Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1233

(09/2021)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Lutte contre le spam

Lignes directrices relatives à la lutte contre le spam par messagerie instantanée

Recommandation UIT-T X.1233

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	**X.1230–X.1249**
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ IMT-2020	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1233

Lignes directrices relatives à la lutte contre le spam par messagerie instantanée

Résumé

La Recommandation UIT-T X.1233 contient des lignes directrices à l'intention des fournisseurs et des utilisateurs de services de messagerie instantanée (IM), afin de lutter contre les spams par messagerie instantanée (SPIM), de réduire leur propagation dans le cyberespace et d'améliorer l'expérience des utilisateurs de services de messagerie instantanée.

La présente Recommandation contient une analyse des scénarios de création de SPIM dans la messagerie instantanée, la spécification de mesures techniques et de mécanismes de lutte contre les SPIM à l'intention des fournisseurs de services de messagerie instantanée, ainsi que des lignes directrices sur la lutte contre les SPIM à l'intention des utilisateurs de services de messagerie instantanée.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1233	03-09-2021	17	11.1002/1000/14773

Mots clés

Lutte contre les SPIM, lignes directrices, fournisseur de services de messagerie instantanée, utilisateur de services de messagerie instantanée.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

En raison de l'engouement qu'elles suscitent, les applications de messagerie instantanée (IM) sont devenues un moyen important de diffusion du spam, au même titre que la voix, le service de messages courts (SMS) et le courrier électronique. Grâce à la transmission efficace et en temps réel de messages, la messagerie instantanée facilite considérablement les relations sociales, mais permet également aux spammeurs d'envoyer des spams par messagerie instantanée (SPIM). Le volume de spams publicitaires, de contenus pornographiques et d'autres informations illégales – par exemple les informations de hameçonnage, les virus, les vers de Troie et les logiciels espions – envoyés par messagerie instantanée augmente de manière exponentielle. Cette situation est non seulement constitutive de harcèlement, voire une source de pertes économiques, pour les utilisateurs, mais compromet aussi gravement la sécurité du cyberespace. La lutte contre les SPIM est devenue un élément important de la lutte contre le spam.

Toutefois, les fournisseurs et les utilisateurs de services de messagerie instantanée désireux de lutter contre les SPIM lorsqu'ils gèrent ou utilisent la messagerie instantanée manquent d'orientations, ce qui signifie que les mesures prises pour lutter contre les SPIM n'ont pas été gérées de façon efficace. Il est donc urgent d'élaborer des normes pertinentes, pour guider les opérateurs et les utilisateurs de services de messagerie instantanée lorsqu'ils appliquent des techniques et des mesures de gestion visant à empêcher la diffusion des SPIM.

Recommandation UIT-T X.1233

Lignes directrices relatives à la lutte contre le spam par messagerie instantanée

1 Domaine d'application

La présente Recommandation contient des lignes directrices à l'intention des fournisseurs et des utilisateurs de services de messagerie instantanée, afin de lutter contre les spams par messagerie instantanée (SPIM). Elle traite des scénarios de spam par messagerie instantanée, des mesures techniques et des mécanismes de lutte contre les SPIM à l'intention des fournisseurs de services de messagerie instantanée, ainsi que des mesures d'intervention en cas d'urgence à l'intention des utilisateurs de services de messagerie instantanée, afin de lutter contre les SPIM, etc.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 spam par messagerie instantanée (SPIM) [b-UIT-T X.1244]: spam visant des utilisateurs d'un service de messagerie instantanée.

NOTE – Aux fins de la présente Recommandation, le terme "spam" n'est pas défini.

3.1.2 spimmeur [b-UIT-T X.1244]: expéditeur de SPIM.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 messagerie instantanée (IM): échange de contenus entre un ensemble de participants en temps quasi réel. Les contenus sont généralement des messages de texte courts, mais tel n'est pas nécessairement le cas.

NOTE – Définition fondée sur la norme [b-IETF RFC 3428].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

IM messagerie instantanée (*instant messaging*)

IP protocole Internet (*internet protocol*)

NE opérateur de réseau (*network operator*)

SMS service de messages courts (*short message service*)

SPIM spam par messagerie instantanée (*spam over instant messaging*)

SP fournisseur de services (*service provider*)

5 Conventions

Le terme "doit" indique une exigence à suivre rigoureusement pour se conformer à la présente Recommandation.

Les termes "devrait" et "ne devrait pas" indiquent que, parmi plusieurs possibilités, l'une d'entre elles est recommandée comme étant particulièrement adaptée, sans mentionner ni exclure les autres possibilités, pour indiquer qu'une ligne de conduite donnée est préférée, mais pas nécessairement exigée, ou (dans la forme négative) qu'une possibilité ou une ligne de conduite donnée est déconseillée, sans pour autant être interdite.

Le terme "peut" indique une exigence optionnelle qui est admissible. Ce mot ne signifie pas que la mise en œuvre doit incorporer l'option.

6 Scénarios de spam par messagerie instantanée

Le spam par messagerie instantanée (SPIM) devient un problème majeur pour les services de messagerie instantanée. Le SPIM nuit à la qualité de fonctionnement des systèmes de messagerie instantanée de diverses manières, par exemple le gaspillage des ressources – notamment de la mémoire, de l'unité centrale de traitement, de l'espace de stockage et de la largeur de bande – et peut être à l'origine de graves problèmes, par exemple la propagation de vers et les attaques par déni de service. Les scénarios de création d'un SPIM sont, sans toutefois s'y limiter, les suivants:

– Utilisation de moyens automatisés pour enregistrer un grand nombre de comptes à des fins répréhensibles, telles que la diffusion de SPIM.
– Utilisation du compte sans autorisation du propriétaire du compte, pour établir une connexion à une session avec l'utilisateur cible afin de propager des SPIM.
– Absence de mécanismes de sécurité intégrés, par exemple de mécanisme de confirmation lors de l'adjonction d'amis, ce qui crée un environnement dans lequel les SPIM peuvent se propager rapidement.
– Divulgation de messages sur un canal de fourniture non sécurisé. Les pirates peuvent falsifier des messages instantanés pendant la transmission. Des messages publicitaires ou des codes malveillants peuvent être insérés dans un message, qui est converti en SPIM.
– Des fabricants agissant illégalement proposent des abonnements SPIM aux utilisateurs à des fins commerciales.

7 Lignes directrices à l'intention des fournisseurs de services de messagerie instantanée pour lutter contre les SPIM

7.1 Configuration des fonctions anti-SPIM

Le fournisseur de services de messagerie instantanée doit fournir des fonctions anti-SPIM lorsqu'il fournit un service de messagerie instantanée. Les fonctions anti-SPIM devraient comprendre, sans toutefois s'y limiter, les éléments suivants:

– Détection et commande automatique de l'enregistrement des utilisateurs.
– Contrôle des autorisations lors de l'adjonction d'amis.
– Détection et limitation du taux d'envoi de messages.
– Filtrage des messages fondé sur des listes noires.
– Plate-forme de réclamation des utilisateurs qui dispose, entre autres fonctionnalités, d'un mécanisme de retour d'information simple permettant d'alerter un fournisseur de services de messagerie instantanée sur les SPIM reçus.

Parallèlement, le fournisseur de services de messagerie instantanée doit maintenir les fonctions anti-SPIM lors de l'exploitation. Les scénarios devraient inclure, sans toutefois s'y limiter, les éléments suivants:

– Tenue à jour des bases de données anti-SPIM, telles que les listes d'amis et les listes noires, afin qu'elles soient disponibles et stables.

– Tenue à jour des informations sur les réclamations des utilisateurs, afin d'améliorer la précision de ces informations.

– Ajustement des seuils utilisés dans les fonctions anti-SPIM, par exemple les seuils de restriction du taux d'envoi de messages et du nombre de réclamations qu'un compte peut recevoir avant d'être inscrit sur une liste noire.

7.2 Surveillance et contrôle du comportement

Le fournisseur de services de messagerie instantanée doit prendre des mesures permettant de surveiller les comportements ci-après et de créer des alarmes lorsque des anomalies sont détectées. Les comportements qu'il convient de surveiller sont notamment les suivants (la liste n'est pas exhaustive):

– Comportement d'échec d'authentification: Par exemple, plusieurs demandes d'authentification sont envoyées depuis la même adresse IP. Si ces comportements sont nombreux, il se peut qu'un spimmeur dérobe des comptes pour envoyer des SPIM. Cela devrait déclencher une alarme et les demandes d'authentification ultérieures provenant de cette adresse IP devraient être éliminées.

– Comportement de réclamation malveillante: Par exemple, un compte soumet un grand nombre de réclamations pendant une certaine période que les réclamations concernent différents comptes ou le même compte; si le nombre de réclamations dépasse un certain seuil, cela devrait déclencher une alarme et les réclamations du compte devraient être ignorées, de façon à améliorer la précision des réclamations.

– Comportement d'adjonction malveillante de comptes sur des listes noires: Par exemple, si certains comptes ajoutent un compte donné sur une liste noire, il convient de détecter si ces comptes figurent sur une liste de comptes suspects. Si la plupart des comptes se trouvent sur une liste de comptes suspects, une alarme devrait être déclenchée. Ces tentatives visant à ajouter un compte donné sur une liste noire ne devraient pas être pris en compte dans le calcul du nombre de fois où le compte en question a été ajouté sur une liste noire, de façon à améliorer la précision de la liste noire.

7.3 Audit et enregistrement

Les fournisseurs de services de messagerie instantanée doivent adopter des mesures techniques permettant de vérifier et d'enregistrer les comportements des utilisateurs et les incidents de cybersécurité, afin de lutter contre les SPIM. Les enregistrements que le service de messagerie instantanée devrait vérifier sont notamment les suivants (la liste n'est pas exhaustive):

– Les journaux de comportement de l'utilisateur, comprenant des informations sur le comportement d'enregistrement et des informations sur l'authentification de l'utilisateur. Par exemple, le fournisseur de services de messagerie instantanée devrait enregistrer les actions historiques de l'utilisateur (par exemple, les comportements d'envoi de messages dépassant le seuil des restrictions du taux d'envoi de messages et les comportements de réclamation malveillante). Les journaux de comportement d'envoi de messages devraient comprendre, sans toutefois s'y limiter, les informations suivantes: informations sur le compte de l'expéditeur (par exemple, adresse IP, nom d'utilisateur, présence ou non de l'expéditeur sur une liste suspecte ou une liste noire), informations sur le compte du destinataire, type de relation entre l'expéditeur et le destinataire (par exemple, amis, non-amis, membres amis d'un groupe, membres non-amis d'un groupe, amis d'autres systèmes de messagerie instantanée, contacts téléphoniques). Les fournisseurs de serveurs de messagerie instantanée devraient intégrer l'analyse de ces informations pour identifier les activités suspectes ou malveillantes. Les journaux de comportement de réclamation malveillante devraient inclure, sans toutefois s'y limiter, les informations suivantes: informations du compte du plaignant (par exemple, adresse IP, nom d'utilisateur, présence ou non sur une liste suspecte ou une liste noire),

informations du compte faisant l'objet de la réclamation et nombre de réclamations au cours d'une période donnée. Si le nombre de réclamations dépasse un seuil, les réclamations provenant du compte du plaignant sont ignorées, ce qui améliore la précision de la plate-forme de réclamations.

– Enregistrement de filtrage de SPIM, qui comprend les comportements de filtrage de SPIM et le message filtré. Un enregistrement de comportement de filtrage de SPIM devrait comprendre, sans toutefois s'y limiter, les informations suivantes: compte d'envoi du message filtré (par exemple, adresse IP, nom d'utilisateur, présence ou non sur une liste suspecte ou une liste noire), mesures de filtrage utilisées (par exemple, filtrage sur la base de listes noires, contrôle du taux d'envoi ou contrôle des autorisations). Le message filtré devrait être enregistré, afin de pouvoir être renvoyé en cas d'erreur de filtrage.

7.4 Intervention en cas d'urgence

Un fournisseur de services de messagerie instantanée devrait élaborer un plan d'intervention en cas d'urgence pour faire face aux incidents graves liés aux SPIM.

Les incidents graves liés aux SPIM devraient être pris en compte dans un plan d'intervention en cas d'urgence, qui devrait notamment comprendre les incidents suivants (la liste n'est pas exhaustive):

– Modification, intrusion ou contrôle de la base de données anti-SPIM du serveur de messagerie instantanée.

– Modification, intrusion ou contrôle de la plate-forme de réclamation concernant des SPIM.

– Modification illégale du seuil d'une fonction d'enregistrement automatique.

– Formulation de réclamations à grande échelle contre des SPIM pendant une période donnée.

Un fournisseur de services de messagerie instantanée devrait déterminer le type et le niveau de chacun de ces incidents liés aux SPIM en fonction de la situation réelle et prévoir un processus d'intervention en cas d'urgence ainsi que des lignes directrices opérationnelles d'urgence pour chaque type et chaque niveau d'incident lié aux SPIM.

Un fournisseur de services de messagerie instantanée devrait mettre en place un mécanisme de surveillance et d'alerte pour les incidents graves liés aux SPIM, découvrir les principaux incidents graves de ce type et en informer rapidement le personnel concerné.

Un fournisseur de services de messagerie instantanée devrait également résumer les causes des principaux incidents liés aux SPIM après une intervention en cas d'urgence, évaluer l'efficacité des mesures d'intervention en cas d'urgence et remédier rapidement au problème.

7.5 Gestion de l'évaluation des risques

Les fournisseurs de services de messagerie instantanée devraient évaluer les risques concernant la probabilité et la gravité des incidents liés aux SPIM. La gestion des risques devrait être intégrée aux activités opérationnelles de base, qu'il s'agisse de l'évaluation de la gestion, de l'évaluation de la sécurité ou de l'évaluation fonctionnelle. La gestion de l'évaluation des risques devrait comprendre, sans toutefois s'y limiter, les éléments suivants:

– Un fournisseur de services de messagerie instantanée devrait procéder à une évaluation de la gestion qui devrait consister, par exemple, à élaborer une politique de lutte contre les SPIM et à vérifier si des processus et des stratégies de conformité en matière de sécurité sont en place pour atténuer les risques liés aux SPIM. De plus, cette évaluation devrait faciliter la mise en œuvre de la politique. Un fournisseur de services de messagerie instantanée devrait également examiner et mettre à jour la politique et la procédure actuelles d'évaluation des risques selon une fréquence définie par l'organisation ou chaque fois que des modifications importantes sont apportées au système de messagerie instantanée ou à l'environnement opérationnel.

– Un fournisseur de services de messagerie instantanée devrait procéder à une évaluation de la sécurité qui devrait consister, par exemple, à automatiser le processus de gestion des vulnérabilités au moyen de normes (par exemple, énumération des défauts d'application et des configurations incorrectes et formatage de listes de contrôle et de procédures de test), afin d'identifier la cause la plus probable des SPIM (par exemple, vulnérabilités des mots de passe, réglages de pare-feu non sécurisés et vers de Troie) et quantifier les conditions propices aux incidents graves liés aux SPIM.

– Un fournisseur de services de messagerie instantanée devrait procéder à une évaluation fonctionnelle qui devrait consister, par exemple, à découvrir des traitements illogiques et des erreurs en cascade pouvant résider dans le code d'un système de messagerie instantanée (par exemple, enregistrement automatique de l'utilisateur, taux d'envoi illimité d'un utilisateur pendant une période donnée, absence de mécanismes de sécurité intégrés et divulgation de messages sur un canal de fourniture non sécurisé) lorsque le système de messagerie instantanée est mis à niveau.

– Un fournisseur de services de messagerie instantanée devrait évaluer les risques à intervalles réguliers ou revoir et mettre à jour, au besoin, sa politique d'évaluation des risques. L'évaluation des risques devrait comporter trois éléments interdépendants: l'évaluation de la gestion, l'évaluation de la sécurité et l'évaluation fonctionnelle. Ainsi, l'évaluation de la gestion et l'évaluation de la sécurité devraient être effectuées en même temps que l'évaluation générale des risques, et l'évaluation fonctionnelle devrait être effectuée avant la mise à niveau d'un système de messagerie instantanée, pendant la mise à niveau de ce système, ou pendant les deux opérations. Parallèlement, un fournisseur de services de messagerie instantanée devrait soit remédier aux failles légitimes dans les temps d'intervention définis par l'organisation, soit mettre en place des contrôles pour empêcher le spimmeur d'exploiter la vulnérabilité.

7.6 Mesures de protection de la sécurité

Un fournisseur de services de messagerie instantanée devrait prendre des mesures de protection de la sécurité pour lutter contre les SPIM. Les mesures de protection de la sécurité devraient notamment être les suivantes (la liste n'est pas exhaustive):

– Un fournisseur de services de messagerie instantanée devrait déployer des mesures de lutte contre les attaques par déni de service réparti pour protéger la bibliothèque de listes noires, la plate-forme de réclamations et les méthodes de surveillance et d'audit de la sécurité et pour améliorer la disponibilité des fonctions anti-SPIM.

– Un fournisseur de services de messagerie instantanée devrait déployer des mesures antivirus, anti-chevaux de Troie et anti-vers pour empêcher le serveur d'être infecté et contrôlé par des spimmeurs susceptibles de modifier les configurations anti-SPIM ou de désactiver les fonctions anti-SPIM et d'envoyer ensuite des SPIM.

– Un fournisseur de services de messagerie instantanée devrait mettre en œuvre plusieurs méthodes de contrôle d'accès au niveau des limites du réseau, des systèmes et des applications du système de messagerie instantanée, afin d'empêcher tout accès non autorisé par des spimmeurs susceptibles de modifier les configurations anti-SPIM ou de désactiver les fonctions anti-SPIM et d'envoyer ensuite des SPIM.

– Un fournisseur de services de messagerie instantanée devrait déployer des méthodes de détection et de protection contre les intrusions pour détecter les attaques du réseau et empêcher l'intrusion dans le système de messagerie instantanée de spimmeurs susceptibles de modifier la configuration ou de désactiver les fonctions anti-SPIM et d'envoyer ensuite des SPIM.

8 Fonctionnalité des utilisateurs de la messagerie instantanée pour prendre en charge la lutte contre les SPIM

Un utilisateur de la messagerie instantanée devrait avoir la possibilité de configurer le client de la messagerie instantanée pour se prémunir contre les SPIM lorsqu'il utilise un système de messagerie instantanée. La configuration devrait inclure, sans toutefois s'y limiter, les éléments suivants. Un utilisateur de la messagerie instantanée devrait avoir la possibilité:

– d'utiliser un mécanisme de confirmation de la vérification, y compris de confirmation des demandes d'authentification et la confirmation des adjonctions au groupe, pour s'assurer que toutes les actions sont approuvées par l'utilisateur;

– de configurer les réglages, de façon à ne pas autoriser la réception de messages ou de fichiers provenant d'utilisateurs non autorisés;

– de configurer une liste noire en temps utile, et de ne pas autoriser la réception de messages ou de fichiers provenant de comptes suspects;

– d'utiliser un mot de passe fort et de le changer régulièrement, pour éviter que le compte soit volé et utilisé pour envoyer des SPIM;

– de surveiller l'exécution des fonctions privilégiées, désactiver et modifier les réglages mis en œuvre s'ils sont susceptibles de provoquer des SPIM (par exemple, accepter la demande d'authentification d'un inconnu).

9 Lignes directrices à l'intention des fournisseurs de services ou opérateurs de réseau concernant la lutte contre les SPIM

Les fournisseurs de services ou opérateurs de réseau (SP/NE) peuvent contribuer à la lutte contre les SPIM en recourant à des moyens tels que la création d'une plate-forme unifiée de réclamations contre les SPIM, la mise en place d'une base de données unifiée de listes noires pour empêcher la diffusion de SPIM, les tests et la vérification des fonctions anti-SPIM d'un système de messagerie instantanée et la fourniture de services de détection des SPIM à l'intention des fournisseurs de services de messagerie instantanée. Cela inclut notamment, mais pas exclusivement, les éléments suivants:

– Les SP/NE devraient créer une plate-forme unifiée de réclamations pour plusieurs services de messagerie instantanée. La plate-forme de réclamations peut accepter les réclamations des utilisateurs concernant un compte envoyant des SPIM, et classer les réclamations en fonction des différents services de messagerie instantanée. Lorsque le nombre de réclamations d'utilisateurs contre un compte de messagerie instantanée atteint un certain seuil, les informations détaillées sur le compte de messagerie instantanée sont envoyées à la base de données correspondante des listes noires du service de messagerie instantanée.

– Les SP/NE devraient créer une base de données unifiée de listes noires pour plusieurs services de messagerie instantanée. La base de données de listes noires est synchronisée avec la base de données de listes noires de chaque service de messagerie instantanée dans le réseau. Il existe deux sources pour la liste noire, les comptes figurant dans la base de données pouvant être:

  • les comptes faisant l'objet des réclamations par le biais de la plate-forme de réclamations susmentionnée;

  • les comptes détectés comme émettant des SPIM par le service de détection de SPIM.

– Les SP/NE devraient fournir un service régulier de vérification du test de numérotation aux fournisseurs de services de messagerie instantanée, afin d'éviter que les fonctions anti-SPIM d'un système de messagerie instantanée ne soient désactivées, éventuellement par suite d'une attaque de pirates. Si la fonction correspondante n'est pas activée après la vérification, un SP/NE peut envoyer une alarme au fournisseur de services de messagerie instantanée. Les

fonctions de vérification du test de numérotation consistent notamment, mais non exclusivement, à simuler:

- le comportement d'enregistrement automatique et à vérifier que le système de messagerie instantanée peut identifier et empêcher l'enregistrement automatique;
- un compte envoyant plusieurs messages pendant une unité de temps (le nombre de messages dépasse le seuil fixé par le système de messagerie instantanée), et à vérifier que le système de messagerie instantanée peut détecter et rejeter les messages envoyés par le compte par la suite;
- un compte inscrit sur une liste noire envoyant un message, et à vérifier que le système de messagerie instantanée peut rejeter les messages envoyés par ce compte;
- des réclamations malveillantes et à vérifier que le système de messagerie instantanée peut les identifier et les rejeter.

– Les SP/NE peuvent fournir un service de détection des SPIM aux fournisseurs de services de messagerie instantanée. Ils devraient signer un accord de niveau de service avec chaque fournisseur de services de messagerie instantanée, qui devrait inclure des conditions de confidentialité afin de protéger la vie privée des utilisateurs. Le processus de détection des SPIM offert par les SP/NE consiste:

- à déployer des systèmes de détection aux nœuds principaux du réseau, et à détecter l'en-tête du paquet du message de messagerie instantanée avec l'autorisation d'un fournisseur de services de messagerie instantanée;
- à analyser le comportement de l'envoi de plusieurs messages de messagerie instantanée par un compte de messagerie instantanée. Si le nombre de messages envoyés par le compte de messagerie instantanée pendant un laps de temps donné dépasse un certain seuil, on peut déterminer que le compte envoie des SPIM;
- à rejeter directement les messages de messagerie instantanée envoyés par le compte mentionné ci-dessus;
- à inclure le compte mentionné ci-dessus dans la base de données de listes noires.

Grâce à un service de détection des SPIM fourni par les SP/NE, les SPIM peuvent être détectés et rejetés à la périphérie proche, ce qui permet non seulement d'économiser la largeur de bande du réseau, mais aussi d'éviter de consommer les ressources du serveur de messagerie instantanée.

Bibliographie

[b-UIT-T X.1244] Recommandation UIT-T X.1244 (2008), *Aspects généraux de la lutte contre le spam dans les applications multimédias IP*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging (Protocole d'initiation de session (SIP), Extension pour la messagerie instantanée)*. Disponible à l'adresse: https://tools.ietf.org/html/rfc3428 [consultée le 09/10/2021]

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2022