Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports,
de l'énergie et de la communication

Office fédéral de la communication OFCOM

Annexe 1.12 de l'ordonnance de l'OFCOM du 9 décembre 1997 sur les services de télécommunication et les ressources d'adressage (RS 784.101.113/1.12

Prescriptions techniques et administratives

concernant

la manipulation non autorisée d'installations de télécommunication au moyen de techniques de transmission des télécommunications

1ère édition: 23.11.2022

Entrée en vigueur: 01.01.2023

Table des matières

1. Généralités

1.1 Champ d'application

Les présentes prescriptions techniques et administratives (PTA) constituent l'annexe 1.12 de l'ordonnance de l'OFCOM du 9 décembre 1997 sur les services de télécommunication et les ressources d'adressage [3]. Elles se fondent sur l'art. 48*a* de la loi du 30 avril 1997 sur les télécommunications (LTC) [1] et sur l'art. 105, al. 1, de l'ordonnance du 9 mars 2007 sur les services de télécommunication (OST) [2]. Elles concrétisent la réglementation prévue aux art. 96*a* à 96*c* OST. Elles s'adressent aux fournisseurs d'accès à Internet via des réseaux fixes et mobiles et règlent les mesures de sécurité ainsi que le service de signalement en lien avec la manipulation non autorisée d'installations de télécommunication au moyen de techniques de transmission des télécommunications.

1.2 Références

[1] RS 784.10
Loi sur les télécommunications du 30 avril 1997 (LTC)

[2] RS 784.101.1
Ordonnance du 9 mars 2007 sur les services de télécommunication (OST)

[3] RS 784.101.113
Ordonnance de l'OFCOM du 9 décembre 1997 sur les services de télécommunication et les ressources d'adressage

[4] M3AAWG Best Common Practices for the Use of a Walled Garden, Version 2.0

[5] M3AAWG Recommendation Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction (2005)

[6] IETF RFC 2827, BCP 38 (Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, may 2000)

[7] IETF RFC 3704, BCP 84 (Ingress Filtering for Multihomed Networks, march 2004)

[8] NIST Cryptographic Standards and Guidelines SP 800-175B Rev. 1 (Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms)

Les PTA ainsi que les plans de numérotation sont publiés sur le site internet www.ofcom.admin.ch et peuvent être obtenus auprès de l'OFCOM, rue de l'Avenir 44, case postale 256, CH-2501 Biel/Bienne.

Les documents du *Messaging, Malware and Mobile Anti-Abuse Working Group* (M3AWG) peuvent être téléchargés sur le site internet www.m3aawg.org.

Les documents de l'*Internet Engineering Task Force* (IETF) peuvent être téléchargés sur le site internet www.rfc-editor.org.

Les standards du *National Institute of Standards and Technology* (NIST) peuvent être téléchargés sur le site internet www.nist.gov.

1.3 Abréviations

BCP	Best Current Practices
CERT	Computer Emergency Response Team
DDoS	Distributed denial of service
IAP	Internet Access Provider
IETF	Internet Engineering Task Force
IP	Internet Protocol
M3AAWG	Messaging, Malware and Mobile Anti-Abuse Working Group
NCSC	Nationales Zentrum für Cybersicherheit
NIST	National Institute of Standards and Technology

RFC Requests For Comments

2. Mesures de sécurité

2.1 Blocage ou restriction de l'utilisation des accès à Internet

Lorsqu'ils bloquent ou restreignent l'utilisation des accès à Internet en vertu de l'art. 96*a*, al. 1, OST [2], les fournisseurs d'accès à Internet respectent les exigences suivantes:

1. Ils veillent à renoncer à un blocage ou à une restriction d'utilisation des accès à Internet en raison de manipulations non autorisées s'ils savent que l'accès en question fait l'objet d'un mandat de surveillance du Service Surveillance de la correspondance par poste et télécommunication (Service SCPT). Ils prennent contact avec le Service SCPT.
2. Ils informent immédiatement leurs clients, par un ou plusieurs canaux appropriés (p. ex. SMS, courriel, lettre, centre clientèle, appel, "page Splash", etc.), de la mise en place du blocage ou de la restriction de l'utilisation de l'accès à Internet.
3. Ils peuvent par exemple utiliser une "sandbox" ("walled garden") en cas de blocage ou de restriction de l'utilisation d'un accès à Internet. Dans ce cas, ils respectent les "Best Common Practices" du M3AAWG [4].
4. Ils bloquent par défaut les connexions TCP sortantes sur le port 25 (SMTP) pour les connexions à Internet des clients privés ou ceux qui disposent d'une adresse IP dynamique. Ils permettent aux clients de débloquer individuellement le port 25 TCP et respectent les "Best Common Practices" du M3AAWG [5].

2.2 Blocage ou restriction de l'utilisation de ressources d'adressage

Lorsqu'ils bloquent ou restreignent l'utilisation de ressources d'adressage en vertu de l'art. 96*a*, al. 1, OST [2], les fournisseurs d'accès à Internet respectent les exigences suivantes:

1. Ils veillent à renoncer à un blocage ou à une restriction d'utilisation de ressources d'adressage en raison de manipulations non autorisées, s’ils savent que la ressource d'adressage en question fait l'objet d'un mandat de surveillance du Service Surveillance de la correspondance par poste et télécommunication (Service SCPT). Ils prennent contact avec le Service SCPT.
2. Au sens de l'art. 48*a* LTC [1], les blocages servent à lutter contre toute manipulation non autorisée d'installations de télécommunication par des transmissions au moyen de techniques de télécommunication (notamment par des logiciels malveillants, des attaques DDoS, des spams, des "exploits" et de l’hameçonnage).
3. Pour les blocages, les fournisseurs d'accès à Internet peuvent obtenir des informations pertinentes sur les infrastructures utilisées par des acteurs criminels auprès du NCSC, conformément aux bases juridiques applicables à celui-ci.

2.3 Attaques DDoS

Afin de lutter contre les attaques DDoS conformément à l'art. 96*a*, al. 2, OST [2], les fournisseurs d'accès à Internet filtrent les paquets IP provenant de leurs réseaux avec une adresse IP source falsifiée. Pour mettre en place ce filtrage, ils tiennent une liste actualisée des réseaux autorisés, générée à partir de la table de routage, conformément aux "Best Current Practices" de l'IETF (BCP 38 [6] pour les réseaux avec des appareils à adresse IP unique; BCP 84 [7] pour les réseaux avec des appareils à adresses IP multiples).

2.4 Configuration des installations de télécommunication, qui sont mises à la disposition des clients

Lorsqu’ils configurent et actualisent les caractéristiques de sécurité des installations de télécommunication qu'ils mettent à la disposition de leurs clients conformément à l'art. 96*a*, al. 3, OST [2], les fournisseurs d'accès à Internet respectent les exigences suivantes:

1. Aucune donnée d'accès standard (nom d'utilisateur, mot de passe) ne doit être utilisée pour l'accès à ces installations de télécommunication. Les données d'accès doivent être attribuées individuellement pour chaque installation de télécommunication. Si cela n'est pas possible, un changement des données d'accès doit être imposé techniquement lors de la mise en service de l'installation de télécommunication.
2. A la livraison d'une installation de télécommunication, les services non utilisés par les clients ou par le fournisseur d'accès à Internet doivent être désactivés par défaut afin de réduire au maximum la surface d'attaque de l'installation de télécommunication. Si un service est requis par les clients ou pour l'exploitation par le fournisseur d'accès à Internet, ce dernier doit permettre aux clients de l'activer eux-mêmes ou l'activer pour eux à leur demande.
3. A la livraison d'une installation de télécommunication, aucun port librement accessible depuis Internet ne doit être ouvert. Les ports ouverts nécessaires à l'exploitation, à la télémaintenance ou à la fourniture de prestations par le fournisseur d'accès à Internet doivent être sécurisés par des mesures techniques (p. ex. restriction IP).
4. Tant qu'ils exercent un contrôle technique sur une installation de télécommunication, les fournisseurs d'accès à Internet ont en outre les obligations suivantes:
    a. Le protocole utilisé pour la télémaintenance de l'installation de télécommunication par le fournisseur d'accès à Internet doit être protégé par une technologie de cryptage moderne, conformément aux Cryptographic Standards and Guidelines actuels de l'US NIST [8].
    b. Dès que des mises à jour de sécurité considérées comme critiques par le fabricant ou les fournisseurs d'accès à Internet sont disponibles, les installations de télécommunication concernées doivent être actualisées sans délai après une phase de test réussie. La phase de test doit être suffisamment courte pour ne pas augmenter de manière significative le risque d'exploitation de la faille de sécurité. Toutes les autres mises à jour de sécurité doivent être installées dans un délai correspondant à leur degré d'urgence. Si plus aucune mise à jour de sécurité n'est mise à disposition, les installations de télécommunication doivent être remplacées conformément à l'art. 96*a*, al. 3, let. b, OST.

3. Service de signalement

Les fournisseurs d'accès à Internet exploitent leur service chargé de recevoir les signalements de manipulations non autorisées d'installations de télécommunication conformément à l'art. 96*b* OST [2] en respectant les exigences suivantes:

1. Le service reçoit les signalements de la part de tiers (p. ex. d'autres fournisseurs de services de télécommunication suisses et étrangers, de CERT étrangers, d'autorités étatiques, de clients) concernant des manipulations non autorisées d'installations de télécommunication qui touchent à la sécurité technique des installations et prend les mesures défensives appropriées dans un délai raisonnable.
2. Les signalements de manipulation adressés par des clients du fournisseur d'accès à Internet peuvent continuer à être envoyés via les points de contact traditionnels (p. ex. hotline, service-desk, etc.).
3. Pour chaque bloc d'adresses IP attribué, les fournisseurs d’accès à Internet doivent enregistrer auprès du "registre Internet régional" (RIR) compétent une adresse électronique ("abuse-c") qui remplit la fonction de service de signalement. Sinon, ils doivent indiquer une adresse électronique générale pour les questions techniques ("tech-c") et s'assurer que ce contact peut remplir la fonction de service de signalement.
4. Ils configurent leurs filtres anti-spam de messagerie de manière à ce que les signalements de manipulation ne soient pas triés.

Biel/Bienne, le 23 novembre 2022

Office fédéral de la communication (OFCOM)

Bernard Maissen, directeur