Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM

Anhang 1.12 der Verordnung des BAKOM vom 9. Dezember 1997 über Fernmeldedienste und Adressierungselemente (SR 784.101.113/)

Technische und administrative Vorschriften

betreffend

Unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen

Ausgabe 2	09.11.2023
Inkrafttreten:	01.03.2024

Inhalt

1. Allgemeines ... 3
1.1 Geltungsbereich ... 3
1.2 Referenzen ... 3
1.3 Abkürzungen ... 3
2. Sicherheitsmassnahmen ... 4
2.1 Sperrung oder Nutzungseinschränkung von Internetzugängen ... 4
2.2 Sperrung oder Nutzungseinschränkung von Adressierungselementen ... 4
2.3 DDoS-Angriffe ... 4
2.4 Konfiguration der Fernmeldeanlagen, die den Kundinnen und Kunden zur Verfügung gestellt werden ... 4
3. Meldestelle ... 5

1. Allgemeines

1.1 Geltungsbereich

Die vorliegenden technischen und administrativen Vorschriften (TAV) bilden Anhang 1.12 der Verordnung des BAKOM vom 9. Dezember 1997 über Fernmeldedienste und Adressierungselemente [3]. Sie stützen sich auf Artikel 48*a* des Fernmeldegesetzes vom 30. April 1997 (FMG) [1] und Artikel 105 Absatz 1 der Verordnung vom 9. März 2007 über Fernmeldedienste (FDV) [2] und konkretisieren die in Artikel 96*a*–96*c* FDV vorgesehene Regelung. Die TAV richten sich an die Anbieterinnen von Internetzugängen über Fest- und Mobilfunknetze (IAP, Internet Access Provider) und regeln die Sicherheitsmassnahmen sowie die Meldestelle im Zusammenhang mit der unbefugten Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen.

1.2 Referenzen

[1] SR 784.10
Fernmeldegesetz vom 30. April 1997 (FMG)

[2] SR 784.101.1
Verordnung vom 9. März 2007 über Fernmeldedienste (FDV)

[3] SR 784.101.113
Verordnung des BAKOM vom 9. Dezember 1997 über Fernmeldedienste und Adressierungselemente

[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)

Die TAV sind auf der Website www.bakom.admin.ch abrufbar. Sie können ebenfalls beim BAKOM, Zukunftstrasse 44, Postfach 252, CH-2501 Biel bezogen werden.

Die Dokumente der *Messaging, Malware and Mobile Anti-Abuse Working Group* (M3AWG) können auf der Website www.m3aawg.org heruntergeladen werden.

Die Unterlagen der *Internet Engineering Task Force* (IETF) stehen unter dem Link www.rfc-editor.org zum Download zur Verfügung.

Die Standards des *National Institute of Standards and Technology* (NIST) können auf der Website www.nist.gov abgerufen werden.

1.3 Abkürzungen

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. Sicherheitsmassnahmen

2.1 Sperrung oder Nutzungseinschränkung von Internetzugängen

Bei der Sperrung oder Nutzungseinschränkung von Internetzugängen gemäss Artikel 96*a* Absatz 1 FDV [2] beachten die IAP folgende Anforderungen:

1. Sie stellen sicher, dass auf eine Sperrung oder Nutzungseinschränkung von Internetzugängen aufgrund von unbefugten Manipulationen im Einzelfall verzichtet wird, sofern der entsprechende Internetzugang Gegenstand eines Überwachungsauftrags des Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ist, und sie vom Dienst ÜPF entsprechend instruiert wurden.
2. Sie informieren ihre Kundinnen und Kunden bei der Implementierung der Sperrung oder Nutzungseinschränkung des Internetzugangs unverzüglich über einen oder mehrere geeignete Kanäle (z.B. SMS, E-Mail, Brief, Kundencenter, Anruf, «Splash-Seite» etc.).
3. Sie können bei einer Sperrung oder Nutzungseinschränkung eines Internetanschlusses beispielsweise eine «Sandbox» («Walled Garden») verwenden. In diesem Falle beachten die IAP die «Best Common Practices» der M3AAWG [4].
4. Sie blockieren standardmässig ausgehende TCP-Verbindungen auf Port 25 (SMTP) für Internetanschlüsse von Privatkundinnen und –kunden oder solche, welche über eine dynamische IP-Adresse verfügen. Sie ermöglichen den Kundinnen und Kunden eine individuelle Freischaltung des Port 25 TCP und beachten die «Best Common Practices» der M3AAWG [5].

2.2 Sperrung oder Nutzungseinschränkung von Adressierungselementen

Bei der Sperrung oder Nutzungseinschränkung von Adressierungselementen gemäss Artikel 96*a* Absatz 1 FDV [2] beachten die IAP folgende Anforderungen:

1. Sie stellen sicher, dass auf eine Sperrung oder Nutzungseinschränkung von Internetzugängen aufgrund von unbefugten Manipulationen im Einzelfall verzichtet wird, sofern der entsprechende Internetzugang Gegenstand eines Überwachungsauftrags des Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ist, und sie vom Dienst ÜPF entsprechend instruiert wurden.
2. Im Sinne von Artikel 48*a* FMG [1] dienen Sperrungen der Bekämpfung von unbefugten Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragungen (insbesondere durch Malware, DDoS-Angriffe, Spam, Exploits und Phishing).
3. Für Sperrungen können die IAP entsprechende Informationen über von kriminellen Akteuren genutzte Infrastrukturen beim NCSC gemäss den auf dieses anwendbaren Rechtsgrundlagen beziehen.

2.3 DDoS-Angriffe

Um DDoS-Angriffe gemäss Artikel 96*a* Absatz 2 FDV [2] zu bekämpfen, filtern die IAP aus ihren Netzwerken stammende IP-Pakete mit gefälschter Quell-IP-Adresse. Zur Einrichtung der entsprechenden Ingress-Filter führen sie eine aktuelle Liste der berechtigten Netze, welche aus der Routingtabelle gemäss den «Best Current Practices» der IETF generiert werden (BCP 38 [6] bei Netzwerken mit Geräten mit einer IP-Adresse; BCP 84 [7] bei Netzwerken mit Geräten mit mehreren IP-Adressen).

2.4 Konfiguration der Fernmeldeanlagen, die den Kundinnen und Kunden zur Verfügung gestellt werden

Die IAP konfigurieren und aktualisieren die Sicherheitseigenschaften der Fernmeldeanlagen, die sie gemäss Artikel 96*a* Absatz 3 FDV [2] ihren Kundinnen und Kunden zur Verfügung stellen, unter Einhaltung der folgenden Anforderungen:

1. Für den Zugriff auf solche Fernmeldeanlagen dürfen keinerlei Standardzugangsdaten (Benutzername, Passwort) verwendet werden. Die Zugangsdaten sind individuell pro Fernmeldeanlage zu vergeben. Falls dies nicht möglich ist, muss bei der Inbetriebnahme der Fernmeldeanlage ein Wechsel der Zugangsdaten technisch erzwungen werden.
2. Im Auslieferungszustand einer Fernmeldeanlage müssen von den Kundinnen und Kunden oder den IAP nicht benötigte Dienste standardmässig deaktiviert sein, um die Angriffsoberfläche der Fernmeldeanlage möglichst gering zu halten. Sollte ein Dienst von den Kundinnen und Kunden oder für den Betrieb durch die IAP benötigt werden, muss die IAP es den Kundinnen und Kunden erlauben, ihn selbst zu aktivieren oder ihn auf Wunsch der Kundinnen und Kunden für diese aktivieren.
3. Im Auslieferungszustand einer Fernmeldeanlage dürfen keinerlei vom Internet her frei erreichbaren Ports offen sein. Für den Betrieb durch die IAP, die Fernwartung oder die Bereitstellung von Dienstleistungen durch die IAP nötige offene Ports müssen durch technische Massnahmen (z. B. IP-Einschränkung) abgesichert werden.
4. Solange sie die technische Kontrolle über eine Fernmeldeanlage ausüben, haben die IAP zudem die folgenden Pflichten:
   a. Das für die Fernwartung der Fernmeldeanlage durch die IAP verwendete Protokoll ist durch eine zeitgemässe Verschlüsselungstechnologie gemäss den aktuellen Cryptographic Standards and Guidelines der US NIST [8] zu schützen.
   b. Sobald vom Hersteller oder den IAP als kritisch eingestufte Sicherheitsupdates verfügbar sind, müssen die betroffenen Fernmeldeanlagen nach Abschluss einer erfolgreichen Testphase unverzüglich aktualisiert werden. Die Testphase ist so kurz zu halten, dass sich das Risiko eines erfolgreichen Ausnützens der Sicherheitslücke nicht signifikant erhöht. Alle anderen Sicherheitsupdates müssen innert einer Frist installiert werden, die ihrer Dringlichkeit entspricht. Werden keine Sicherheitsupdates mehr zur Verfügung gestellt, so sind die Fernmeldeanlagen gemäss Artikel 96*a* Absatz 3 Buchstabe b FDV auszutauschen.

3. Meldestelle

Die IAP betreiben ihre Stelle, die Meldungen über unbefugte Manipulationen von Fernmeldeanlagen gemäss Artikel 96*b* FDV [2] entgegennimmt, unter Einhaltung der folgenden Anforderungen:

1. Die Meldestelle nimmt Meldungen von Dritten (z.B. andere in- und ausländische Fernmeldedienstanbieterinnen, ausländische CERTs, staatliche Behörden, Kundinnen und Kunden) über unbefugte Manipulationen von Fernmeldeanlagen, welche die technische Sicherheit von Anlagen. betreffen, entgegen und leitet innert angemessener Frist geeignete Abwehrmassnahmen ein.
2. Manipulationsmeldungen von Kundinnen und Kunden der IAP dürfen weiterhin über die herkömmlichen Kontaktpunkte (z. B. Hotline, Service-Desk etc.) erfolgen.
3. Für jeden zugeteilten IP-Adressblock haben die IAP bei der zuständigen «Regional Internet Registry» (RIR) eine elektronische Adresse («abuse-c») zu hinterlegen, welche die Funktion der Meldestelle wahrnimmt. Anderenfalls müssen sie eine generelle elektronische Adresse für technische Fragen («tech-c») hinterlegen und sicherstellen, dass dieser Kontakt die Funktion der Meldestelle wahrnehmen kann.
4. Sie konfigurieren ihre E-Mail-Spamfilter so, dass Manipulationsmeldungen nicht aussortiert werden.

Biel/Bienne, 24. Januar 2024

Bundesamt für Kommunikation BAKOM

Maissen Bernard T3OS5O
24.01.2024

Info: admin.ch/esignature | validator.ch

Bernard Maissen
Direktor