Sicherheitsvorkehrungen und Meldepflicht für Anbieter digitaler Dienste

§ 21. (1) Zur Gewährleistung der NIS haben Anbieter digitaler Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, das dem bestehenden mit vernünftigem Aufwand feststellbaren Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) Sicherheit der Systeme und Anlagen,

b) Bewältigung von Sicherheitsvorfällen,

c) Betriebskontinuitätsmanagement,

d) Überwachung, Überprüfung und Erprobung,

e) Einhaltung der internationalen Normen.

(2) Anbieter digitaler Dienste haben einen Sicherheitsvorfall, der einen von ihnen bereitgestellten digitalen Dienst betrifft, unverzüglich an das nationale Computer-Notfallteam, sofern ein solches eingerichtet ist, ansonsten an das GovCERT zu melden, das die Meldung unverzüglich an den Bundesminister für Inneres weiterleitet. Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten. § 19 Abs. 3 gilt sinngemäß.

(3) Wenn ein Sicherheitsvorfall bei einem Anbieter digitaler Dienste einen oder mehrere andere Mitgliedstaaten der Europäischen Union betrifft, hat der Bundesminister für Inneres oder das zuständige Computer-Notfallteam gemäß Abs. 2 im Wege der zentralen Anlaufstelle (SPOC) die zentrale Anlaufstelle in diesen Mitgliedstaaten darüber zu unterrichten.

(4) Der Bundesminister für Inneres ist, wenn ihm nachweisliche Umstände bekannt werden, dass ein Anbieter digitaler Dienste seinen Pflichten gemäß Abs. 1 nicht nachkommt, ermächtigt zu verlangen, dass dieser Nachweise über geeignete Sicherheitsvorkehrungen erbringt. Zu diesem Zweck stellt der betroffene An-

bieter digitaler Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen zur Verfügung. Der Bundesminister für Inneres kann dazu auch Einschau in die Netz- und Informationssysteme, die für die Bereitstellung des digitalen Dienstes genutzt werden, und diesbezügliche Unterlagen nehmen. § 17 Abs. 4 zweiter und dritter Satz gilt. Zur Herstellung der Anforderungen nach Abs. 1 ist der Bundesminister für Inneres ermächtigt, Empfehlungen auszusprechen, für deren Befolgung und entsprechenden Nachweis erforderlichenfalls eine angemessene Frist zu setzen ist, widrigenfalls die Befolgung bescheidmäßig angeordnet wird.

Stammfassung.

Materialien: Art 16 und 17 NIS-RL; ErläutRV 369 BlgNR 26. GP 21.

Übersicht

I. Sicherheitsvorkehrungen für Anbieter digitaler Dienste

A. Anforderungen aus der NIS-RL

Da Anbieter digitaler Dienste einem auf EU-Ebene stärker harmonisierten Konzept unterliegen (s Rz 92), kommt den **Anforderungen aus der NIS-RL** eine höhere Bedeutung zu als bei Betreibern wesentlicher Dienste. **1**

Art 16 Abs 1 NIS-RL sieht vor, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen müssen. Diese sollen die Risiken für die Sicherheit der Netz- und Informationssysteme, die die Anbieter im Rahmen der Bereitstellung der digitalen Dienste (Art 4 Nr 5 NIS-RL) nutzen, bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Die NIS-RL nimmt an, dass in der Praxis das **2**

Risiko für Betreiber wesentlicher Dienste, die oftmals für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind, höher als das Risiko für Anbieter digitaler Dienste ist. Deshalb sollten die an Anbieter digitaler Dienste gestellten Sicherheitsanforderungen geringer sein (ErwGr 49 NIS-RL).

Im Unterscheid zu den Betreibern wesentlicher Dienste (Art 14 Abs 1 NIS-RL) sieht Art 16 Abs 1 NIS-RL bestimmte Elemente vor, die bei den Sicherheitsanforderungen zu berücksichtigen sind, nämlich

a) Sicherheit der Systeme und Anlagen,

b) Bewältigung von Sicherheitsvorfällen,

c) Betriebskontinuitätsmanagement,

d) Überwachung, Überprüfung und Erprobung sowie

e) Einhaltung der internationalen Normen.

3 Fast gleichlautend wie bei den Betreibern (Art 14 Abs 2 NIS-RL) bestimmt Art 16 Abs 2 NIS-RL, dass den Auswirkungen von Sicherheitsvorfällen vorgebeugt bzw diese so gering wie möglich gehalten werden, um die Verfügbarkeit der digitalen Dienste zu gewährleisten.

4 Es gilt zu beachten, dass die MS den Anbietern digitaler Dienste gem Art 16 Abs 10 NIS-RL keine weiteren Sicherheits- oder Meldepflichten auferlegen dürfen, womit dieser Bereich der NIS-RL **vollharmonisiert** ist. Aus diesem Grund besitzen die in § 11 NISV aufgelisteten Sicherheitsmaßnahmen für Anbieter digitaler Dienste auch keine rechtliche Relevanz, doch ergeben sich in der Praxis natürlich zahlreiche Überschneidungen. Dies liegt in dem Umstand begründet, dass sich die in § 11 NISV genannten Sicherheitsmaßnahmen an international anerkannten Standards orientieren und Anbieter digitaler Dienste aufgrund ihrer grenzüberschreitenden Tätigkeit in erster Linie auf internationale Standards zurückgreifen werden bzw dies bereits jetzt tun. Auch finden sich die in Art 2 der Durchführungsverordnung (EU) 2018/15 (s sogleich) genannten Sicherheitselemente in den Sicherheitsmaßnahmen gemäß NISV wieder, wie bspw Risikoanalyse, Sicherheitsarchitektur und das Betriebskontinuitätsmanagement. Anbietern digitaler Dienste ist es generell freigestellt, die Maßnahmen zu ergreifen, die sie für angemessen halten (ErwGr 49 NIS-

RL und ErläutRV 21), weshalb sie auch die in § 11 NISV aufgelisteten Sicherheitsmaßnahmen zur Umsetzung heranziehen können.

B. Nationale Umsetzung

Wie auch schon bei den Betreibern wurden die Sicherheitsanforderungen in der nationalen Umsetzung mit einem anderen Wortlaut versehen, ohne inhaltlich einen wesentlichen Unterschied herbeizuführen. Gem Abs 1 sind die Anbieter digitaler Dienste verpflichtet, in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Auch diese haben den Stand der Technik zu berücksichtigen und müssen dem Risiko angemessen sein. **5**

Wie bei den Betreibern wesentlicher Dienste ist die Pflicht, Sicherheitsvorkehrungen zu treffen, auf die Netz- und Informationssysteme eingeschränkt, die sie für die Bereitstellung des digitalen Dienstes nutzen. Die digitalen Dienste sind in den Begriffsbestimmungen definiert (s § 3 Z 15, 16 und 17). **6**

Zur allgemeinen Rechtfertigung der Datenverarbeitung durch Anbieter digitaler Dienste s § 9 Rz 11, zur Abgrenzung der Datensicherheits-Verpflichtungen nach der DSGVO s § 17 Rz 11 f sowie zur Abgrenzung zu DSGVO-Meldepflichten s § 19 Rz 17 ff. **7**

C. Durchführungsverordnung (EU) 2018/15

Nach ErwGr 49 unterliegen Anbieter digitaler Dienste aufgrund des grenzüberschreitenden Charakters ihrer Tätigkeiten einem auf Unionsebene stärker harmonisiertem Konzept. Dementsprechend sieht Art 16 Abs 8 NIS-RL vor, dass die Europäische Kommission Durchführungsrechtsakte zu erlassen hat, um die in Art 16 Abs 1 genannten Elemente genauer zu bestimmen. Dies soll zu einer einheitlichen Behandlung der Anbieter digitaler Dienste in der EU führen (ErwGr 57 NIS-RL). Der Durchführungsrechtsakt hätte bis zum 9. 8. 2017 erlassen werden sollen, wurde aber erst am 30. 1. 2018 von der Kommission als **Durchführungsverordnung (EU) 2018/15,** ABl L 2018/26, 48 (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1539) angenommen. In dieser Durchführungsverordnung werden ua die og Elemente näher festgelegt, die die Anbieter digitaler Dienste zu berücksichtigen haben, wenn sie Maßnahmen ermitteln und ergreifen, die ein bestimmtes Sicher- **8**

heitsniveau der Netz- und Informationssysteme gewährleisten (Art 1).

9 Nach Art 2 Abs 1 umfasst die Sicherheit der Systeme und Anlagen

1. das systematische Management von Netz- und Informationssystemen durch die Erfassung und Abbildung der Informationssysteme und die Einführung einer Reihe von geeigneten Maßnahmen für das Management der Informationssicherheit, wobei dies explizit Risikoanalyse, Humanressourcen, Betriebssicherheit, Sicherheitsarchitektur, Lebenszyklus-Management gesicherter Daten und Systeme sowie gegebenenfalls Verschlüsselung und Verschlüsselungsmanagement erfasst,
2. die physische Sicherheit und die Sicherheit der Umgebung, wobei ein risikobasierter Allgefahrenansatz, der bspw Systemversagen, menschliche Fehler, böswillige Handlungen oder Naturereignisse berücksichtigt, zu verfolgen ist,
3. die Versorgungssicherheit, worunter die Gewährleistung der Zugänglichkeit und gegebenenfalls der Rückverfolgbarkeit unentbehrlicher Güter oder Vorleistungen, die für die Bereitstellung der Dienste genutzt werden, verstanden wird,
4. die Kontrolle des Zugangs zu Netz- und Informationssystemen, dh die Genehmigung und Einschränkung des physischen und logischen Zugangs zu Netz- und Informationssystemen sowie die Gewährleistung der administrativen Sicherheit.

10 Die Sicherheitsvorkehrungen zur **Bewältigung von Sicherheitsvorfällen** haben gem Art 2 Abs 2 Folgendes zu umfassen:

1. Erkennungsprozesse und -verfahren, die aufrechtzuerhalten und zu erproben sind und die eine rechtzeitige und angemessene Lageerfassung gewährleisten sollen.
2. Meldeprozesse und die Feststellung von Schwachstellen und Anfälligkeiten.
3. Die verfahrensgemäße Reaktion und eine Berichterstattung über die Ergebnisse der ergriffenen Maßnahme(n).
4. Bewertung der Schwere des Sicherheitsvorfalls und Dokumentation sowie Informationssammlung, insbesondere um auf Basis von Erkenntnissen Verbesserungsprozesse zu fördern.

11 Das Betriebskontinuitätsmanagement wird in Art 2 Abs 3 definiert als „die Fähigkeit einer Organisation zur Aufrechterhaltung bzw

Wiederherstellung der Erbringung von Diensten auf einem zuvor festgelegten akzeptablen Niveau nach einer Störung" und hat Nachfolgendes zu umfassen:

1. Notfallpläne, die auf der Grundlage einer Analyse der betrieblichen Auswirkungen zur Gewährleistung der Kontinuität zu erstellen und anzuwenden sind und die auch regelmäßig bewertet und zB durch Übungen zu erproben sind.
2. Wiederherstellungskapazitäten.

12 Die Überwachung, Überprüfung und Erprobung umfassen folgende Maßnahmen:

1. Kontrollen oder Messungen zur Beurteilung, ob die Netz- und Informationssysteme bestimmungsgemäß funktionieren.
2. Kontrolle und Überprüfung der Befolgung von Normen und Leitlinienkatalogen, der Korrektheit von Aufzeichnungen und der Erfüllung von Effizienz- und Wirksamkeitsvorgaben.
3. Prozesse zur Feststellung von Mängeln in den Sicherheitsmechanismen eines Netz- und Informationssystems, wobei die Prozesse neben technischen Verfahren auch das Personal zu umfassen haben.

13 Bezüglich der **Einhaltung der internationalen Normen** bestimmt Art 2 Abs 5, dass es sich hierbei um von einer internationalen Normungsorganisation angenommene Normen handelt, aber auch gem Art 19 NIS-RL europäische oder international anerkannte Normen und Spezifikationen sowie bestehende nationale Normen verwendet werden können.

14 Die ENISA hat im Februar des Jahres 2017 einen Bericht veröffentlicht, der die Anbieter digitaler Dienste (und die MS) bei der Festlegung eines gemeinsamen Ansatzes für die Sicherheitsmaßnahmen unterstützen soll. Es werden gemeinsame grundlegende Sicherheitsziele für Anbieter digitaler Dienste und verschiedene Sicherheitsmaßnahmen beschrieben, mit denen diese Sicherheitsziele erfüllt werden können. Ferner enthält das Dokument ein Mapping bekannter Standards, nationaler Rahmenbedingungen und Zertifizierungssysteme. Der Bericht ist abrufbar unter https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/.

15 Anbieter digitaler Dienste unterliegen keiner Nachweispflicht wie Betreiber wesentlicher Dienste (vgl § 17 Abs 3).

II. Meldepflicht für Anbieter digitaler Dienste

16 Anbieter digitaler Dienste unterliegen einer Meldepflicht von Sicherheitsvorfällen (§ 3 Z 6). Diese sind unverzüglich an das nationale Computer-Notfallteam (s https://nis.cert.at/) zu melden, das die Meldung unverzüglich an den BMI weiterzuleiten hat (Abs 2).

17 Gem Art 16 Abs 3 NIS-RL ist jeder Sicherheitsvorfall zu melden, der erhebliche Auswirkungen auf die Bereitstellung des Dienstes hat. Zur Feststellung der Erheblichkeit der Auswirkungen gibt Art 16 Abs 4 demonstrativ **Parameter** vor, die es zu berücksichtigen gilt. Diese Parameter werden in Art 3 Durchführungsverordnung (EU) 2018/15 wie folgt näher bestimmt:

- Bei der **Zahl der von dem Sicherheitsvorfall betroffenen Nutzer** muss der Anbieter digitaler Dienste in der Lage sein, eine Schätzung vorzunehmen. Der Parameter umfasst die Zahl der 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 genutzt haben, wobei für Letzteres insb frühere Verkehrsdaten zugrunde zu legen sind.
- Die **Dauer eines Sicherheitsvorfalls** wird definiert als die Zeitspanne von der Unterbrechung der ordnungsgemäßen Bereitstellung des Dienstes in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit bis zum Zeitpunkt der Wiederherstellung.
- Bei der **geografischen Ausbreitung** in Bezug auf das vom Sicherheitsvorfall betroffene Gebiet muss der Anbieter digitaler Dienste in der Lage sein zu ermitteln, ob der Sicherheitsvorfall die Bereitstellung seiner Dienste in bestimmten MS beeinträchtigt.
- Für das **Ausmaß der Unterbrechung** der Bereitstellung des Dienstes wird lediglich vorgegeben, dass diese anhand von Merkmalen, die durch den Sicherheitsvorfall beeinträchtigt werden, nämlich die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten oder entsprechender Dienste zu beurteilen ist.
- Zum **Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten** wird vorgegeben, dass der Anbieter digitaler Dienste aufgrund von Angaben wie der Art der vertraglichen Beziehungen mit dem Kunden oder der potenziellen Zahl der Nutzer feststellen können muss, ob der Sicherheitsvorfall zu erheblichen materiellen oder immateriellen Verlusten – zB die Ge-

sundheit, Sicherheit oder Sachschäden betreffend – für die Nutzer geführt hat.

Art 4 Durchführungsverordnung (EU) 2018/15 regelt, wann ein Sicherheitsvorfall (§ 3 Z 6) **erhebliche Auswirkungen** hat und somit meldepflichtig ist. Dies ist der Fall, wenn mindestens einer der folgenden Fälle eingetreten ist: **18**

- Der Dienst war mehr als 5.000.000 Nutzerstunden lang nicht verfügbar, wobei „Nutzerstunde" als die Zahl der Nutzer in der EU, die für die Dauer einer Stunde betroffen waren, definiert ist.
- Mehr als 100.000 Nutzer in der EU sind von dem Sicherheitsvorfall betroffen.
- Der Sicherheitsvorfall hat zu einer öffentlichen Gefahr oder einem Risiko für die öffentliche Sicherheit geführt oder es sind Menschen ums Leben gekommen.
- Mindestens ein Nutzer in der EU hat einen Sachschaden in Höhe von mehr als 1.000.000 EUR infolge eines Sicherheitsvorfalls erlitten.

Im Vergleich zu Betreibern wesentlicher Dienste unterliegen Anbieter digitaler Dienste der Meldepflicht nur insofern, als sie **Zugang zu Informationen** haben, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten (Art 16 Abs 4 NIS-RL, umgesetzt in Abs 2 zweiter Satz NISG). Ähnlich normiert Art 3 Abs 6 Durchführungsverordnung (EU) 2018/15, dass sie nicht verpflichtet sind, zusätzliche Informationen einzuholen, die ihnen nicht zugänglich sind. Somit ergibt sich die paradoxe Situation, dass ein Anbieter digitaler Dienste einerseits in der Lage sein muss, bestimmte Parameter zu schätzen oder ermitteln; andererseits muss er dies nur auf Basis von Informationen können, die ihm zugänglich sind. Es bleibt zu fragen, wie die zuständigen Behörden die Einhaltung der Meldepflicht beaufsichtigen werden – wozu sie nach Art 17 NIS-RL verpflichtet sind –, wenn ein Anbieter digitaler Dienste sich auf den Standpunkt zurückzieht, dass ihm die notwendigen Informationen nicht vorlagen und er auch keiner Pflicht unterlag, sich Zugang zu diesen zu verschaffen. Verschärfend tritt der Umstand hinzu, dass der BMI die Überwachungsmaßnahmen nur ex post treffen darf und die MS Anbieter digitaler Dienste nicht bestimmen bzw ermitteln sollen (vgl ErwGr 57 NIS-RL). Erfüllen Anbieter digitaler Dienste ihre Meldepflicht daher nicht, so wird den zuständigen Behörden ihre Existenz unter Umständen verbor- **19**

gen bleiben und die Nichteinhaltung der Meldepflicht schwerlich verfolgbar sein. Es wird sich zeigen, ob die NIS-RL bei Anbietern digitaler Dienste zu einer tatsächlichen Erhöhung der NIS führen wird. Um ihrer Aufsichtstätigkeit nachkommen zu können, sollten die zuständigen Behörden der MS daher den Markt auf mögliche Anbieter digitaler Dienste hin untersuchen. Auch wenn die MS die Anbieter grundsätzlich nicht selbst bestimmen bzw ermitteln sollen, bedeutet dies nicht, dass sie nicht eine Liste möglicher Adressaten erstellen können. Der Argumentation, dass dem Anbieter die notwendigen Informationen nicht vorlagen und er auch keiner Pflicht unterlag, sich Zugang zu diesen zu verschaffen, um das Überschreiten der Meldeschwellenwerte zu beurteilen, ist entgegenzuhalten, dass man davon ausgehen kann, dass digitalen Diensteanbietern wohl jedenfalls Informationen über die Anzahl der Nutzer, die den Dienst aktuell nutzen, vorliegen.

20 Die NISV stützt sich auf § 4 Abs 2 NISG und enthält folglich prinzipiell nur Bestimmungen, die für Betreibern wesentlicher Dienste gelten. Dies gilt jedenfalls für den 2. und 3. Abschnitt der NISV. Da die Begriffsbestimmung des Sicherheitsvorfalls in § 3 Z 6 NISG nicht auf Betreiber beschränkt ist, gilt § 3 NISV, der Begriffsbestimmungen zu Sicherheitsvorfällen enthält und das NISG in diesem Punkt konkretisiert, auch für Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung. Solche näheren Durchführungen in einer VO sind im Hinblick auf Art 18 Abs 2 B-VG als zulässig zu betrachten. Die in der NISV festgelegten Begriffsbestimmungen zu Sicherheitsvorfällen haben jedoch aufgrund des Anwendungsvorrangs von Unionsrecht im Hinblick auf Anbieter digitaler Dienste insoweit unanwendbar zu bleiben, als die Durchführungsverordnung (EU) 2018/15 anderes bestimmt. So sind zB die Dauer des Sicherheitsvorfalls und Nutzerstunden abweichend definiert.

21 Zum vorgesehenen Inhalt einer verpflichtenden Meldung wird auf die Ausführungen zu § 19 Abs 3 verwiesen (s Rz 19ff), zum Inhalt der freiwilligen Meldung von Risiken und Vorfällen auf die Ausführungen zu § 23 Abs 4 und 5 (s Rz 7).

22 Hat ein Sicherheitsvorfall bei einem Anbieter einen **grenzüberschreitenden Bezug,** so sind die zentralen Anlaufstellen in den betroffenen MS im Wege der zentralen Anlaufstelle (SPOC, s § 6) über diesen Sicherheitsvorfall zu informieren (Abs 3). Bei Anbietern digi-

taler Dienste wird infolge des grenzüberschreitenden Charakters digitaler Dienste eine Betroffenheit anderer MS wahrscheinlicher sein als bei Betreibern wesentlicher Dienste oder einer Einrichtung der öffentlichen Verwaltung.

Die Kooperationsgruppe hat im Juli 2018 ein Dokument erstellt und veröffentlicht, das unverbindliche technische Leitlinien für die zuständigen Behörden enthält, wie die Meldepflicht von Anbietern digitaler Dienste aufsichtsrechtlich umgesetzt und wie andere MS im Falle grenzüberschreitender Auswirkungen informiert werden können. Das Dokument ist online abrufbar unter https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. **23**

Die ENISA hat im Februar 2017 einen umfassenden Leitfaden für Anbieter digitaler Dienste herausgegeben, wie die Anforderungen an die Meldepflicht umgesetzt werden können. Der Leitfaden ist online abrufbar unter https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/. **24**

III. Aufsicht über Anbieter digitaler Dienste

Im Vergleich zu Betreibern wesentlicher Dienste unterliegen Anbieter digitaler Dienste einer weniger strikten **Aufsicht:** **25**

So unterliegen sie keiner Nachweispflicht im Hinblick auf ihre Sicherheitsvorkehrungen, wie dies Betreiber wesentlicher Dienste tun (vgl § 17 Abs 3). Der BMI darf nur dann tätig werden, wenn ihm nachweisliche Umstände zur Kenntnis gelangen, dass ein Anbieter digitaler Dienste die Sicherheitsanforderungen nicht erfüllt. Der BMI kann seine Aufsichtstätigkeit daher nur reaktiv (ex post) wahrnehmen und hat somit keine generelle Verpflichtung zur Beaufsichtigung. Nach Art 17 Abs 1 NIS-RL darf die zuständige Behörde nämlich nur im Wege von **ex-post**-Überwachungsmaßnahmen tätig werden. Gerechtfertigt wird dies durch die Art ihrer Dienste und Tätigkeiten (ErwGr 60 NIS-RL). **26**

Der BMI wird insb im Falle des Erhalts einer Meldung über einen Sicherheitsvorfall **Kenntnis** erlangen und Aufsichtsmaßnahmen einleiten. Nachweisliche Umstände können dem BMI bspw auch durch den Anbieter digitaler Dienste selbst oder einen von dessen Angestellten, durch einen Mitbewerber, durch eine andere Behörde – auch der eines anderen EU-MS – oder durch einen Nutzer des Dienstes bekannt werden. **27**