Bundeskanzleramt

Umsetzungsleitfaden für Einrichtungen des Bundes

NIS Fact Sheet 9/2019

Wien, September 2019

Inhalt

1 Motivation

Mit 29. Dezember 2018 trat das Netz- und Informationssystemsicherheitsgesetz (NISG)[1] in Kraft. Dieses Bundesgesetz verpflichtet seither Einrichtungen des Bundes zur Umsetzung von Sicherheitsvorkehrungen für Netz- und Informationssysteme, die sie für die Bereitstellung von wichtigen Diensten nutzen.[2] Darüber hinaus werden Einrichtungen des Bundes verpflichtet, Sicherheitsvorfälle, die einen der wichtigen Dienste betreffen, unverzüglich zu melden.[3]

Eine nähere Festlegung der Kriterien für wichtige Dienste und Meldeverpflichtungen erfolgt nicht im NISG. Der **NIS Fact Sheet** soll Einrichtungen des Bundes in der Festlegung der wichtigen Dienste sowie der Meldekriterien **unterstützen**.

Adressaten des Umsetzungsleitfadens sind **Einrichtungen des Bundes**, das sind alle Bundesministerien, die Gerichtshöfe des öffentlichen Rechts, der Rechnungshof, die Volksanwaltschaft, die Präsidentschaftskanzlei und die Parlamentsdirektion.[4]

Die Empfehlungen im Umsetzungsleitfaden ergeben sich aus den Diskussionen der Informationsveranstaltungen vom 28. Jänner 2019, 29. April 2019 und 01. Juli 2019 sowie aus den Rückmeldungen einer vorgenommenen Umfrage. Zur Sammlung von konkreten Beispielen aus den Einrichtungen wurde eine Matrix ausgesandt, die sich an einer bereits vorliegenden Ausarbeitung des Bundesministeriums für Digitalisierung und Wirtschaftsstandort orientiert. Zur Bestimmung von wichtigen Diensten wurden insgesamt neunzehn verschiedene Arten von Kriterien herangezogen, zur Bestimmung der Meldekriterien acht.

Es wird darauf hingewiesen, dass dieser Umsetzungsleitfaden ein **unverbindliches Dokument** darstellt. Die konkrete Ausgestaltung der Umsetzung der Vorgaben aus dem NISG liegt ausschließlich in der **Verantwortung der jeweiligen Einrichtung**.

[1] BGBl. I Nr. 111/2018.
[2] § 22 Abs. 1 NISG.
[3] § 22 Abs. 2 NISG.
[4] § 3 Z 18 NISG.

2 Wichtige Dienste

2.1 Einleitung

Das NISG gibt an verschiedenen Stellen im Gesetz Kriterien zur Identifizierung von wesentlichen Diensten vor. Der Umsetzungsleitfaden orientiert sich bei der Festlegung der Kriterien zur Bestimmung eines wichtigen Dienstes und eines Sicherheitsvorfalls an diesen gesetzlichen Vorgaben (vgl. § 3 Z 6 und § 16 Abs. 2 NISG).

Von der Nutzung von allgemeingültigen, im Vorfeld definierten und festgelegten Werten, Wertgrenzen oder Wertebereichen wird abgesehen, da **nur die individuelle Ausprägung eines oder die Kombination mehrerer Kriterien** die Identifikation eines wichtigen Dienstes ermöglichen kann. Sollte eines der Kriterien nicht erfüllt sein, so ist dies kein Ausschließungskriterium (mit Ausnahme der Abhängigkeit von Netz- und Informationssystemen; siehe sogleich). Es kommt letztendlich immer auf den jeweiligen Dienst in der Einrichtung des Bundes an, wobei die Wichtigkeit eines Kriteriums für den jeweiligen Dienst zu ermitteln ist.

Es kann sein, dass der Betrieb von Netz- und Informationssystemen selbst einen wichtigen Dienst darstellt.

Bei der Beurteilung der Wichtigkeit eines Dienstes ist nicht nur die technische Dimension, sondern auch die wirtschaftliche, politische, staatliche, rechtliche und gesellschaftliche Dimension zu beachten.

Die Wichtigkeit im Hinblick auf den Nutzen ist daher nicht nur in technisch abrufbaren Systemen (z.B. Websites, e-Government-Services etc.) zu messen. Vielmehr sind weiche Faktoren (z.B. Ansehens- oder Vertrauensverlust, Ausfall einer Dienststelle etc.) ebenso zu berücksichtigen.

Ebenfalls mitbetrachtet wird, ob der Nutzen, den ein Dienst generiert, nur mit Hilfe dieses Dienstes erbracht werden kann, oder ob derselbe Nutzen nicht zeitverzögert und ohne vorhergehende Anpassung, auch über andere Systeme, bereitgestellt werden kann.

2.2 Kriterien für wichtige Dienste

In einem ersten Schritt ist zu fragen, welche Dienste überhaupt in Frage kommen. Erst anschließend sind die in Frage kommenden Dienste anhand von Kriterien dahingehend zu beurteilen, ob sie auch wichtige Dienste sind.

Dienste können insbesondere Sachverantwortungen gemäß dem BMG und IT-Verfahren (im Sinne des Betriebes von Netz- und Informationssystemen) sein.

Wichtige Dienste sind oben genannte Dienste, wenn sie von der Einrichtung des Bundes aufgrund einer Beurteilung anhand von bestimmten Kriterien als wichtig eingestuft wurden.

Für die Beurteilung der Wichtigkeit eines Dienstes kommen insbesondere folgende **Kriterien** in Betracht:

- Abhängigkeit von Netz- und Informationssystemen
- Unersetzbarkeit des Dienstes
- Art und Anzahl der Nutzer
- Art der verarbeitenden Daten
- Auswirkungen eines Sicherheitsvorfalls

Auf den folgenden Seiten werden diese Kriterien näher beschrieben.

2.2.1 Abhängigkeit von Netz- und Informationssystemen

- Voraussetzung für einen wichtigen Dienst ist stets die Abhängigkeit von Netz- und Informationssystemen, was dann der Fall ist, wenn bei der Bereitstellung bzw. Erbringung des wichtigen Dienstes Netz- und Informationssysteme eingesetzt werden.
- Es handelt sich bei der (Un-)Abhängigkeit von Netz- und Informationssystemen um das einzige Ausschließungskriterium. Wenn keinerlei Netz- und Informationssysteme bei der Bereitstellung bzw. Erbringung des wichtigen Dienstes eingesetzt werden, so kann kein wichtiger Dienst iSd NISG vorliegen.

Konkrete Werte:

Musskriterium

Ja/Nein (Ja = Voraussetzung für wichtigen Dienst)

2.2.2 Art der Notwendigkeit des Dienstes für seine Nutzer

- Bei der Bestimmung der zu bewertenden Notwendigkeit des Dienstes für seine Nutzer sollte mitbetrachtet werden, ob nur mit Hilfe dieses Dienstes die Wirkung für die Nutzer erbracht werden kann oder ob dieselbe Wirkung nicht zeitverzögert und ohne vorhergehende Anpassung, auch über andere Systeme, konsumiert werden kann.
- Ein Indikator für die Wichtigkeit eines Dienstes kann sein, dass er nicht substituierbar ist.

Konkrete Werte:

Notwendigkeit des Dienstes

Ja/Nein (Ja = Indikator für wichtigen Dienst)

2.2.3 Art- und Anzahl der Nutzer / Nutzungshäufigkeit

- Dieses Kriterium zielt auf die Anzahl der Nutzer des Dienstes ab. Dabei kann zwischen Bediensteten und Bürgern unterschieden werden.
- Bedienstete sind Mitarbeiter der jeweiligen Einrichtung des Bundes oder von Unternehmen, die den Dienst direkt für ihre Tätigkeit im Rahmen ihres Dienst- bzw. Arbeitsver-

hältnisses verwenden und mit Hilfe dieses Dienstes einen Nutzen für Bürger/Unternehmen generieren.

- Wenn die Anzahl der Nutzer nicht bekannt ist, ist eine Schätzung vorzunehmen. Ist auch eine Schätzung mit vernünftigem Aufwand nicht seriös zu bewerkstelligen, kann im Zweifelsfall die größtmögliche potentielle Nutzergruppe angenommen werden.
- Wenn die Anzahl der Bediensteten einer Einrichtung des Bundes nicht konkret bestimmbar ist, so ist im Zweifelsfall die Anzahl der Mitarbeiter in der zuständigen Abteilung, Gruppe/Bereich, Sektion oder der gesamten Einrichtung des Bundes anzunehmen.
- Ist die Anzahl der Nutzer für ein zu bewertendes IT-Verfahren nicht aussagekräftig, kann stattdessen auch die Durchschnittsnutzerzahl als Indikator angegeben und verwendet werden.
- Abgesehen von der Anzahl der Nutzer ist ebenso die Stellung der betroffenen Bediensteten innerhalb der Einrichtung des Bundes zu berücksichtigen (einschließlich Entscheidungsträger).
- Daher ist nicht nur auf quantitative Dimension zu achten, sondern auch die qualitative Komponente der betroffenen Nutzergruppe(n) zu berücksichtigen.
- Besonderen Stellenwert haben Nutzergruppen, die für die Erfüllung der Aufgaben der Einrichtung des Bundes gemäß BMG eine wesentliche Rolle spielen.

Konkrete Werte:

Anzahl der Nutzer in der Verwaltung

> XXX (größer einem zu bestimmenden Wert=Indikator für wichtigen Dienst, hängt direkt vom Dienst ab)

Sonstige Nutzer (Bürger/Unternehmer)

> YYY (größer einem zu bestimmenden Wert=Indikator für wichtigen Dienst, hängt direkt vom Dienst ab)

2.2.4 Art der verarbeitenden Daten

- Ein Kriterium zur Bestimmung der Wichtigkeit eines Dienstes kann die **Art der verarbeiteten Daten** sein. Dabei können insbesondere datenschutzrelevante oder informationssicherheitsrelevante Daten berücksichtigt werden.

- Ebenso ist zu berücksichtigen, ob die Daten **öffentlich zugänglich** sind oder nicht.
- Eine weitere Entscheidungshilfe ist die Frage, ob die Daten von einem **anderen IT-Verfahren auch zur Verfügung gestellt** werden.

Konkrete Werte:

Verarbeitung von **klassifizierten Dokumente** gemäß InfoSiG iVm InfoSiV und GehSO.

Klassifizierte Dokumente

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Verarbeitung von **besonderen Kategorien** von personenbezogenen Daten gemäß **Art. 9 DSGVO**

Auszug aus der DSGVO: „Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt."

Art.9 DSGVO

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO

Auszug aus der DSGVO: „Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist."

Art.10 DSGVO

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Verarbeitung von öffentlich nicht zugänglichen personenbezogenen Daten, welche die **finanzielle Situation** von Personen betreffen.

Finanzielle Daten

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Verarbeitung von öffentlich nicht zugänglichen personenbezogenen Daten, welche die **persönliche Stellung** bzw. **persönliche Beziehungen** von Personen untereinander betreffen.

Daten über persönliche Stellung

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Verarbeitung von öffentlich nicht zugänglichen **wettbewerbsrelevanten** Unternehmensdaten

Wettbewerbsrelevante Unternehmensdaten

Ja/Nein (Ja = Indikator für wichtigen Dienst)

2.2.5 Auswirkungen eines Sicherheitsvorfalls

- Ein maßgebliches Kriterium ist die Bestimmung und Bewertung eines Ausfalls oder der Einschränkung der Verfügbarkeit des Dienstes im Hinblick auf die **Erheblichkeit der Auswirkungen.**
- Eine wesentliche Indikation ist die Notwendigkeit des Dienstes für seine Nutzer bzw. die Ersetzbarkeit des Dienstes und wie zeitnah sich ein Sicherheitsvorfall beim Nutzer bemerkbar macht.

- Ebenfalls miteinzubeziehen ist die **Art der Auswirkung auf den Nutzer oder die Einrichtung des Bundes** selbst.
- Wenn **eine andere Einrichtung** der öffentlichen Verwaltung oder ein Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste durch den Sicherheitsvorfall bzw. Dienstausfall **seinen Dienst** bzw. Nutzen **ebenfalls nicht mehr erbringen** kann, so ist dieser Dienst ebenfalls als wichtiger Dienst zu kennzeichnen.

Nach dem Kriterium „Auswirkungen eines Sicherheitsvorfalls" liegt ein starkes Indiz für das Vorliegen eines wichtigen Dienstes vor, wenn einer der folgenden unten dargestellten Punkte erfüllt ist:

Konkrete Werte:

Auswirkungen eines Sicherheitsvorfalls auf die öffentliche Sicherheit, die Funktionsfähigkeit des (Rechts-)Staates oder die Daseinsvorsorge (Grundversorgung der Bevölkerung).

Es ist zu prüfen, ob der von der **Einrichtung des Bundes** bereitgestellte Dienst für die Daseinsvorsorge Österreichs unmittelbar relevant ist.

Daseinsvorsorge

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Es ist zu prüfen, ob der von der Einrichtung des Bundes bereitgestellte Dienst potentiellen Einfluss auf die Bereitstellung anderer wesentlicher, digitaler oder wichtiger Dienste hat, oder Voraussetzung dafür ist. In diesem Zusammenhang liegt ein starkes Indiz für einen wichtigen Dienst vor, wenn ein IT-Verfahren gemäß diesem Kriterium einen der folgenden Punkte erfüllt: Voraussetzung für andere wesentliche, digitale oder wichtige Dienste.

Wechselwirkung mit anderen Betreibern oder Anbietern

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Die Auswirkungen eines Sicherheitsvorfalls treten binnen zu definierenden **Stunden** ein. Dabei ist es unerheblich, welche Auswirkungen und in welcher Intensität diese eintreten.

Einschränkung der Verfügbarkeit oder Ausfall des betriebenen Dienstes binnen xx Std.

von/bis [Std]: Wert größer als zu definierende Std = Indikator für wichtigen Dienst

Die Auswirkungen eines Sicherheitsvorfalls können für die Einrichtung des Bundes **rechtliche Konsequenzen** nach sich ziehen (z.B. Datenschutz-, Amtshaftungs- bzw. Schadenersatz- oder EU-Vertragsverletzungsverfahren gegen die Republik).

Rechtliche Konsequenzen für Einrichtung

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Beim Ausfall oder der Einschränkung des wichtigen Dienstes ist von einem Reputationsverlust der Einrichtung des Bundes auszugehen.

Potentieller Ansehens- oder Vertrauensverlust

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Potentielle Medienberichterstattung

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Gesamter Stillstand einer hoheitlichen Tätigkeit in einem oder mehreren materiell rechtlichen Angelegenheiten. Dabei ist es unerheblich, wo örtlich und in welcher Einrichtung des Bundes sich die Bediensteten befinden.

Stillstand hoheitlicher Tätigkeit

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Auswirkungen eines Sicherheitsvorfalls auf die zeit- und sachgemäße Erledigung von Verwaltungstätigkeiten (insbesondere nach BMG).

Zeit- und sachgemäße Erledigung

Ja/Nein (Ja = Indikator für wichtigen Dienst)

Die Wiederherstellungszeit für das IT-Verfahren wurde vom Verfahrensverantwortlichen (z.B. mittels Lastenheft, Risikoanalyse, Informationssicherheitsanalyse, ...) auf kleiner gleich zu definierenden Stunden gesetzt.

Wiederherstellungszeit < Std.

von/bis [Std]: das Erreichen der max. Wiederherstellungszeit ist Indikator für wichtigen Dienst

3 Meldung von Sicherheitsvorfällen

3.1 Einleitung

Eine Einrichtung des Bundes hat einen Sicherheitsvorfall, der einen von ihr bereitgestellten wichtigen Dienst betrifft, unverzüglich zu melden.[5]

Ein „**Sicherheitsvorfall**" ist

- eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen,
- die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des wichtigen Dienstes
- mit erheblichen Auswirkungen geführt hat.[6]

Damit ein Sicherheitsvorfall vorliegt, müssen alle drei der oben genannten Voraussetzungen erfüllt sein.

Eine **Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen** kann beispielsweise neben Cyberangriffen oder Einwirkungen Dritter auch durch physische Ereignisse wie etwa Naturereignisse, aber auch durch Ereignisse wie z.B. Stromausfälle oder das Verhalten eigener Mitarbeiter verursacht werden.[7]

Die Begriffe „**Ausfall**" und „**Einschränkung der Verfügbarkeit**" wurden in der NISV[8] näher bestimmt:

- Ausfall bedeutet die Unverfügbarkeit des wichtigen Dienstes für Nutzer.[9]
- Einschränkung der Verfügbarkeit des wichtigen Dienstes bedeutet die signifikant geminderte Verfügbarkeit des wichtigen Dienstes in qualitativer Dimension für Nutzer.[10]

---

[5] § 22 Abs. 2 erster Satz NISG.
[6] § 3 Z 6 NISG.
[7] ErläutRV 369 BlgNR 26. GP 4.
[8] BGBl. II Nr. 215/2019.
[9] Vgl. § 3 Z 1 NISV.
[10] Vgl. § 3 Z 2 NISV.

- Bei der Ermittlung, ob **erhebliche Auswirkungen** vorliegen, sind pro wichtigen Dienst insbesondere folgende Parameter zu berücksichtigen: Die voraussichtliche
- Zahl der betroffenen Nutzer,[11]
- Dauer des Sicherheitsvorfalls,[12]
- Geografische Ausbreitung,[13]
- Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.[14]

Darüber hinaus kann auch die Art des Sicherheitsvorfalls als Parameter berücksichtigt werden.

Die Frage, ob eine erhebliche Auswirkung vorliegt, ist für jeden einzelnen wichtigen Dienst individuell zu beurteilen. Dabei kann ein oder können mehrere der oben angeführten Parameter herangezogen werden.

3.2 Parameter zur Beurteilung der Erheblichkeit von Auswirkungen

Im Folgenden werden die einzelnen im Kapitel 3.1 genannten Parameter näher beschrieben.

Zahl der betroffenen Nutzer

- Die „Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen", ist die Zahl der von einem Sicherheitsvorfall betroffenen natürlichen und juristischen Personen, mit denen ein Vertrag über die Bereitstellung des Dienstes abgeschlossen wurde, oder die Zahl der betroffenen Nutzer, die den Dienst im Zeitpunkt des Sicherheitsvorfalls genutzt haben oder für die voraussichtliche Dauer des Sicherheitsvorfalls nutzen würden.[15]
- Abhängig vom Vorfall können eine Teilmenge oder alle für diesen wichtigen Dienst ermittelten Nutzer betroffen sein. Zu definieren gilt es, ab welcher Menge ein erheblicher Sicherheitsvorfall vorliegt. Grundsätzlich gilt, je mehr Nutzer betroffen sind, desto eher ist ein Vorfall als Sicherheitsvorfall anzusehen.

---

[11] § 3 Z 6 lit. a NISG.
[12] § 3 Z 6 lit. b NISG.
[13] § 3 Z 6 lit. c NISG.
[14] § 3 Z 6 lit. d NISG.
[15] § 3 Z 3 NISV.

- Zu der Art der Nutzer gibt es keine Vorgaben, es kann sich um Bedienstete der Einrichtung oder um Institutionen, Bürger oder Unternehmen handeln.
- Ein Sicherheitsvorfall kann aber auch dann vorliegen, wenn nur wenige, aber wichtige Nutzergruppen des wichtigen Dienstes betroffen sind. Ein Kriterium zur Feststellung der Wichtigkeit der Nutzergruppen kann auch der Umstand sein, dass diese den wichtigen Dienst für die Bereitstellung ihrer eigenen Dienste benötigen, wobei wichtige Dienste anderer Einrichtungen des Bundes und wesentliche Dienste gemäß der NISV besondere Berücksichtigung finden können.

Konkrete Werte:

Betroffene Nutzer

von/bis [Anz] individuell zu bewerten, das Erreichen der festgelegten Anzahl ist ein (möglicher) Auslöser einer verpflichtenden Vorfallsmeldung

3.2.1 Dauer des Sicherheitsvorfalls

- Die „Dauer des Sicherheitsvorfalls" ist der in Stunden angegebene Zeitraum vom Ausfall oder von der Einschränkung der Verfügbarkeit des wichtigen Dienstes bis zum Zeitpunkt der uneingeschränkten Wiederherstellung.[16]
- Dieses Kriterium gibt an, wie lange ein wichtiger Dienst ausfallen oder eingeschränkt verfügbar sein kann, ehe ein Sicherheitsvorfall vorliegt. Erst wenn diese Dauer erreicht wurde, ist ein Vorfall auch tatsächlich ein meldepflichtiger Sicherheitsvorfall.

Konkrete Werte:

Dauer

von/bis [Std.] pro wichtigem Dienst zu bewerten; das Erreichen der festgelegten Dauer ist ein (möglicher) Auslöser für eine verpflichtende Vorfallsmeldung

[16] Vgl. § 3 Z 4 NISV.

3.2.2 Geografische Ausbreitung

- Die „geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet" bedeutet eine geografische Ausbreitung, bei der der Ausfall oder die Einschränkung der Verfügbarkeit des wichtigen Dienstes Gebiete in einem oder mehreren Mitgliedstaaten der EU oder der EFTA betrifft.[17]
- Je mehr Gebiete in einem oder mehreren Mitgliedstaaten der EU oder der EFTA betroffen sind, auch weil beispielsweise Nutzer aus diesen Gebieten auf den wichtigen Dienst zugreifen oder auf dessen Funktionsfähigkeit angewiesen sind, desto eher liegt ein Sicherheitsvorfall vor.

Konkrete Werte:

Ausbreitung

[Beschreibung] Bspw. Anzahl anderer betroffener Mitgliedstaaten oder Regionen. Das Auslösen einer verpflichtenden Vorfallsmeldung hängt von der Tragweite und Schwere des Kriteriums „Geografische Ausbreitung" ab.

Auswirkung auf wirtschaftliche und gesellschaftliche Tätigkeiten

- „Auswirkung auf wirtschaftliche und gesellschaftliche Tätigkeiten" sind jegliche nachteiligen Auswirkungen auf Einrichtungen und Personen, insbesondere betroffene Nutzer, unabhängig davon, ob diese Auswirkungen materielle oder immaterielle Verluste für diese verursacht haben.[18]
- An dieser Stelle ist zu bewerten, welche Auswirkungen ein Sicherheitsvorfall auf die wirtschaftliche und gesellschaftliche Tätigkeit hat, auch die der Einrichtung des Bundes selbst. Unter gesellschaftlicher Tätigkeit kann bei Einrichtungen des Bundes gegebenenfalls auch die politische Tätigkeit verstanden werden.
- Als Kriterium kann berücksichtigt werden, welchen Einfluss ein Sicherheitsvorfall für die Nutzer eines wichtigen Dienstes direkt oder indirekt hat. Je störender sich ein Vorfall auf das tägliche Leben oder die Arbeitstätigkeit der Nutzer auswirkt, desto eher ist ein Vorfall als Sicherheitsvorfall zu bewerten.

[17] Vgl. § 3 Z 5 NISV.
[18] Vgl. § 3 Z 6 NISV.

- Es kann sein, dass sich ein Vorfall auf verschiedene Nutzergruppen unterschiedlich auswirkt. In diesem Fall ist jede Nutzergruppe samt die zu erwartenden Auswirkungen zu dokumentieren. Die Einstufung eines Vorfalls ergibt sich aus der Wichtigkeit der Nutzergruppe und aus der Summe aller Auswirkungen auf die unterschiedlichen Nutzergruppen.

Konkrete Werte:

Wirtschaftlich

[Beschreibung] Das Auslösen einer verpflichtenden Vorfallsmeldung hängt von der Tragweite und Schwere des Kriteriums „Wirtschaftliche Auswirkungen" ab.

Gesellschaftlich

[Beschreibung] Das Auslösen einer verpflichtenden Vorfallsmeldung hängt von der Tragweite und Schwere des Kriteriums „Gesellschaftliche Auswirkungen" ab.

Politisch

[Beschreibung] Das Auslösen einer verpflichtenden Vorfallsmeldung hängt von der Tragweite und Schwere des Kriteriums „Politische Auswirkungen" ab.

3.2.3 Art des Sicherheitsvorfalls

- In seiner Definition des Begriffes Sicherheitsvorfall unterscheidet das NISG hinsichtlich der Art eines Sicherheitsvorfalls dahingehend, ob Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit gestört ist. Vorfälle, die diese einzelnen Indikatoren betreffen, sind nicht unbedingt gleichwertig zu betrachten.
- Vorfälle, welche die Integrität, Authentizität und Vertraulichkeit betreffen, können prinzipiell als schwerwiegender eingestuft werden, was im Hinblick auf die Parameter für die Beurteilung der erheblichen Auswirkungen entsprechend berücksichtigt werden kann.

Konkrete Werte:

Verfügbarkeit:

Ja/Nein, das Ergebnis „Ja" ist ein (möglicher) Auslöser für eine Vorfallsmeldung

Integrität/Authentizität/Vertraulichkeit:

Ja/Nein, das Ergebnis „Ja" ist ein Auslöser für eine verpflichtende Vorfallsmeldung

3.3 Meldeprozess für Einrichtungen des Bundes

3.3.1 Pflichtmeldungen und freiwillige Meldungen

Jede Einrichtung des Bundes hat einen Sicherheitsvorfall, der einen von ihr bereitgestellten wichtigen Dienst betrifft, unverzüglich zu melden (**Pflichtmeldung**).[19]

Risiken[20] und Vorfälle[21] hingegen können auf freiwilliger Basis gemeldet werden (**freiwillige Meldung**).[22]

[19] § 22 Abs. 2 NISG.
[20] S. § 3 Z 8 NISG.
[21] S. § 3 Z 7 NISG.
[22] § 22 Abs. 3 NISG.

3.3.2 GovCERT- und IKDOK-Meldungen

Abhängig von der Einrichtung des Bundes kann zwischen IKDOK-Meldungen und GovCERT-Meldungen unterschieden werden.

Grundsätzlich hat jede Einrichtung des Bundes Pflicht- und freiwillige Meldungen an das GovCERT[23] zu melden (**GovCERT-Meldungen**).[24]

Davon ausgenommen sind lediglich das BKA, BMI, BMLV und BMEIA, weil diese im IKDOK vertreten sind[25] und die Pflicht- und freiwilligen Meldungen daher im Rahmen des IKDOK abzusetzen haben (**IKDOK-Meldungen**).[26]

3.3.3 Meldungsinhalt von Pflichtmeldungen

Die Pflichtmeldung muss sämtliche relevante Angaben zum Sicherheitsvorfall und den technischen Rahmenbedingungen, die im Zeitpunkt der **Erstmeldung** bekannt sind, enthalten. Dabei handelt es sich insbesondere um die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage. Angaben über später bekanntgewordene Umstände zum Sicherheitsvorfall sind in **Nachmeldungen** und letztendlich in einer **Abschlussmeldung** ohne unangemessene weitere Verzögerung mitzuteilen.[27]

Zwischen GovCERT- und IKDOK-Meldungen besteht zum Meldungsinhalt kein Unterschied.

---

[23] Das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) ist beim Bundeskanzler eingerichtet. Gemäß § 14 Abs. 4 NISG kommen dem GovCERT neben der Entgegennahme und Weiterleitung von Meldungen gemäß § 22 Abs. 2 und 3 die Aufgaben gemäß § 14 Abs. 2 Z 3 bis 5 und Abs. 3 zweiter Satz NISG in Hinblick auf die Einrichtungen der öffentlichen Verwaltung, soweit es sich dabei nicht um eine im IKDOK vertretene Einrichtung handelt, zu.

[24] § 22 Abs. 2 erster Satz NISG.

[25] § 3 Z 4 iVm § 7 NISG.

[26] § 22 Abs. 2 dritter Satz NISG.

[27] § 22 Abs. 2 zweiter Satz iVm § 19 Abs. 3 NISG.

3.3.4 Meldungsinhalt von freiwilligen Meldungen

Zum Inhalt der freiwilligen Meldung gilt sinngemäß das oben zum Meldungsinhalt von Pflichtmeldungen Ausgeführte.[28] Die freiwillige Meldung muss jedoch weder die Identität der Einrichtung, noch Informationen, die auf diese schließen lassen, enthalten.[29]

Die freiwillige meldende Einrichtung des Bundes kann personenbezogene Daten gemäß § 9 Abs. 3 Z 2 NISG, das sind Kontakt- und Identitätsdaten sowie technische Daten von Personen, die mit einer Meldung zu einem Risiko, Vorfall oder Sicherheitsvorfall in Zusammenhang stehen, wie insbesondere Opfer und Angreifer, an das GovCERT übermitteln.[30]

3.3.5 NIS-Meldeportal

Meldungen über Risiken, Vorfälle und Sicherheitsvorfälle in der öffentlichen Verwaltung können über das NIS-Meldeportal unter nis.govcert.gv.at eingebracht werden.

Dazu ist die entsprechende Art der Meldung (Pflicht- oder freiwillige Meldung) auszuwählen und das entsprechende Meldeformular zu befüllen, sodass gegebenenfalls bestmöglich bei der Behandlung unterstützt werden kann.

[28] § 22 Abs. 3 zweiter Satz iVm § 23 Abs. 4 zweiter Satz NISG.
[29] § 23 Abs. 4 erster Satz NISG.
[30] § 23 Abs. 5 NISG.

4 Sicherheitsvorkehrungen

Zur Gewährleistung der Netz- und Informationssystemsicherheit haben Einrichtungen des Bundes in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung wichtiger Dienste nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.[31]

Es ist dem Verantwortungsbereich der jeweiligen Einrichtung des Bundes belassen, welche Maßnahmen sie zur Gewährleistung der Netz- und Informationssystemsicherheit trifft.

Ein Nachweismechanismus, wie er für Betreiber wesentlicher Dienste vorgeschrieben ist,[32] besteht für Einrichtungen des Bundes nicht. Es obliegt daher der Entscheidung der Einrichtungen des Bundes, ob sie beispielsweise ein Self Assessment vornimmt oder ein internes oder externes Audit durchführen lässt.

In der NISV werden die Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste festgelegt.[33] Diese Sicherheitsvorkehrungen sind geeignet und berücksichtigen den Stand der Technik. Sie setzen sich aus insgesamt 29 Sicherheitsmaßnahmen zusammen, die elf Kategorien zugeordnet sind. In der Anlage 1 zur NISV werden die Sicherheitsmaßnahmen näher konkretisiert.

Die Sicherheitsvorkehrungen in der NISV sind ausschließlich von Betreibern wesentlicher Dienste verpflichtend umzusetzen. Nachdem die Sicherheitsvorkehrungen in der NISV jedoch *per legem* „geeignet sind und den Stand der Technik berücksichtigen" und die Texte der §§ 17 und 22 NISG ident sind, scheint eine Orientierung an den Vorgaben für die Betreiber wesentlicher Dienste zweckmäßig.

Um die Betreiber wesentlicher Dienste bei der Umsetzung der Sicherheitsmaßnahmen aus der NISV zu unterstützen, wurden vom BKA und BMI zwei NIS Fact Sheets herausgegeben. Im **NIS Fact Sheet 08/2019** über „Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste" findet sich eine nähere Erläuterung der in der NISV genannten Sicherheitsmaßnahmen.

---

[31] § 22 Abs. 1 NISG.
[32] § 17 Abs. 3 NISG.
[33] § 11 Abs. 1 NISV iVm § 17 Abs. 1 NISG.

Der **NIS Fact Sheet 08/2018** stellt in Form einer „Mapping-Tabelle" eine Gegenüberstellung der einzelnen Sicherheitsmaßnahmen der NISV mit bestehenden nationalen und internationalen IKT-Sicherheitsstandards wie auch mit Cyber Security Best Practices zur Verfügung.

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Autoren: Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS)
Wien, 2019
Stand: 22. August 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.