

# Kontaktstellen von Betreibern wesentlicher Dienste

NIS Fact Sheet 1/2019 – Version 3

## Inhalt

<b>Inhalt .....</b>	<b>2</b>
<b>1 Rahmen .....</b>	<b>3</b>
1.1 Anwendungsbereich .....	3
1.2 Zuständigkeiten und Kommunikation .....	3
<b>2 Kontaktstellen .....</b>	<b>5</b>
2.1 Kontaktdaten .....	5
2.2 Bekanntgabe der Kontaktstelle .....	6
2.3 Änderung der Kontaktstelle.....	6
<b>3 Betrieb von Kontaktstellen .....</b>	<b>7</b>
3.1 Erreichbarkeit .....	7
3.2 Personal .....	8
3.3 Technische Rahmenbedingungen.....	8
3.4 Taxonomie der Nachrichtenübermittlung.....	9
<b>4 Versionshistorie .....</b>	<b>12</b>
<b>Impressum .....</b>	<b>13</b>

# 1 Rahmen

## 1.1 Anwendungsbereich

Betreiber wesentlicher Dienste müssen **innerhalb von zwei Wochen nach Zustellung des Bescheides**, mit dem sie vom Bundeskanzler als Betreiber wesentlicher Dienste gemäß § 16 Abs. 1 NISG ermittelt werden, eine Kontaktstelle **bekanntgeben**. Darüber hinaus müssen die **Erreichbarkeit** des Betreibers **während der Bereitstellung des bzw. der wesentlichen Dienste gewährleistet** sein sowie **Änderungen** der Kontaktstelle **unverzüglich** bekannt gegeben werden. (§ 16 Abs. 3 NISG)

## 1.2 Zuständigkeiten und Kommunikation

**Hinweis:** Auf der Webseite [www.nis.gv.at](http://www.nis.gv.at), welche als Anlaufstelle für das Netz- und Informationssystemsecuritygesetz (NISG) und damit zusammenhängender Rechtsgrundlagen und weiterer Informationen fungiert, sind die **aktuellen Kontaktdaten** der NIS-Behörden unter dem Menüpunkt „Kontakt“ ersichtlich.

### 1.2.1 Strategische NIS-Behörde

Die Wahrnehmung der „strategischen“ Aufgaben des Bundeskanzlers im Rahmen des NISG fällt in die Zuständigkeit des **Büros für strategische Netz- und Informationssystemsecurityheit (NIS-Büro)** der Abteilung I/8 für Cybersicherheit, GovCERT, NIS Büro und ZAS im Bundeskanzleramt. Hierzu zählt im Zusammenhang mit Kontaktstellen der Betreiber wesentlicher Dienste insbesondere die Entgegennahme der Bekanntgabe von Kontaktstellen und diesbezüglicher Änderungen. Zur Kommunikation steht folgende E-Mailadresse bereit:

#### E-Mail

Das offizielle E-Mailpostfach lautet: [nis@bka.gv.at](mailto:nis@bka.gv.at)

Dieses Funktionspostfach stellt S/MIME zur Gewährleistung von Authentizität (Signatur) und Vertraulichkeit (Ende-zu-Ende Verschlüsselung) zur Verfügung.

## 1.2.2 Operative NIS-Behörde

Nach der Organisationsstruktur des Bundesministeriums für Inneres nimmt die **Abteilung IV/S/2 Netz- und Informationssystemicherheit** als zuständige Organisationseinheit **für den Bundesminister für Inneres** im Rahmen des NISG „operative“ Aufgaben wahr. Die Sicherstellung der Kommunikation mit den Kontaktstellen der Betreiber wesentlicher Dienste stellt hierbei eine zentrale Kompetenz dar. Zur Kommunikation mit der operativen NIS-Behörde stehen die nachstehend angeführten Möglichkeiten bereit:

### E-Mail

Das offizielle E-Mailpostfach lautet: [post@nis.gv.at](mailto:post@nis.gv.at)

Dieses Funktionspostfach stellt sowohl S/MIME als auch PGP zur Gewährleistung von Authentizität (Signatur) und Vertraulichkeit (Ende-zu-Ende Verschlüsselung) zur Verfügung.

### BMI-Cryptshare

Austauschplattform BMI-Cryptshare: <https://cryptshare.bmi.gv.at>

Der BMI-Cryptshare ist eine Webanwendung, die einen verschlüsselten (256 Bit AES) Datenaustausch zwischen zwei Stellen gewährleistet. Es ist als alternatives Medium für die Kommunikation vorgesehen, sollte S/MIME als auch PGP nicht beiden Kommunikationsstellen zur Verfügung stehen. Unter [https://www.bmi.gv.at/Impressum/files/Cryptshare\\_Leitfaden\\_20181215.pdf](https://www.bmi.gv.at/Impressum/files/Cryptshare_Leitfaden_20181215.pdf) findet sich die allgemeine Anleitung zur Verwendung des BMI-Cryptshare.

### Telefon

Die Rufnummer lautet: +43 59133 989480

## 2 Kontaktstellen

Die Kontaktstelle dient dem Zweck, die Kommunikation zwischen dem Bundeskanzler (strategische NIS-Behörde), dem Bundesminister für Inneres (operative NIS-Behörde) oder dem zuständigen Computer-Notfallteam mit dem Betreiber wesentlicher Dienste sicherzustellen. Über die Kontaktstelle können beispielsweise NIS Fact Sheets, IT-Sicherheitswarnungen, Schwachstelleninformationen, IT-Sicherheitslagebilder oder Rückfragen zu Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle empfangen werden.

Es kommen als Kontaktstellen z.B. auch externe IT-Dienstleister in Frage. Eine „österreichische“ Kontaktstelle bzw. ein österreichischer Standort der Kontaktstelle ist nicht erforderlich. Bei der Bekanntgabe einer im Ausland gelegenen Kontaktstelle ist aber darauf zu achten, dass eine Kommunikation in der Staatssprache Deutsch möglich ist.

Die Meldung von Sicherheitsvorfällen an das für den Betreiber wesentlicher Dienste zuständige Computer-Notfallteam (§ 19 Abs. 1 NISG) muss nicht über die Kontaktstelle erfolgen. Dennoch bietet sich die Meldung eines Sicherheitsvorfalls über die entsprechende Meldeplattform durch die jeweilige Kontaktstelle an, weil in weiterer Folge eine Kontaktaufnahme durch das Computer-Notfallteam oder die operative NIS-Behörde wahrscheinlich ist.

### 2.1 Kontaktdaten

Zu einer Kontaktstelle gibt der Betreiber wesentlicher Dienste zumindest eine E-Mailadresse und Telefonnummer („**Kontaktdaten-Paar**“) an. Es kann nur eine Kontaktstelle je Betreiber wesentlicher Dienste geben, doch kann die Kontaktstelle aus mehreren Kontaktdaten-Paaren bestehen, was insbesondere dann Sinn macht, wenn ein Betreiber mehrere unterschiedliche wesentliche Dienste erbringt. Im letztgenannten Fall würde der Betreiber für die unterschiedlichen wesentlichen Dienste jeweils ein Kontaktdaten-Paar angeben.

Bei E-Mailadressen wird generell die Verwendung von Funktionspostfächern empfohlen.

## 2.2 Bekanntgabe der Kontaktstelle

Die Bekanntgabe der Kontaktstelle hat gegenüber der strategischen NIS-Behörde zu erfolgen, welche die Kontaktdaten der operativen NIS-Behörde und dem für den Betreiber wesentlicher Dienste zuständigen Computer-Notfallteam übermittelt. An die Art der Bekanntgabe an die strategische NIS-Behörde wird kein (Form-)Erfordernis geknüpft, doch sollte eine nachweisbare und dokumentierte Bekanntgabe erfolgen. Dies kann etwa durch E-Mail an [nis@bka.gv.at](mailto:nis@bka.gv.at) geschehen.

## 2.3 Änderung der Kontaktstelle

Betreiber wesentlicher Dienste haben Änderungen in Bezug auf die Kontaktstelle, somit auch Änderungen der Kontaktdaten der Kontaktstelle, der strategischen NIS-Behörde **unverzüglich** bekanntzugeben. Änderungen können in der gleichen Form wie Bekanntgaben an die strategische NIS-Behörde übermittelt werden, somit etwa durch E-Mail an [nis@bka.gv.at](mailto:nis@bka.gv.at).

Sollte eine Kontaktstelle der strategischen NIS-Behörde nicht innerhalb von zwei Wochen nach Zustellung des Ermittlungsbescheides (§ 16 Abs. 3 erster Satz NISG) bekanntgegeben werden, so liegt eine **Verwaltungsübertretung** nach § 26 Abs. 1 Z 1 NISG vor. Ebenso liegt eine Verwaltungsübertretung vor, wenn Änderungen der Kontaktstelle (§ 16 Abs. 3 dritter Satz NISG) **nicht unverzüglich** bekanntgegeben werden.

# 3 Betrieb von Kontaktstellen

## 3.1 Erreichbarkeit

Als Anforderung an die Kontaktstelle sieht § 16 Abs. 3 NISG vor, dass Betreiber wesentlicher Dienste zumindest in jenem Zeitraum, in dem der bzw. die wesentlichen Dienste bereitgestellt werden, über die Kontaktstelle erreichbar sein müssen. Daher ist auf die **Erreichbarkeit während der Erbringung des wesentlichen Dienstes** abzustellen und nicht etwa auf Büro- oder Öffnungszeiten.

Es liegt eine Verwaltungsübertretung gemäß § 26 Abs. 1 Z 1 NISG vor, wenn ein Betreiber wesentlicher Dienste unter der bekanntgegebenen Kontaktstelle nicht in jenem Zeitraum, in dem der bzw. die wesentlichen Dienste bereitgestellt werden, erreichbar ist.

Auf Seiten der Betreiber wesentlicher Dienste wird die Einrichtung der Kontaktstelle grundsätzlich als **Single Point of Contact (SPOC)** empfohlen. Hierbei reicht es aus, dass diese Kontaktstelle des Betreibers aus einer E-Mailadresse und einer zugehörigen Telefonrufnummer (Kontaktdaten-Paar) besteht.

Wie ein Betreiber wesentlicher Dienste Nachrichten bzw. Informationen, die an die Kontaktstelle ergehen, organisationsintern weiterleitet und behandelt, obliegt dem jeweiligen Betreiber wesentlicher Dienste selbst.

### 3.1.1 E-Mail

Die Ausgestaltung der Kontaktstelle über E-Mail sollte nach Möglichkeit in Form eines **Funktionspostfachs** erfolgen, um die Erreichbarkeit gewährleisten zu können. Diese Implementierung entspricht der Erreichbarkeit der strategische als auch der operativen NIS-Behörde.

Bei der Bekanntgabe und Verwendung personenbezogener E-Mailadressen wird auf die **Sicherstellung der erforderlichen Erreichbarkeit auch während der Abwesenheit des Adressinhabers**, z. B. außerhalb der Dienstzeiten, an Wochenenden oder bei Urlauben, hingewiesen.

### 3.1.2 Telefon

Die Notwendigkeit der Bekanntgabe einer telefonischen Erreichbarkeit im Rahmen der Kontaktstelle ergibt sich u. a. auch aus Überlegungen zur Schaffung von Redundanz zur vorrangig genutzten Verbindung über E-Mail. Speziell in dringenden oder krisenhaften Situationen kommt dieser Form der direkten gegenseitigen Kommunikation hohe Bedeutung zu. Jedoch sollten unter dem Aspekt der erweiterten Redundanz auch alternative Sprechverbindungen in Betracht gezogen werden. Neben den herkömmlichen Telefonnummern im **Festnetz** wird hier auf Erreichbarkeiten im **Mobilfunknetz** hingewiesen. All jenen Betreibern wesentlicher Dienste, die im Zuge des Staatlichen Krisen- und Katastrophenmanagements (SKKM) mit Geräten des **digitalen Bündelfunks BOS-AUSTRIA** ausgestattet sind, wird auch die Bekanntgabe der ISSI-Rufnummer als Kontaktdaten der Kontaktstelle empfohlen.

## 3.2 Personal

Eine Kontaktstelle erfordert kein besonders geschultes oder qualifiziertes Personal, weil die Kontaktstelle nicht für bestimmte technische Aufgaben, z. B. im Rahmen der Bewältigung von Sicherheitsvorfällen, vorgesehen ist. Es müssen jedoch jedenfalls der Empfang und gegebenenfalls die Weiterleitung der Information gewährleistet sein. Aus diesem Grund kann es sich auch um ein Funktionspostfach oder um die Kontaktdaten einer Fachabteilung oder natürlichen Person handeln, die beim Betreiber wesentlicher Dienste keine Rolle im Bereich der Netz- und Informationssystemsicherheit wahrnimmt. Sinnvoll und effizient erscheint dennoch die Bekanntgabe einer Kontaktstelle, die beim Betreiber wesentlicher Dienste mit Aufgaben im Bereich der Netz- und Informationssystemsicherheit betraut ist.

## 3.3 Technische Rahmenbedingungen

Sollte die operative NIS-Behörde anlassbezogen Informationen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen bzw. zur Vorbeugung von Sicherheitsvorfällen (§ 5 Abs. 1 Z 4 NISG) an die Kontaktstelle übermitteln wollen, so wird dies nur geschehen, wenn gegenüber der operativen NIS-Behörde nachgewiesen wurde, dass die Kontaktstelle die erforderliche Sicherheit zur Behandlung sensibler Informationen gewährleistet. Bei der Übertragung von Nachrichten kann dies z. B. durch die Verwendung von Ende-zu-Ende Verschlüsselung sichergestellt werden (S/MIME, PGP, BMI Cryptshare).

Die Auswahl kryptografischer Funktionen und die Länge des verwendeten Schlüsselmaterials sollten generell den Stand der Technik berücksichtigen. Empfehlungen hierzu können u. a. dem Dokument »Handreichung zum „Stand der Technik“«, herausgegeben vom Bundesverband IT-Sicherheit e.V. (TeleTrusT, <https://www.teletrust.de>), in der jeweils aktuellen Fassung entnommen werden.

### **Verschlüsselung der Nachrichtenübermittlung**

Die Basis sollte die Konfiguration des Mailservers mit **mandatory TLS** darstellen. Diese Maßnahme entspricht dem Stand der Technik. Dadurch wird der Übertragungskanal, der **Transport Layer**, zwischen den Mailservern des Absenders und Empfängers geschützt.

Der durchgängige Schutz von Nachrichten zwischen Absender und Empfänger ist durch Etablierung einer **Ende-zu-Ende Verschlüsselung** zu erreichen. Hierfür kommen entweder S/MIME oder PGP in Frage.

Nähere Informationen zu verwendeten S/MIME-Zertifikaten oder bestehender PGP-Schlüssel der operativen NIS-Behörde sind auf <https://www.nis.gv.at> unter „Kontakt“ abrufbar. Hierzu wird auf <https://securemail.bmi.gv.at/> verwiesen, wo mittels Suchfunktion („Suchen“) unter Eingabe der E-Mailadresse der operativen NIS-Behörde die entsprechenden Informationen abrufbar sind.

Sollten interne technische oder organisatorische Gründe gegen den Einsatz von Ende-zu-Ende Verschlüsselung von E-Mails sprechen, so steht alternativ die Austauschplattform des BMI-Cryptshare zur Kommunikation zur Verfügung.

## **3.4 Taxonomie der Nachrichtenübermittlung**

Zur Unterstützung einer kontextbasierenden Weiterleitung eingehender Nachrichten bei den Kontaktstellen wird die nachfolgende Taxonomie definiert. Die dabei verwendeten Begriffe lassen eine Kategorisierung hinsichtlich Art und Dringlichkeit einer Nachricht zu. Die entsprechenden Begriffe werden hierfür an den Beginn der Betreffzeile von E-Mails an die Betreiber wesentlicher Dienste bzw. deren Kontaktstellen gesetzt.

Sollte zusätzlich zur oben angeführten Kategorisierung eine Empfangsbestätigung über die Formen der automatisierten Übertragungs- und Lesebestätigungen von Mailservern hinaus erforderlich sein, so wird dieses Erfordernis grundsätzlich im Text der E-Mail angeführt.

## **Art**

INFORMATION | COMCHECK | WARNUNG

### **INFORMATION**

Aussendungen der Kategorie INFORMATION besitzen vorrangig informativen Charakter und erfordern grundsätzlich keine unmittelbare Veranlassung von Maßnahmen beim Adressaten.

### **COMCHECK**

Ein entscheidender Punkt zur Aufrechterhaltung der Funktionsfähigkeit und Erreichbarkeit einer Kontaktstelle liegt in einer fortlaufenden und regelmäßigen Durchführung von Probeverbindungen (COMCHECKs). Unabhängig von den Verpflichtungen der einzelnen Betreiber zur Sicherstellung der Erreichbarkeit im Zeitraum der Erbringung des wesentlichen Dienstes und der Bekanntgabe von Änderungen von Kontaktdaten, ist nur durch eine begleitende Überprüfung der Kontaktstelle zu gewährleisten, dass die beabsichtigte Funktion im Ernstfall, z. B. bei einem Sicherheitsvorfall oder Warnmeldungen, auch tatsächlich gegeben ist.

Dies soll durch die operative NIS-Behörde in zweierlei Hinsicht überprüft bzw. erreicht werden. Einerseits wird bei Bekanntgaben von Kontaktdaten deren Funktionalität initial auf Korrektheit der Angaben und den Umfang hin geprüft. Andererseits wird in regelmäßigen Abständen die allgemeine Funktionalität der Kontaktstelle geprüft. COMCHECKs können jedoch auch stichprobenartig oder bei begründetem Verdacht, dass die Erreichbarkeit einer Kontaktstelle nicht gegeben ist, im Anlassfall erfolgen.

### **WARNUNG**

Aussendungen der Kategorie WARNUNG können bspw. bestehende Risiken zu etablierten Produkten, laufende Angriffswellen oder Kampagnen von Schadsoftware, etc. betreffen. Bei

Aussendungen der Kategorie WARNUNG, die auch als KRITISCH eingestuft sind (siehe unten), kann im Anlassfall zusätzlich telefonisch durch die operative NIS-Behörde mit Kontaktstellen betroffener wesentlicher Dienste Kontakt aufgenommen werden, um diese ohne unnötigen Zeitverzug in Kenntnis setzen zu können.

## Dringlichkeit

ROUTINE | DRINGEND | KRITISCH

In zeitlicher Hinsicht erfolgen unterschiedliche Kategorisierungen, die Auskunft über erforderliche bzw. erwartete Reaktionszeiten oder die Brisanz der beinhaltenen Informationen geben. Hierbei werden folgenden Zeiträume vorgegeben:

- **ROUTINE**  
Keine zeitlichen Vorgaben bzw. keine unmittelbare Veranlassung erforderlich
- **DRINGEND**  
Anmerkungen zu gegebenenfalls terminlichen Vorgaben im Text der Nachrichten
- **KRITISCH**  
Umgehende Veranlassung, ohne unnötigen Zeitverzug

## Beispiele für „kategorisierte“ Betreffzeilen in E-Mails

Betreff: INFORMATION | ROUTINE | Bekanntgabe von Kontaktdaten

Betreff: WARNUNG | KRITISCH | Risikowarnung für Produkt X

## 4 Versionshistorie

Bei diesem Dokument handelt es sich um die Version 3 vom April 2023.

Änderungen und Anpassungen der Version 2 gegenüber der Version 1 (aus dem Jänner 2019) ergaben sich insbesondere durch ergänzende Erläuterungen hinsichtlich folgender Punkte:

- Gliederung des Dokuments zur besseren Übersicht und Verwendung
- Spezifizierung und nähere Erläuterung der Abläufe
- Taxonomie

Änderungen und Anpassungen der Version 3 gegenüber der Version 2 (aus dem März 2021) betreffen folgende Punkte:

- Aktualisierung der Kontaktdaten der NIS-Behörden
- Klarere Formulierung

## **Impressum**

Medieninhaber, Verleger und Herausgeber:

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien

Autoren: Bundeskanzleramt Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) und Bundesministerium für Inneres Abteilung IV/S/2 Netz- und Informationssystemsicherheit Wien, 2023. Stand: 19. April 2023

Copyright und Haftung:

Auszugsweiser Abdruck ist nur mit Quellenangabe gestattet, alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig. Es wird darauf verwiesen, dass alle Angaben in dieser Publikation trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Bundeskanzleramtes und des Bundesministeriums für Inneres ausgeschlossen ist. Rechtausführungen stellen die unverbindliche Meinung der Autoren dar und können der Rechtsprechung der unabhängigen Gerichte keinesfalls vorgreifen.

Abschließende Anmerkungen:

Es wird darauf hingewiesen, dass Änderungen vorbehalten sind.

Alle in diesem NIS Fact Sheet verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an [nis@bka.gv.at](mailto:nis@bka.gv.at) und [post@nis.gv.at](mailto:post@nis.gv.at).