Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Ufficio federale delle comunicazioni UFCOM

Allegato 1.12 dell'ordinanza dell'UFCOM del 9 dicembre 1997 sui servizi di telecomunicazione e gli elementi d'indirizzo (RS 784.101.113/1.12)

Prescrizioni tecniche e amministrative

relative

a manipolazioni non autorizzate di impianti di telecomunicazione commesse con trasmissione mediante telecomunicazione

Edizione 2: 09.11.2023

Entrata in vigore: 01.03.2024

Indice

1. In generale

1.1 Campo d'applicazione

Le presenti prescrizioni tecniche e amministrative (PTA) costituiscono l'allegato 1.12 dell'ordinanza dell'UFCOM del 9 dicembre 1997 sui servizi di telecomunicazione e gli elementi d'indirizzo [3]. Si fondano sull'articolo 48*a* della legge del 30 aprile 1997 sulle telecomunicazioni (LTC) [1] e sull'articolo 105 capoverso 1 dell'ordinanza del 9 marzo 2007 sui servizi di telecomunicazione (OST) [2]. Attuano la regolamentazione prevista agli articoli 96*a*–96*c* OST. Queste PTA si rivolgono ai fornitori di accesso a Internet tramite reti fisse e mobili (IAP, Internet Access Provider) e disciplinano le misure di sicurezza e la centrale di segnalazione in relazione alla manipolazione non autorizzata degli impianti di telecomunicazione commessa con trasmissione mediante telecomunicazione.

1.2 Riferimenti

[1] RS 784.10
Legge del 30 aprile 1997 sulle telecomunicazioni (LTC)

[2] RS 784.101.1
Ordinanza del 9 marzo 2007 sui servizi di telecomunicazione (OST)

[3] RS 784.101.113
Ordinanza dell'UFCOM del 9 dicembre 1997 sui servizi di telecomunicazione e gli elementi d'indirizzo

[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)

Le PTA sono consultabili sul sito internet www.ufcom.admin.ch e sono ottenibili presso l'UFCOM, rue de l'Avenir 44, casella postale 256, CH-2501 Biel/Bienne.

I documenti del *Messaging, Malware and Mobile Anti-Abuse Working Group* (M3AWG) possono essere consultati sul sito Internet www.m3aawg.org.

I documenti dell'Internet *Engineering Task Force* (IETF) possono essere consultati sul sito Internet www.rfc-editor.org.

Gli standard del *National Institute of Standards and Technology* (NIST) possono essere consultati sul sito Internet www.nist.gov.

1.3 Abbreviazioni

CENAL	Centrale nazionale d'allarme
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	Centro nazionale per la cibersicurezza
NIST	National Institute of Standards and Technology
RFC	Requests For Comments

2. Misure di sicurezza

2.1 Blocco o limitazione dell'uso di accessi a Internet

Quando bloccano o limitano l'uso di accessi a Internet ai sensi dell'articolo 96*a* capoverso 1 OST [2], gli IAP osservano i seguenti requisiti:

1. Garantiscono che il blocco o la limitazione dell'uso degli accessi a Internet a causa di manipolazioni non autorizzate non venga applicato qualora l'accesso Internet corrispondente sia oggetto di un ordine di sorveglianza da parte del Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT) e gli IAP stessi siano stati informati in tal senso dal servizio SCPT.
2. Quando attuano il blocco o la limitazione dell'uso dell'accesso a Internet, informano immediatamente i propri clienti attraverso uno o più canali adeguati (ad esempio SMS, e-mail, lettera, centro clienti, telefonata, "splash page", ecc.)
3. In caso di blocco o limitazione dell'uso di un accesso a Internet possono utilizzare una "sandbox" ("walled garden"). In questo caso, gli IAP seguono le "Best Common Practices" dell'M3AAWG [4].
4. Per impostazione predefinita, bloccano le connessioni TCP in uscita sulla porta 25 (SMTP) per le connessioni Internet dei clienti privati o di quelli che hanno un indirizzo IP dinamico. Consentono ai clienti di attivare individualmente la porta 25 TCP e osservano le "Best Common Practices" dell'M3AAWG [5].

2.2 Blocco o limitazione dell'uso di elementi d'indirizzo

Quando bloccano o limitano l'uso di elementi d'indirizzo ai sensi dell'articolo 96*a* capoverso 1 OST [2] gli IAP osservano i seguenti requisiti:

1. Garantiscono che il blocco o la limitazione dell'uso degli accessi a Internet a causa di manipolazioni non autorizzate non venga applicato qualora l'accesso Internet corrispondente sia oggetto di un ordine di sorveglianza da parte del Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT) e gli IAP stessi siano stati informati in tal senso dal servizio SCPT.
2. Ai sensi dell'articolo 48a LTC [1] i blocchi servono a lottare contro qualsiasi manipolazione non autorizzata degli impianti di telecomunicazione effettuata attraverso la trasmissione mediante telecomunicazione (soprattutto attraverso malware, attacchi DDoS, spam, exploit e phishing).
3. A fini di blocco, gli IAP possono ottenere informazioni pertinenti sulle infrastrutture utilizzate da attori criminali dall'NCSC, conformemente alle basi giuridiche ad esso applicabili.

2.3 Attacchi DDoS

Per combattere gli attacchi DDoS secondo l'articolo 96*a* capoverso 2 OST [2], gli IAP filtrano i pacchetti IP con un indirizzo IP sorgente falsificato provenienti dalle loro reti. Per impostare i filtri di ingresso corrispondenti, tengono un elenco aggiornato delle reti autorizzate, che vengono generate dalla tabella di routing secondo le "Best Current Practices" dell'IETF (BCP 38 [6] per le reti con dispositivi con un unico indirizzo IP; BCP 84 [7] per le reti con dispositivi con più indirizzi IP).

2.4 Configurazione degli impianti di telecomunicazione messi a disposizione dei clienti

Gli IAP configurano e aggiornano i parametri di sicurezza degli impianti di telecomunicazione che mettono a disposizione dei loro clienti conformemente all'articolo 96*a* capoverso 3 OST [2], nel rispetto dei seguenti requisiti:

1. Per accedere a tali impianti di telecomunicazione non si possono utilizzare dati di accesso standard (nome utente, password). I dati di accesso devono essere assegnati individualmente per ogni impianto di telecomunicazione. Se questo non è possibile, quando l'impianto viene messo in funzione, occorre forzare tecnicamente un cambiamento dei dati di accesso.

2. Allo stato di consegna, un impianto di telecomunicazione deve avere disattivati per impostazione predefinita i servizi non richiesti dai clienti o dall'IAP al fine di ridurre al minimo la sua superficie di attacco. Se i clienti o l'IAP dovessero necessitare di un servizio, l'IAP deve consentire ai clienti di attivarlo autonomamente o deve farlo per loro.
3. Allo stato di consegna, un impianto di telecomunicazioni non deve avere porte accessibili liberamente da Internet. Le porte aperte necessarie per l'esercizio da parte dell'IAP, la manutenzione remota o la fornitura di servizi da parte dell'IAP devono essere protette da misure tecniche (ad es. restrizione IP).
4. Fintanto che esercitano il controllo tecnico su un impianto di telecomunicazione, gli IAP hanno i seguenti obblighi:
   a. Il protocollo utilizzato per la manutenzione a distanza dell'impianto di telecomunicazione da parte dell'IAP deve essere protetto da una tecnologia di crittografia aggiornata in conformità con gli attuali Cryptographic Standards and Guidelines dell'US NIST [8].
   b. Non appena sono disponibili aggiornamenti di sicurezza classificati come critici dal fabbricante o dall'IAP, gli impianti di telecomunicazione interessati devono essere aggiornati immediatamente dopo il completamento di una fase di test con esito positivo. La fase di test deve essere sufficientemente breve da non aumentare significativamente il rischio di sfruttamento della vulnerabilità. Tutti gli altri aggiornamenti di sicurezza devono essere installati entro un periodo corrispondente alla loro urgenza. Se non sono più disponibili aggiornamenti di sicurezza, gli impianti di telecomunicazione devono essere sostituiti ai sensi dell'articolo 96*a* capoverso 3 lettera b OST.

3. Servizio di segnalazione

Gli IAP gestiscono il loro servizio specializzato che riceve le segnalazioni di manipolazioni non autorizzate di impianti di telecomunicazione ai sensi dell'articolo 96*b* OST [2], nel rispetto delle seguenti esigenze:

1. Il servizio di segnalazione riceve le segnalazioni di terzi (ad es. altri fornitori di servizi di telecomunicazione nazionali ed esteri, CERT stranieri, autorità statali, clienti) relative a manipolazioni non autorizzate di impianti di telecomunicazione che incidono sulla sicurezza tecnica degli impianti e avvia le opportune misure di difesa entro un periodo di tempo ragionevole.
2. Le segnalazioni dei clienti dell'IAP possono continuare a essere effettuate tramite i punti di contatto convenzionali (ad es. hotline, service desk, ecc.).
3. Per ogni serie di indirizzi IP assegnata, gli IAP devono depositare un indirizzo elettronico ("abuse-c") presso il "Regional Internet Registry" (RIR) competente, che svolge la funzione di servizio di segnalazione. Alternativamente devono depositare un indirizzo elettronico generale per le domande tecniche ("tech-c") e garantire che questo punto di contatto possa svolgere la funzione di servizio di segnalazione.
4. Configurano i filtri antispam per le loro e-mail in modo che i messaggi di manipolazione non vengano smistati.

(RS 784.101.113/1.12

Biel/Bienne, il 24 gennaio 2024

Ufficio federale delle comunicazioni (UFCOM)

Maissen Bernard T3OS5O
24.01.2024

Info: admin.ch/esignature | validator.ch

Bernard Maissen
Direttore