Bundeskanzleramt

Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Qualifizierte Stellen

NIS Fact Sheet 7/2019

Wien, Juli 2019

Inhalt

1 Einleitung

1.1 Rahmen

Betreiber wesentlicher Dienste (BwD) haben gemäß § 17 Abs. 3 NISG mindestens alle drei Jahre nach deren Identifizierung gegenüber dem Bundesminister für Inneres nachzuweisen, dass sie geeignete und verhältnismäßige **Sicherheitsvorkehrungen** hinsichtlich jener Netz- und Informationssysteme getroffen haben, die sie für die Bereitstellung des wesentlichen Dienstes nutzen. **Qualifizierte Stellen** nehmen dabei eine zentrale Rolle ein, da sie als **Prüfstellen für BwD** fungieren und von diesen auch heranzuziehen sind. Die Formalia der Überprüfungen selbst sind zwischen BwD und den qualifizierten Stellen mittels Vertrag bzw. Ausschreibung zu regeln.

Mit der Verordnung zur Festlegung der Erfordernisse und besonderer Kriterien für qualifizierte Stellen nach dem Netz- und Informationssystemsicherheitsgesetz (Verordnung über qualifizierte Stellen – QuaSteV) legt der Bundesminister für Inneres, im Einvernehmen mit dem Bundesminister für EU, Kunst, Kultur und Medien, jene **Erfordernisse** fest, die qualifizierte Stellen **erfüllen müssen**, um BwD nach dem NISG überprüfen zu können.

1.2 Anwendungsbereich

Dieses NIS Fact Sheet beschreibt den **Ablauf des Verfahrens** zur Feststellung von qualifizierten Stellen näher und soll als Hilfestellung für Antragstellerinnen[1] dienen.

Zudem ist dieses Fact Sheet als Bekanntmachung hinsichtlich des elektronischen Verkehrs zwischen Antragstellerin und der zuständigen Organisationseinheit gemäß § 13 Abs. 2 AVG zu werten.

[1] Falls nicht näher erläutert, beziehen sich die verwendeten Begriffe in diesem Fact Sheet auf jene des NISG und der QuaSteV (z.B. Antragstellerin als Einrichtung im Sinne des § 3 Z 11 NISG, die mit Bescheid als qualifizierte Stelle festgestellt werden möchte).

1.3 Zuständigkeit

Nach der Organisationsstruktur des Bundesministeriums für Inneres ist das **Referat NIS** der Abteilung 5-Cybersicherheit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) für die Feststellung von qualifizierten Stellen zuständig. Das offizielle E-Mailpostfach des Referats NIS als zuständige Organisationseinheit lautet

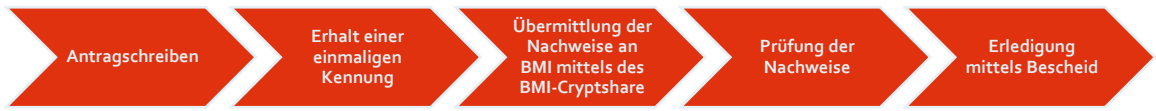
nis@bvt.gv.at[2]

Es wird empfohlen, spezifische Fragen zum Feststellungsverfahren vor dessen Einleitung mit der zuständigen Organisationseinheit abzuklären.

[2] Die verschlüsselte Kommunikation mittels S/MIME ist möglich.

2 Ablauf der Feststellung einer qualifizierten Stelle

Die folgende Grafik bietet eine Prozessübersicht. Die einzelnen Schritte werden in den folgenden Kapiteln näher erläutert.



2.1 Antragschreiben

Es handelt sich dabei um einen **formlosen Antrag**, der von der Antragstellerin per E-Mail an nis@bvt.gv.at übermittelt wird. Dabei hat die Antragstellerin ihre offizielle E-Mailadresse zu verwenden, mit der sie üblicherweise im elektronischen Geschäftsverkehr nach außen hin tätig wird. Aus dem Antrag hat hervorzugehen, um welche Einrichtung (Name, Rechtsform etc.) es sich handelt und wo sich die Niederlassung befindet. Der Antrag hat zudem darzulegen, in welchem Aufgabenbereich (d.h. welche Kategorie(n) oder einzelne Sicherheitsmaßnahme(n) der Anlage 1 zur NISV) die Antragstellerin tätig werden möchte.

2.2 Erhalt einer Kennung

Nachdem das Antragschreiben bei der zuständigen Organisationseinheit eingegangen ist, wird **der Antragstellerin** per E-Mail **eine einmalige Kennung übermittelt**, die bei der Übermittlung der Nachweise anzuführen bzw. zu verwenden ist. Sie dient dazu, die jeweilige Antragstellerin eindeutig identifizieren und eine mögliche missbräuchliche Verwendung unterbinden zu können.

2.3 Übermittlung der Nachweise

Folgende Erfordernisse, die der Übersichtlichkeit halber kategorisch aufgezählt werden, haben Antragstellerinnen im Rahmen der Vorgaben der QuaSteV nachzuweisen. Alle Nachweise sind im **PDF-Format** zu übermitteln und entsprechend ihres Inhalts zu kennzeichnen.

2.3.1 Prüfer

Für jede Person, die als Prüfer tätig sein soll, ist Folgendes nachzuweisen:

- Durchgeführte Sicherheitsüberprüfung inkl. abgegebener Sicherheitserklärung
- Einschlägige Berufserfahrung (z.B. durch Dienstzeugnisse)
- Ausbildung(en), Zertifizierung(en) sowie sonstige äquivalente Nachweise der Kenntnis im jeweiligen Fachbereich (organisatorisch und/oder technisch)

2.3.2 Sicherheitsvorkehrungen

Qualifizierte Stellen haben für ihre Netz- und Informationssysteme **technische und organisatorische Sicherheitsvorkehrungen** zu treffen, die geeignet, verhältnismäßig und dem Risiko angemessen sind sowie den Stand der Technik berücksichtigen. Es handelt sich dabei um jene Vorgaben der Anlage 1 der NISV, die auch BwD umzusetzen haben, mit dem Unterschied, dass der Anwendungsbereich (Scope) der Sicherheitsvorkehrungen auf jenen Netz- und Informationssystemen liegt, die im Zuge einer Überprüfung genutzt werden.

Die Antragstellerin hat durch eine detaillierte Aufstellung (bspw. durch Prüfberichte, Maßnahmenbeschreibungen usw.) nachzuweisen, dass die getroffenen Sicherheitsvorkehrungen ausreichend sind.

2.3.3 Werkzeuge

Es ist darzulegen, welche **Werkzeuge** (Soft- und Hardware) für **Überprüfungen** von BwD verwendet werden sollen.

2.3.4 Prüfprozess

Qualifizierte Stellen haben für die Überprüfung von BwD einen **geeigneten Prüfprozess** zu verwenden (Wie wird aus prozessualer und inhaltlicher Sicht geprüft?). Zudem ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass die Sicherheit der Prüfdaten ein entsprechendes Schutzniveau erreicht.

Die Antragstellerin hat dabei

- den von ihr zukünftig angewendeten **Prüfprozess detailliert und aussagekräftig** zu beschreiben,
- darzulegen, wie und in welcher Form **Prüfdaten aufgearbeitet und bewertet** werden sollen sowie
- darzulegen, welche technischen und organisatorischen Maßnahmen zur Gewährleistung der **Sicherheit der Prüfdaten** getroffen werden.

2.3.5 Meldeprozess

Qualifizierte Stellen haben bei Vorfällen, die ihre Netz- und Informationssysteme derart stören, dass die Integrität oder Vertraulichkeit der Prüfdaten nicht mehr gewährleistet werden kann, einen geeigneten **internen und externen Meldeprozess** anzuwenden.

Die Antragstellerin hat diesen zukünftig anzuwendenden Meldeprozess systematisch zu beschreiben und darzulegen, wie ein solcher Vorfall der zuständigen Organisationseinheit gemeldet werden wird.

2.3.6 Kontaktstelle

Die Antragstellerin hat eine Kontaktstelle für die Kommunikation mit der zuständigen Organisationseinheit bekanntzugeben. Diese Kontaktstelle soll in der Praxis als **Single Point of Contact** für die zuständige Organisationseinheit dienen und den Kommunikationsfluss zwischen Behörde und qualifizierter Stelle vereinfachen. Es reicht, wenn als Kontaktstelle eine E-Mailadresse und eine entsprechende Telefonnummer bekanntgeben werden.

2.3.7 Technische Übermittlung

Um eine sichere und komfortable Übermittlung der Nachweise zu ermöglichen, soll der sog. **BMI-Cryptshare**[3] (erreichbar unter https://cryptshare.bmi.gv.at) verwendet werden.

Unter https://www.bmi.gv.at/Impressum/files/Cryptshare_Leitfaden_20181215.pdf findet sich die allgemeine Anleitung zur Verwendung des BMI-Cryptshare, wobei folgende Schritte im Sinne der gegenständlichen Verwendung zu spezifizieren sind:

[3] Der BMI-Cryptshare ist eine Webanwendung, die einen verschlüsselten (256 Bit AES) Datenaustausch zwischen zwei Stellen gewährleistet.

- Bei Schritt 2 sind die Kennung im Namensfeld, eine entsprechende Telefonnummer (sinnvollerweise jene der zukünftig vorgesehenen Kontaktstelle) sowie die offizielle E-Mailadresse der Antragstellerin anzugeben.
- Bei Schritt 4 ist nis@bvt.gv.at als Empfänger anzugeben.
- Bei Schritt 6 ist das Ablaufdatum so zu wählen, dass der Abruf für die zuständige Organisationseinheit sieben Tage (eine Woche) möglich ist.
- Das Kennwort wird seitens der zuständigen Organisationseinheit von der Antragstellerin rückgefragt.

2.4 Prüfung der Nachweise und Erledigung mittels Bescheid

Seitens der zuständigen Organisationseinheit werden die Nachweise nach Übermittlung **formal und inhaltlich geprüft** und **mittels Bescheid ausgesprochen,** ob und für welchen Aufgabenbereich die Antragstellerin als qualifizierte Stelle tätig werden kann. Bei einem rechtskräftigen positiven Bescheid wird die qualifizierte Stelle in die von der zuständigen Organisationseinheit geführte Liste gemäß § 18 Abs. 4 NISG eingetragen. In diese Liste wird Betreibern wesentlicher Dienste auf Anfrage Einsicht gewährt.

3 Exkurs Sicherheitsüberprüfungen

3.1 Überblick

Die Sicherheitsüberprüfung ist die **Abklärung der Vertrauenswürdigkeit eines Menschen** anhand personenbezogener Daten, die Aufschluss darüber geben, ob Anhaltspunkte dafür bestehen, dass er gefährliche Angriffe begehen werde.

Eine Sicherheitsüberprüfung hat ua. zu erfolgen (gemäß § 55a Abs. 2 SPG):

*3a. auf begründetes Ersuchen jenes Unternehmens, in dem der Betroffene eine Tätigkeit wahrnimmt oder anstrebt, bei der er Zugang zu vertraulicher Information hat, deren unzulässige Verwertung eine nachhaltige Funktionsstörung oder Zerstörung einer **kritischen Infrastruktur** bewirken würde;*

Die Zulässigkeit einer Sicherheitsüberprüfung setzt die **Zustimmung** des zu Überprüfenden und seine **„Sicherheitserklärung"** voraus (die Zustimmung und eine Erklärung des Betroffenen hinsichtlich seines Vorlebens und seiner gegenwärtigen Lebensumstände). Diese Zustimmung muss auch für die Übermittlung des Ergebnisses der Überprüfung an das ersuchende Unternehmen vorliegen.

Das Unternehmen, das um die Durchführung der Sicherheitsüberprüfung ersucht, hat deren Kosten zu tragen. Der Pauschalsatz für die Durchführung der Sicherheitsüberprüfung bei einer Sicherheitserklärung für den Zugang zu geheimer Information beträgt gemäß § 5 Z 2 SGV derzeit **593,- Euro**. Die Sicherheitsüberprüfung wird zentral vom BVT durchgeführt.

Unter https://www.bmi.gv.at/Downloads/Sicherheitserklaerung.aspx finden sich das zu verwendende **Formular** für Sicherheitserklärungen der Stufe "geheim", wobei nach Möglichkeit das Formular in Deutsch zu verwenden ist, sowie ein allgemeines Merkblatt zur Sicherheitsüberprüfung.

3.2 Vorgehensweise bei Prüfern

Für jeden Prüfer bzw. jede Person, die als Prüfer tätig werden soll, ist das Ersuchen auf Sicherheitsüberprüfung separat per E-Mail an nis@bvt.gv.at zu richten, wobei folgende Form zu wahren ist:

Betreff: [Vorname Nachname], geb. [TT.MM.JJJJ], SÜ Vertraulichkeitsstufe B, [Unternehmensbezeichnung] – NIS-QuaSte

Anlage: Sicherheitserklärung

Inhalt:

- Das Unternehmen [Unternehmensbezeichnung] ersucht um Sicherheitsüberprüfung des/der Beschäftigten [Name] gemäß § 55 SPG nach Vertraulichkeitsstufe B.
- Begründung der Notwendigkeit: Warum haben Mitarbeiter bzw. Prüfer Zugang zu vertraulichen Informationen, durch deren missbräuchliche Verwendung diese kritischen Infrastrukturen bzw. Betreiber wesentlicher Dienste schädigen könnten? (siehe § 55a SPG)
- Rechnungsanschrift des Unternehmens (nach Möglichkeit elektronisch)
- Erledigungsadresse: Stelle bzw. Person im Unternehmen, zu deren Handen das Ergebnis der Sicherheitsüberprüfung übermittelt werden soll (nach Möglichkeit elektronisch)

Nach einer kurzen Formalprüfung durch die zuständige Organisationseinheit wird das Ersuchen auf Sicherheitsüberprüfung an das zuständige Referat vollinhaltlich weitergeleitet. Das zuständige Referat für Sicherheitsüberprüfungen im BVT führt die Abklärung durch und übermittelt das Ergebnis der Sicherheitsüberprüfung an das ersuchende Unternehmen.

3.3 Vorgehensweise bei noch nicht vorhandenen Sicherheitsüberprüfungen im Feststellungsverfahren

Da es sich bei der Ermittlung von qualifizierten Stellen um ein verwaltungsrechtliches Feststellungsverfahren handelt, sieht § 9 Abs. 1 QuaSteV grundsätzlich vor, dass alle Nachweise einschließlich der Sicherheitsüberprüfung der gemeldeten Prüfer bereits im Zeitpunkt der Antragstellung bzw. der Übermittlung der Nachweise vorliegen müssen.

Im Falle von **noch nicht durchgeführten Sicherheitsüberprüfungen** wird seitens der zuständigen Organisationseinheit aber angeboten, die **sonstigen Nachweise vorab zu prüfen** und mit einem Mängelbehebungsauftrag der Antragstellerin die Möglichkeit zu geben, innerhalb einer angemessenen Frist den Nachweis der durchgeführten Sicherheitsüberprüfen nachzureichen. Damit kann das Verwaltungsverfahren für Antragstellerin effizienter gestaltet werden.

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, 2019
Stand: 10. Juli 2019

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.