامية. ويركّز العمل الأولي على وضع مواصفات تقنية لمكافحة الرسائل الاقتحامية. وتتوسع الأعمال بعد ذلك لتشمل وضع الحلول التقنية لمكافحة الرسائل الاقتحامية في تطبيقات ببروتوكول الإنترنت متعددة الوسائط مثل المهاتفة IP والمراسلة اللحظية وغيرها. وتغطي المواصفات التقنية المبادئ التوجيهية والمتطلبات والأطر التقنية والوسائل التقنية لمكافحة مختلف أنماط الرسائل الاقتحامية، أو تخطط لتغطيتها.

2.3.I فريق مهام هندسة الإنترنت (IETF)

وضع فريق مهام هندسة الإنترنت عدة معايير RFC بشأن مكافحة البريد الإلكتروني الاقتحامي تتراوح ما بين مبادئ توجيهية ومواصفات تقنية على النحو التالي:

- المعيار [b-IETF RFC 2505] "توصيات لمكافحة الرسائل الاقتحامية تتعلق بوكلاء نقل البريد MTA في بروتوكول SMTP":

  يقدم هذا المعيار عدداً من التوصيات التنفيذية التي تتعلق بوكلاء نقل البريد (MTA) الذين يستعملون البروتوكول SMTP لتعزيز قدراتهم على الحد من أثر الرسائل الاقتحامية. والغرض من ذلك هو أن تسهم هذه التوصيات في تحسين الحالة إزاء الرسائل الاقتحامية عندما تطبَّق على عدد كافٍ من الوكلاء SMTP MTA على شبكة الإنترنت، وأن تُستخدم كمبادئ توجيهية لبائعي مختلف البرامج MTA. ولا يُعتبر ذلك حلاً نهائياً ولكن إذا أُدرجت هذه التوصيات واستُخدمت في كل برامج SMTP MTA على شبكة الإنترنت، فإن الأمور ستتحسن كثيراً وستتيح الوقت الكافي لتصميم حل طويل المدى. ويقترح القسم الخاص بالعمل في المستقبل بعض الأفكار التي قد تكون جزءاً من الحل طويل المدى. ومع ذلك، فإن طابع الحل النهائي قد يكون اجتماعياً أو سياسياً أو قانونياً أكثر منه تقنياً. ومن الضروري أن يدرك المنفذون احتمال تزايد هجمات رفض الخدمة جراء بعض الطرائق المقترحة. فقد يؤدي مثلاً

العدد المتزايد من الاستفسارات الموجهة إلى المخدمات DNS وتعاظم حجم ملفات تسجيل الوقائع إلى تحميل الأنظمة أكثر من طاقتها وإلى انهيارها خلال الهجمات.

- المعيار [b-IETF RFC 2635]" مجموعة مبادئ توجيهية بعنوان **لا تفيض بشأن** الرسائل والمنشورات الجماعية غير المطلوبة (الرسائل الاقتحامية*)":

يشرح هذا المعيار الأسباب التي تجعل الرسائل الإلكترونية الجماعية غير المطلوبة ضارة للمجتمعات التي تستخدم التوصيل الشبكي. وهو يقدم مجموعة من المبادئ التوجيهية بشأن كيفية معالجة الرسائل غير المطلوبة لصالح المستخدمين ومديري الأنظمة ومديري الأخبار ومديري القوائم البريدية. وهي توفر أيضاً اقتراحات قد يعمل بها موردو خدمة الإنترنت.

- المعيار [b-IETF RFC 3685] "تمديدات اختبار الرسائل الاقتحامية واختبار الفيروسات، برنامج SIEVE لترشيح البريد الإلكتروني":

تتيح تمديدات "اختبار الرسائل الاقتحامية" و"اختبار الفيروسات"، SIEVE، للمستعملين إمكانية استخدام عمليات تحكم بسيطة ومتنقلة لإجراء اختبارات الرسائل الاقتحامية والفيروسات على رسائل البريد الإلكتروني. ويوفر كل تمديد اختباراً جديداً يستخدم عمليات مزاوجة مقابل "علامات" رقمية. والبرنامج SIEVE المعني هو المسؤول عن إجراء عمليات التحقق الفعلي التي تترجَم إلى قيم تعطيها الاختبارات.

- المعيار [b-IETF RFC 4686] "تحليل التهديدات التي تطلق وظيفة البريد المعرَّف بمفاتيح الميادين (DKIM)":

يقدم هذا المعيار تحليلاً لبعض التهديدات التي يتعرض لها البريد الإلكتروني للإنترنت والتي يتعين معالجتها من خلال استيقان البريد استناداً إلى التواقيع، ولا سيما من البريد المعرَّف بمفاتيح الميادين. ويدرس طبيعة الجهات الفاعلة الشريرة وموقعها وقدراتها والأهداف التي تتوخاها عبر هجماتها.

وفضلاً عما تقدم، هناك عدة مشاريع قيد الإعداد تصف الاستيقان على مستوى الميادين وتنطبق على مكافحة البريد الإلكتروني الاقتحامي.

4.I قائمة بتحالفات ومبادرات الدوائر الصناعية لمكافحة الرسائل الاقتحامية

فيما يلي قائمة بالمبادرات الصادرة عن دوائر الصناعة من مختلف أنحاء العالم. وهي قائمة غير حصرية وينبغي أن يُنظر إليها بوصفها محاولة لبيان التنوع الشديد في المشاريع التي تضطلع بها مختلف المنظمات بهدف مكافحة الرسائل الاقتحامية بطريقة منسقة وفعالة.

1.4.I فريق العمل المعني بمكافحة الانتحال

فريق العمل المعني بمكافحة الانتحال (APWG) [b-APWG] رابطة عالمية صناعية لإنفاذ القوانين تركز على القضاء على عمليات الاحتيال وانتحال الهوية الناجمة عن تفاقم مشكلة الانتحال والتضليل وتزوير البريد الإلكتروني. وتتيح هذه الرابطة منبراً لمناقشة مسائل الانتحال، وتعرِّف مدى تأثير مشكلة الانتحال من حيث التكاليف المتعلقة بالعتاد والبرمجيات وتتبادل المعلومات وأفضل الممارسات من أجل القضاء على هذه الظاهرة. ويعمل فريق العمل أيضاً حسب الاقتضاء على تبادل هذه المعلومات مع أجهزة إنفاذ القوانين.

2.4.I تحالف الاستيقان والثقة على الخط

أنشئ موقع Email Authentication.org (استيقان البريد الإلكتروني) في أكتوبر 2004، ثم أصبح هيئة تُدعى تحالف الاستيقان والثقة على الخط (AOTA Inc.) هدفها تعزيز الثقة على الخط والاطمئنان إلى مختلف أشكال المراسلة الإلكترونية والتجارة الإلكترونية والعمليات المصرفية الإلكترونية والإنترنت، كما تساعد على تعزيز الأمان وتوفير الحماية على الخط للمؤسسات التجارية والمستهلكين على حد سواء. وتشمل الأهداف تيسير أفضل الممارسات وتقاسم البيانات ونشر وتنفيذ أساليب استيقان البريد الإلكتروني والإنترنت ووضع معايير وحلول الهوية والسمعة واستراتيجيات للدفاع عن الميادين وتقديم

المشورة الناظمة والقابلة للتطبيق لنظام إيكولوجي في بيئة حيادية من حيث البائعين. ويتألف تحالف الاستيقان والثقة على الخط (AOTA) من شركات تجارية وصناعية رائدة ومنظمات لا تستهدف الربح غايتها تعزيز الثقة والشعور بالاطمئنان إلى المراسلات الإلكترونية والإنترنت والتجارة الإلكترونية. وهذا التعاون أمر في غاية الأهمية في وجه الانتحال والتزوير الإلكتروني لما لهذا التعاون من دور في ضمان موثوقية البريد الإلكتروني وضمان القدرة على تسليمه وتعزيز الثقة بالاتصالات الإلكترونية والاطمئنان إليها، وحماية الأسماء التجارية للشركات وأسماء ميادينها في مختلف أرجاء العالم.

وفي أوائل عام 2004، بدأت مجموعة من روَّاد الأعمال والصناعة والتسويق، تتصدرها Bigfoot Interactive وائتلاف مرسلي البريد الإلكتروني وموردي الخدمة (ESPC) وميكروسوفت وسندميل (Sendmail)، تعقد اجتماعات بهدف البحث عن حلول لاستيقان البريد الإلكتروني وتعزيز ثقة المستعملين. وقد صدر عن القمة التي عقدتها في نوفمبر 2004 لجنة التجارة الفدرالية الأمريكية للاستيقان، والتي شارك في رعايتها المعهد الوطني للمعايير والتكنولوجيا التابع لوزارة التجارة، قرار باتخاذ تدابير حاسمة من أجل إحراز تقدم في مجال استيقان البريد الإلكتروني وبإنشاء منظمة emailauthentication.org. وإزاء استمرار هجمات الانتحال والتضليل من خلال البريد الإلكتروني مما ينال من ثقة المستعملين ودوائر الأعمال، تحوَّلت المنظمة في سبتمبر 2006 إلى تحالف الاستيقان والثقة على الخط (AOTA).

وفي الوقت الذي حافظ فيه التحالف AOTA على تركيزه وريادته التقنية في مجال استيقان البريد الإلكتروني فقد وسع مهمته لتشمل المساهمة في معالجة المسائل والتهديدات الأوسع نطاقاً التي تنال من الثقة في الاتصالات على الخط.

3.4.I شبكة اتصال السلطات المعنية بمكافحة الرسائل الاقتحامية (CNSA)

استُحدث، بناءً على مبادرة المفوضية الأوروبية، فريق غير رسمي يتألف من السلطات الوطنية المعنية بإنفاذ المادة 13 من التوجيه 2002/58/EC المتعلق بالخصوصية والاتصالات الإلكترونية بعنوان "شبكة اتصال السلطات المعنية بمكافحة الرسائل الاقتحامية (CNSA)".

ويتم، في إطار الشبكة CNSA، تبادل المعلومات بين السلطات الوطنية بشأن الممارسات الراهنة لمكافحة الرسائل الاقتحامية. وتضم هذه المعلومات أفضل الممارسات لتلقّي معلومات الشكاوى والتحري والبحث بشأن الرسائل الاقتحامية ومعالجتها. والمفوضية الأوروبية مسؤولة عن أمانة الشبكة CNSA. وفي الشبكة أيضاً جهة تنسيق تقوم بتسهيل تبادل المعلومات بين أعضائها وتوفّر الدعم لأمانة المفوضية. وجهة التنسيق الحالية هي مكتب رئيس الوزراء الفرنسي. وتجتمع الشبكة CNSA بانتظام (3-4 مرات سنوياً) في بروكسل. كما تعقد الشبكة سنوياً اجتماعات مشتركة مع خطة عمل لندن.

وقد وضعت الشبكة CNSA إجراء تعاون يرمي إلى تيسير نقل معلومات الشكاوى أو غيرها من معلومات التحري ذات الصلة بين السلطات الوطنية.

4.4.I شبكة مكافحة الانتحال الرقمي

أنشئت شبكة مكافحة الانتحال الرقمي (DPN) في 8 ديسمبر 2004 كعملية إنفاذ تعاونية تهدف إلى الجمع بين شركات صناعية رائدة في الخدمات التكنولوجية والمصرفية والمالية والمزادات على الخط مع هيئات إنفاذ القانون لمكافحة "الانتحال"، ذلك الشكل الهدام المتفاقم من أشكال انتحال الهوية على الخط.

والانتحال تهديد ناشئ على الخط شديد الضرر والتضليل ينطوي على استدراج المستهلكين إلى مواقع مزيفة على الويب، عادة من خلال رسائل إلكترونية اقتحامية مزورة أو خادعة، من أجل إدخال معلومات مالية شخصية كأرقام بطاقات الائتمان وكلمات السر. وبينما تركز مجموعات صناعية أخرى على تحديد مواقع الانتحال على الويب وعلى تبادل أفضل الممارسات والمعلومات عن الحالات، فإن الشبكة DPN هي أول مجموعة من نوعها تركز على مساعدة هيئات إنفاذ القوانين الجنائية في إلقاء القبض على المسؤولين عن ارتكاب جرائم ضد المستهلكين من خلال الانتحال ومقاضاتهم. وتقيم الشبكة DPN خط اتصال واحداً موحداً بين دوائر الصناعة وهيئات إنفاذ القانون بحيث يمكن تجميع البيانات الهامة لمكافحة الانتحال وإتاحتها لهيئات إنفاذ القانون في الوقت الفعلي.

5.4.I ائتلاف مرسلي البريد الإلكتروني وموردي خدماته

ائتلاف مرسلي البريد الإلكتروني ومزودي خدماته مجموعة تعاونية من شركات صناعية رائدة تعمل من أجل التوصل إلى حلول لمسألة الانتشار المستمر للرسائل الاقتحامية وللمشكلة الناشئة في قابلية تسليمه. ويقر أعضاء الائتلاف بالحاجة إلى حلول جذرية لظاهرة الرسائل الاقتحامية قادرة على ضمان تسليم البريد الإلكتروني المشروع، وهم ناشطون جداً في مكافحة الاقتحام. ويسعى الائتلاف إلى التوصل إلى حلول لمشكلتي الرسائل الاقتحامية وقابلية التسليم من خلال مزيج من استقطاب الدعم التشريعي والتطور التكنولوجي ومعايير الصناعة.

ويتألف الائتلاف من أربع لجان فرعية هي:

- اللجنة التشريعية التي توجه جهود الائتلاف لاستقطاب الدعم للتشريعات المناهضة للرسائل الاقتحامية على الصعيد الاتحادي وصعيد الولايات.
- لجنة علاقات المتلقين التي شُكلت لتسهم في تيسير الفهم الأفضل والحوار المستمر بين جماعات المرسلين وجماعات المتلقين القائمة.
- لجنة التكنولوجيا التي تقيِّم وتطوِّر الحلول التكنولوجية التي من شأنها أن تتيح وسائل أكثر دقة للتصدي للرسائل الاقتحامية (وعدداً أقل من الإيجابيات الكاذبة). وقد جرى تشكيل فريق عمل تقني ضمن هذه اللجنة مهمته استكشاف الحلول وتقديم الاقتراحات بشأنها. ويجتمع فريق العمل هذا عند الحاجة ويعقد اجتماعات وجهاً لوجه بين الفينة والأخرى.
- لجنة الاتصالات التي تضع للائتلاف استراتيجية عريضة لشؤون الجمهور.

6.4.I معهد السياسات العامة المتعلقة بالرسائل الاقتحامية والإنترنت (ISIPP)

معهد السياسات العامة المتعلقة بالرسائل الاقتحامية والإنترنت (ISIPP) مكرس لتوفير التحليلات والمعلومات والاستشارات بشأن قضايا الصناعة المتصلة بالسياسات والعمليات الخاصة بالجمهور والمتعلقة بالرسائل الاقتحامية والبريد الإلكتروني وقابلية تسليم البريد الإلكتروني والإنترنت. ويوفر المعهد أيضاً خدمة اعتماد لمرسلي البريد الإلكتروني (SuretyMail) تُستخدم على نطاق واسع. وينظم ويرعى المعهد منتديات للصناعة، مثل اجتماعات المائدة المستديرة بشأن إدارة البريد الإلكتروني واجتماعات القمة الخاصة بقابلية تسليم البريد الإلكتروني ومؤتمرات "الرسائل الاقتحامية والقانون".

7.4.I خطة عمل لندن

خطة عمل لندن شبكة عالمية من وكالات إنفاذ القوانين وممثلي الصناعة المعنيين بمكافحة الرسائل الاقتحامية والانتحال وغيرهما من التهديدات على الخط. وقد مهد لوضع خطة عمل لندن عام 2004 كل من اللجنة الاتحادية للتجارة في الولايات المتحدة ومكتب التجارة العادلة في المملكة المتحدة. وتضم خطة عمل لندن اليوم أعضاء ما يزيد عن عشرين بلداً. وقد شجعت الخطة منذ وضعها إقامة علاقات ثنائية ومتعددة الأطراف على حد سواء بين وكالات إنفاذ القوانين فيسَّرت بذلك التعاون الدولي في عدة تحقيقات بشأن الرسائل الاقتحامية. وتعاونت خطة عمل لندن عام 2005 مع عدة شركاء حكوميين في عملية لمكافحة إرسال الرسائل الاقتحامية بواسطة برمجيات انقيادية ("Operation Spam Zombie"). وهي مبادرة قامت في نطاقها وكالات من كل أرجاء العالم بإرسال رسائل إلى موردي خدمة الإنترنت تحثهم فيها على اعتماد تدابير وقائية من أجل منع السطو على حواسيب المستهلكين وتسخيرها لغرض إرسال رسائل اقتحامية.

وكما ورد آنفاً، فإن خطة عمل لندن تعقد اجتماعات سنوية مشتركة مع شبكة اتصال السلطات المعنية بمكافحة الرسائل الاقتحامية (CNSA). ومؤخراً عقدت خطة عمل لندن ورشة العمل المشتركة الثالثة مع الشبكة CNSA في واشنطن العاصمة في الفترة 9-11 أكتوبر 2007. وعُقدت هذه الورشة المشتركة بالاقتران مع الاجتماع العام الحادي عشر لفريق العمل المعني بمكافحة إساءة استعمال المراسلات (MAAWG). وعقدت خطة عمل لندن والشبكة CNSA عدة جلسات مشتركة مع الفريق MAAWG ركزت على العديد من الموضوعات ذات الصلة.

وعقدت خطة عمل لندن خلال ورشة عمل 2007 دورات تدريبية لوكالات إنفاذ القوانين وناقشت مزايا المبادرات التعاونية بين القطاعين العام والخاص، ودرست سبل تعزيز التعاون عبر الحدود في مجال الإنفاذ. وحضر ورشة العمل المشتركة ممثلون عن وكالات إنفاذ القوانين والقطاع الخاص من أكثر من 20 بلداً.

8.4.I فريق العمل المعني بمكافحة إساءة استعمال المراسلات (MAAWG)

فريق العمل المعني بمكافحة إساءة استعمال المراسلات (MAAWG) منظمة عالمية تركز على حماية المراسلات الإلكترونية من الاستغلال وإساءة الاستعمال على الخط وتهدف إلى تعزيز شعور المستعملين بالثقة والطمأنينة مع ضمان قابلية تسليم الرسائل المشروعة. ويعمل فريق العمل MAAWG اعتماداً على قاعدة عريضة من موردي خدمة الإنترنت ومشغلي الشبكات الذين يمثلون أكثر من 600 مليون صندوق بريد إلكتروني ومع موردي التكنولوجيا والمرسلين الرئيسيين، من أجل التصدي لإساءة استعمال الرسائل من خلال التركيز على التكنولوجيا والتعاون ضمن قطاع الصناعة ومبادرات السياسة العامة.

وهدف الفريق هو جمع العاملين في صناعة المراسلات كيما يتعاونوا من أجل التصدي بنجاح لمختلف أشكال إساءة استعمال المراسلات من قبيل الرسائل الاقتحامية وهجمات الفيروسات وهجمات رفض الخدمة وغيرها من أشكال إساءة الاستعمال. ولتحقيق ذلك، يعكف الفريق على تطوير مبادرات في ثلاثة مجالات ضرورية لحل مشكلة إساءة استعمال المراسلات، وهي: التعاون، والتكنولوجيا، والسياسات العامة.

9.4.I مشروع "سبامهاوس"

مشروع سبامهاوس (Spamhaus) منظمة دولية لا تستهدف الربح مهمتها تعقّب عصابات المقتحمين والرسائل الاقتحامية وخدمات الاقتحام وتزويد الشبكات القائمة على بروتوكول الإنترنت بحماية موثوقة من الرسائل الاقتحامية في الوقت الفعلي، والتعاون مع وكالات إنفاذ القوانين من أجل تحديد هوية المقتحمين وملاحقتهم في كل أرجاء العالم، والعمل على استقطاب دعم الحكومات من أجل اعتماد تشريعات فعالة لمكافحة الرسائل الاقتحامية. وأنشئت منظمة سبامهاوس عام 1998 ولها مقر في جنيف، سويسرا، وآخر في لندن، المملكة المتحدة، ويديرها فريق متفرّغ من 25 محققاً يتواجدون في تسعة بلدان.

وتنشر منظمة سبامهاوس سجل عمليات الرسائل الاقتحامية المعروفة باسم (ROKSO)، وهو قاعدة بيانات تجمع المعلومات والقرائن عن أسوأ 200 عصابة معروفة في العالم في مجال الرسائل الاقتحامية. ويستخدم موردو خدمة الإنترنت هذه النشرة من أجل تفادي قبول اشتراك المقتحمين المعروفين الذين يمكن أن يسيئوا استعمال شبكاتهم وكذلك تستخدمها وكالات إنفاذ القوانين لتساعدها على استهداف المقتحمين المحترفين وملاحقتهم قضائياً.

وتنشر منظمة سبامهاوس عدداً من قواعد البيانات المانعة للرسائل الاقتحامية في الوقت الفعلي، بما في ذلك قائمة سبامهاوس المانعة (SBL) وقائمة منع المستغلين (XLB) وقائمة سياسات المنع (PBL). وتبث قوائم سبامهاوس المانعة من شبكة من 40 مخدم DNS في 17 بلداً ويستخدمها العديد من كبار موردي خدمة الإنترنت والشركات والجامعات والحكومات والشبكات العسكرية.

ويجري تمويل العمليات من خلال الجهات الراعية والهبات. أما تمويل البنى التحتية الدولية فيتم عن طريق توفير خدمة تزامن قوائم منع الرسائل الاقتحامية ("Spamhaus Data Feed") التي توردها منظمة لوجستيات منفصلة إلى الشبكات الكبرى القائمة على بروتوكول الإنترنت وإلى شركات ترشيح الرسائل الاقتحامية التجارية.

10.4.I تحالف منع الرسائل الاقتحامية

تحالف منع الرسائل الاقتحامية مبادرة مشتركة لجمع المعلومات والموارد المتعلقة بمكافحة الرسائل الاقتحامية. والجهات التي اضطلعت بهذه المبادرة هي مجلس التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) وشبكة اتصال السلطات المعنية بمكافحة البريد الإلكتروني (CNSA) التابعة للاتحاد الأوروبي والاتحاد الدولي للاتصالات وخطة عمل لندن ومنظمة التعاون والتنمية في الميدان الاقتصادي (OECD) ومجموعة سيول–ملبورن لمكافحة الرسائل الاقتحامية.

وانسجاماً مع برنامج عمل تونس الصادر عن القمة العالمية لمجتمع المعلومات الذي طلب من الأعضاء "أن يعالجوا مشكلة الرسائل الاقتحامية الهامة والمتفاقمة معالجة فعالة" ودعوة جميع أصحاب المصلحة إلى اتباع نهج متعدد المحاور لمكافحة الرسائل الاقتحامية – تنشئ صفحات تحالف منع الرسائل الاقتحامية وصلات مع المبادرات المتخذة في مجال تشريعات مكافحة الرسائل الاقتحامية وأنشطة الإنفاذ وتوعية المستهلك ودوائر الأعمال وأفضل الممارسات والتعاون الدولي.

ويتوفر أيضاً "برنامج مشترك للأحداث" يضم الأحداث الدولية التي تنظمها المنظمات المعنية والمتعلقة بالرسائل الاقتحامية والتهديدات ذات الصلة، وعنوان التحالف على شبكة الويب: http://stopspamalliance.org/.

11.4.I منتدى الاتصالات الإلكترونية الموثوقة (TECF)

منتدى الاتصالات الإلكترونية الموثوقة مجموعة شركات تشمل عدة مجالات صناعية ومناطق جغرافية مهمتها تقييس التكنولوجيات والتقنيات وأفضل الممارسات في مكافحة الانتحال والتضليل وسرقة الهوية. ويركز المنتدى على العمل بكفاءة وفعالية من أجل التوصل إلى حلول للمشاكل التي تُعرض في إطار البحوث والدراسات والتحليلات وتلك التي يعرضها أعضاؤه، ويسعى إلى نشر هذه الحلول واعتمادها. ويقدم الدعم لأفرقة عمل ولجان لتقوم بوضع تقنيات وأدوات خصيصاً للتصدي للتهديدات بالغة الخطورة التي يبينها المنتدى و/أو إثبات صلاحيتها.

ببليوغرافيا

[b-WSIS-2003] WSIS First Phase (2003), *Declaration of Principles*. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>

[b-WSIS-2005] WSIS Second Phase (2005), *Tunis Agenda for the Information Society*. <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>

[b-APWG] Anti-Phishing Working Group, <http://www.antiphishing.org/>.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*. <http://www.ietf.org/rfc/rfc2505.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 2822] IETF RFC 2822 (2001), *Internet Message Format*. <http://www.ietf.org/rfc/rfc2822.txt>

[b-IETF RFC 3461] IETF RFC 3461 (2003), *Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*. <http://www.ietf.org/rfc/rfc3461.txt>

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

[b-IETF RFC 3885] IETF RFC 3885 (2004), *SMTP Service Extension for Message Tracking*. <http://www.ietf.org/rfc/rfc3885.txt>

[b-IETF RFC 4686] IETF RFC 4686 (2006), Analysis of Threats Motivating DomainKeys Identified Mail (DKIM). <http://www.ietf.org/rfc/rfc4686.txt>

[b-FTC] United States Federal Trade Commission, *Email Address Harvesting and the Effectiveness of Anti-Spam Filters*, November, 2005. <http://www.ftc.gov/opa/2005/11/spamharvest.pdf>

[b-Lyris] Lyris Technologies, Inc., *Email Advisor: ISP Email Deliverability Report Card*, 2nd quarter, 2007. <http://www.lyris.com/resources/reports/deliverability_report_Q22007.pdf>

[b-OECD TF] OECD Task Force on Spam (2006), *Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures*. <http://www.oecd.org/dataoecd/63/28/36494147.pdf>

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