Bundeskanzleramt

Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Kontaktstellen von Betreibern wesentlicher Dienste

NIS Fact Sheet 1/2019 – Version 2

Wien, März 2021

Inhalt

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

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 Informationssystemsicherheit (NIS-Büro)** der Abteilung I/8 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 des NIS Büros lautet: 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 das **Referat NIS** der Abteilung 5-Cybersicherheit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) 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 dem Referat NIS stehen die nachstehend angeführten Möglichkeiten bereit.

E-Mail:

Das offizielle E-Mailpostfach des Referats NIS lautet: nis@bvt.gv.at

Dieses Funktionspostfach stellt sowohl S/MIME als auch OpenPGP 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. Er kann als alternatives Medium für die Kommunikation verwendet werden. Unter https://www.bmi.gv.at/Impressum/files/Cryptshare_Leitfaden_20181215.pdf findet sich die allgemeine Anleitung zur Verwendung des BMI-Cryptshare.

Telefon:

Die telefonische Erreichbarkeit des Referats NIS ist über den Journaldienst des BVT unter folgender Rufnummer gegeben: +43 1 53126 4100

2 Kontaktstellen

Die Kontaktstelle dient dem Zweck, die Kommunikation zwischen dem Bundeskanzler, dem Bundesminister für Inneres 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 Kontaktstelle an, weil in weiterer Folge eine Kontaktaufnahme durch das Computer-Notfallteam oder den Bundesminister für Inneres 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.

2.2 Bekanntgabe der Kontaktstelle

Die Bekanntgabe der Kontaktstelle hat gegenüber dem Bundeskanzler zu erfolgen, welcher die Kontaktdaten dem Bundesminister für Inneres und dem für den Betreiber wesentlicher Dienste zuständigen Computer-Notfallteam übermittelt. An die Art der Bekanntgabe an den Bundeskanzler wird kein (Form-)Erfordernis geknüpft, doch sollte eine nachweisbare und dokumentierte Bekanntgabe erfolgen. Dies kann etwa durch E-Mail an 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, dem Bundeskanzler unverzüglich bekanntzugeben. Änderungen können in der gleichen Form wie Bekanntgaben an den Bundeskanzler übermittelt werden.

Es wird die Verwendung von Funktionspostfächern empfohlen.

Sollte eine Kontaktstelle dem Bundeskanzler 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, oder wenn ein Betreiber wesentlicher Dienste unter der Kontaktstelle nicht in jenem Zeitraum, in dem der bzw. die wesentlichen Dienste bereitgestellt werden, erreichbar ist (§ 16 Abs. 3 zweiter Satz NISG).

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.

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 die Kommunikation des Betreibers wesentlicher Dienste intern ausgestaltet ist, oder welcher Prozesse er sich innerhalb der Unternehmensstruktur bedient, bleibt ihm überlassen. Dabei steht es dem Betreiber frei, eingehende Nachrichten intern zu verteilen bzw. weiterzuleiten. Hierbei sind die Anforderungen an die zeitliche Erreichbarkeit weiterhin sicherzustellen. Die Verteilung bzw. Weiterleitung ist zusätzlich zur allgemeinen Erreichbarkeit der Kontaktstelle zu verstehen.

3.1.1 E-Mail

Die Erreichbarkeit der Kontaktstelle über E-Mail sollte nach Möglichkeit in Form eines **Funktionspostfachs** erfolgen. Diese Implementierung entspricht auch jener der Erreichbarkeit der zuständigen Organisationseinheiten im Bundeskanzleramt und im Bundesministerium für Inneres.

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 Kontaktdatum der Kontaktstelle empfohlen.

Sollten speziell bei Telefonaten **Zweifel an der Authentizität des Anrufers** bestehen, wird folgende Vorgehensweise empfohlen. Betreiber wesentlicher Dienste fragen Name, Funktion und Erreichbarkeit der Person, die sich als ein Vertreter bzw. eine Vertreterin der NIS-Behörden ausgibt, ab. Anschließend kann bei Bedarf über die in Kapitel 1.2.2 (Seite 4) ersichtliche telefonische Erreichbarkeit der **operativen NIS-Behörde zurückgerufen** und um Weiterleitung an diese Person ersucht werden. Die NIS-Behörden werden bei vergleichbarem Zweifel die bekanntgegebene **Kontaktstelle** des betreffenden Betreibers wesentlicher Dienste **zurückrufen**, um die Authentizität eines Anrufers bzw. einer Anruferin zu verifizieren.

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 der Bundesminister für Inneres 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 dem Bundesminister für Inneres 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.

Die Auswahl kryptografischer Funktionen und die Länge des verwendeten Schlüsselmaterials sollte 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 aktuellsten 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 OpenPGP in Frage. Bei der Verwendung von S/MIME wird darauf hingewiesen, dass die hierfür erforderlichen S/MIME Zertifikate von öffentlich zugänglichen Vertrauensdiensteanbietern (Root-CA) zu beziehen sind. Die Verwendung von „self-signed“ Zertifikaten ist ungenügend. Die Verwendung von OpenPGP und hierbei der Austausch der öffentlichen Schlüssel ist direkt mit der Behörde abzusprechen.

Nähere Informationen zu den S/MIME Zertifikaten bzw. OpenPGP Schlüsseln der NIS-Behörden sind auf www.nis.gv.at ersichtlich.

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 nachfolgende Taxonomie definiert. Diese 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 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 (COMCHECK s). 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.
  Die Zwecke des COMCHECK s werden durch das NIS-Referat im Bundesministerium für Inneres in zweierlei Hinsicht erreicht. Einerseits wird bei Bekanntgaben von Kontaktdaten deren Funktionalität initial auf Korrektheit der Angaben und den Umfang hin geprüft. Andererseits wird in regelmäßigen Abständen von etwa sechs Monaten die allgemeine Funktion geprüft. COMCHECK s können jedoch auch stichprobenartig oder bei begründetem Verdacht, dass die Erreichbarkeit einer Kontaktstelle nicht gegeben ist, erfolgen.

- WARNUNG
  Aussendungen der Art WARNUNG, die zusätzlich auch zumindest als KRITISCH eingestuft sind (s.u.), werden grundsätzlich durch zusätzliche, auch mehrmalige Versuche zur Kontaktaufnahmen mit der bzw. den Telefonnummern der Kontaktstelle ergänzt. Diese Maßnahme dient dazu, um in derartigen Fällen den betroffenen Betreiber wesentlicher Dienste ohne unnötigen Zeitverzug in Kenntnis zu setzen.

Dringlichkeit

ROUTINE | DRINGEND | KRITISCH

In zeitlicher Hinsicht erfolgen unterschiedliche Kategorisierungen, die Auskunft über erforderliche bzw. erwartete Reaktionszeiten oder die Brisanz der beinhalteten 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 2 vom 1. März 2021.

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

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

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Autoren: Bundeskanzleramt Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) und BMI/II/BVT/5.3-NIS
Wien, 2021. Stand: 1. März 2021

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 und nis@bvt.gv.at.