TT, November 2018

Die Auswirkungen der NIS-Richtlinie[1] für Unternehmer

Die europäische NIS-Richtlinie hätte von den Mitgliedstaaten der Europäischen Union bis zum 9.5.2018 umgesetzt werden müssen. Derzeit liegt ein Entwurf des nationalen Umsetzungsgesetzes vor. In diesem Artikel werden die wichtigsten Punkte dieses Gesetzes für Sie kompakt zusammengefasst.

Zum Stand des Gesetzgebungsverfahrens

Mit der „Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (in der Folge: „NIS-RL") soll unionsweit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden[2]. Die NIS-RL wird durch das „Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen" (in der Folge: „NISG") in nationales Recht umgesetzt werden. Der Entwurf zu diesem Gesetz wurde bereits veröffentlicht[3]. **Die folgenden Erläuterungen beziehen sich stets auf diesen Entwurf. Es ist möglich, dass die Endfassung des Gesetzes vom Entwurf abweicht**.

Betreiber eines wesentlichen Dienstes

Das NISG wendet sich an (i) **Betreiber wesentlicher Dienste** in den Sektoren

- Energie,
- Verkehr,
- Bankwesen,
- Finanzmarktinfrastrukturen,
- Gesundheitswesen,
- Trinkwasserversorgung und
- Digitale Infrastruktur.

Ausdrücklich ist darauf hinzuweisen, dass nicht jedes Unternehmen, das in einer der genannten Branchen tätig ist, in den Anwendungsbereich des NISG fällt. Dies ist nur dann

[1] Stand Entwurf 78/ME XXVI. GP – Ministerialentwurf – Erläuterungen.
[2] Erläuterungen zum Entwurf 78/ME XXVI. GP – Ministerialentwurf – Erläuterungen, S 1.
[3] https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00078/index.shtml (Stand 2.10.2018).

der Fall, wenn ein „**wesentlicher Dienst**" betrieben wird. Ob der Betrieb „wesentlich" in diesem Sinne ist, ist insbesondere anhand nachstehender Kriterien[4] zu beurteilen:

- Zahl der Nutzer;
- Abhängigkeit anderer in den oben genannten Sektoren vom Betrieb;
- Marktanteil des Betriebs;
- Geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;
- Auswirkungen von Sicherheitsvorfällen hinsichtlich Ausmaß und Dauer auf wirtschaftlich oder gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit;
- Bedeutung des Betreibers wesentlicher Dienste für die Aufrechterhaltung des Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes;
- Berücksichtigung sektorspezifischer Faktoren.

Sofern ein Betrieb einen wesentlichen Dienst erbringt, **wird dieser vom Bundeskanzler mit Bescheid ermittelt** werden[5]. Die Qualifikation als Betreiber eines wesentlichen Dienstes setzt im Übrigen eine feste Einrichtung in Österreich voraus[6]. Die spezifischen Sicherheitsanforderungen des NISG sollen sich nur auf jene Bereiche eines Unternehmens beziehen, die auf einen „wesentlichen Dienst" im Sinne dieses Gesetzes Bezug nehmen[7]. Die Bereitstellung des „Einkaufsbereichs" ist damit beispielsweise nicht vom NISG erfasst[8].

Anbieter digitaler Dienste

Das NISG betrifft weiters (ii) **Anbieter digitaler Dienste**. Anbieter digitaler Dienste sind Online-Marktplätze, Online-Suchmaschinen oder Cloud-Computing-Dienste. Ein Online-Marktplatz ist ein digitaler Dienst, der es Verbrauchern oder Unternehmern ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmen entweder auf der Website des Online-Marktplatzes oder auf der Website eines Unternehmens, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschließen[9]. **Demnach ist fraglich, ob Unternehmen, die einen Online-Vertrieb anbieten, in den Anwendungsbereich des NISG fallen**. Diese Unternehmen sind jedenfalls vom Anwendungsbereich ausgenommen, wenn es sich um ein Kleinstunternehmen oder ein

[4] § 14 Abs 2 Entwurf NISG.
[5] § 14 Abs 1 Entwurf NISG.
[6] ErwGr 21 der NIS-RL.
[7] Dieser Umstand sollte bei einem etwaigen „Statement of Applicability" iSd ISO-27001-Reihe berücksichtigt werden.
[8] ErwGr 22 des NIS-RL.
[9] § 3 Z 12 Entwurf NISG.

kleines Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6.5.2003[10] handelt. Damit sind Unternehmen ausgenommen, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw Jahresbilanz 10 Mio EUR nicht übersteigt. Fraglich ist allerdings, ob ein Anbieter digitaler Dienste nur dann in den Anwendungsbereich des NISG fällt, wenn dieser von „hoher Bedeutung für das Funktionieren des Gemeinwesens" iSd § 2 Abs 1 zweiter Satz NISG ist. Dafür würde ErwGr 48 zur NIS-RL sprechen, wonach *„Anbieter digitaler Dienste diejenigen sind, von denen angenommen wird, dass sie digitale Dienste anbieten, von den vielen* ***Unternehmen*** *in der Union zunehmend* ***abhängig*** *sind*". Die Legaldefinition des „Online-Marktplatzes"[11] ist kryptisch - letztlich wird dieser Begriff gar nicht definiert, sondern nur darauf verwiesen. In den Erläuterungen ist davon die Rede, dass „sämtliche Anbieter eines Online-Marktplatzes" (offenbar) in den Anwendungsbereich des NISG fallen sollen[12]. Durchforstet man unionsrechtliche Vorschriften nach dem Begriff des „Online-Marktplatzes", so wird man in der Verordnung über die Online-Streitbeilegung in Verbraucherangelegenheiten[13] (Stichwort: Internet-Ombudsmann) fündig[14]. Auch dort heißt es sehr extensiv: *„Online-Marktplätze sind Online-Plattformen, die es Unternehmen ermöglichen, den Verbrauchern ihre Waren und Dienstleistungen anzubieten*"[15]. **Jedenfalls wäre eine Klarstellung durch den Gesetzgeber wünschenswert**.

Auch hinsichtlich der **Cloud-Computing-Dienste[16]** ist der Anwendungsbereich (mehr als) schwierig zu lesen. Nach der Legaldefinition handelt es sich um einen digitalen Dienst, der den Zugang zu einem (i) skalierbaren und (ii) elastischen Pool (iii) gemeinsam nutzbarer (iv) Rechenressourcen ermöglicht. Nach den Gesetzesmaterialien[17] ist dieser Begriff weit auszulegen. (i) „Skalierbar" bezeichnet „Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können". Daraus folgt meines Erachtens, dass die **Rechenressourcen auf mindestens zwei geografische Standorte aufgeteilt** sein müssen. (ii) „Elastischer Pool" wird verwendet, „um die Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die verfügbaren Ressourcen je nach Arbeitsaufkommen rasch auf- bzw abgebaut werden

---

[10] Beachte auch ABl. Nr. L 124 vom 20.5.2003, S. 36.
[11] § 3 Z 12 Entwurf NISG bzw Art 4 Z 12 NIS-RL.
[12] Erläuterungen zum Entwurf 78/ME XXVI. GP – Ministerialentwurf – Erläuterungen, S 1 bzw ErwGr 57 zur NIS-RL.
[13] Verordnung (EU) Nr. 524/2013 des Europäischen Parlament und des Rates vom 21.5.2013 fündig.
[14] Es ist jedoch darauf hinzuweisen, dass die Begriffsbestimmungen der NIS-RL unbeschadet anderer Rechtsakte zu interpretieren sind (vgl ErwGr 55 zur NIS-RL).
[15] ErwGr 30.
[16] § 3 Z 14 Entwurf NISG.
[17] Erläuterungen zum Entwurf 78/ME XXVI. GP – Ministerialentwurf – Erläuterungen, S 5 bzw ErwGr 17 zur NIS-RL.

können". Damit ist wohl gemeint, dass die erforderlichen Speicherkapazitäten die Möglichkeit eröffnen müssen, nach oben und unten (je nach Arbeitsaufwand) auspendeln zu können. (iii) „Gemeinsam nutzbar" wird verwendet, „um die Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreife, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von derselben elektronischen Einrichtung erbracht wird". Damit soll wohl zum Ausdruck gebracht werden, dass die Möglichkeit bestehen muss, mehrere Benutzerkonten einrichten zu können. Zu den (iv) Rechenressourcen zählen Ressourcen wie „Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste". Unter „Anwendungen und Diensten" sind meines Erachtens auch Softwareprogramme[18] zu verstehen. Zusammenfassend ist auch der Begriff der Cloud-Computing-Dienste kryptisch formuliert. Für eine derartige Qualifikation dürfte erforderlich sein, dass die Server auf mehrere geografische Standorte aufgeteilt sind. Damit dürften etwa Rechenzentren, die nur einen Standort haben, nicht von dieser Legaldefinition erfasst sein.

Einrichtungen des Bundes

Schließlich umfasst das NISG (iii) **Einrichtungen des Bundes[19]**. Einrichtungen des Bundes in diesem Sinne sind die Bundesministerien, die Gerichtshöfe des öffentlichen Rechts, der Rechnungshof, die Volksanwaltschaft, die Präsidentschaftskanzlei und die Parlamentsdirektion. Dies Aufnahme der „Einrichtungen des Bundes" in das NISG ist insofern bemerkenswert, weil dies vom europäischen Gesetzgeber nicht gefordert wird[20]. Sinnvoll ist dies freilich allemal. Weitere Dienststellen können vom zuständigen Bundesminister durch Verordnung bestimmt werden. Es ist darauf hinzuweisen, dass insbesondere Cloud-Computing-Dienste, die von öffentlichen Einrichtungen eingesetzt werden, vertraglich zu einem hohen Sicherheitsniveau verpflichtet werden[21].

Unterstützung durch Computer-Notfallteams und nationales „Intrusion Prevention System[22]"

Zur Unterstützung der Betreiber wesentlicher Dienste und Anbieter digitaler Dienste wird zum Zwecke der Unterstützung bei der Bewältigung von Risiken und Sicherheitsvorfällen

---

[18] Softwareentwickler sind allerdings keine Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste (vgl ErwGr 50 der NIS-RL).
[19] § 3 Z 15 Entwurf NISG.
[20] ErwGr 67 zur NIS-RL.
[21] ErwGr 54. Zudem wird regelmäßig auch der Abschluss eines Auftragsverarbeitervertrags nach Art 28 DSGVO erforderlich sein.
[22] „Frühwarnsystem".

ein nationales Computer-Notfallteam eingerichtet[23]. Diesem Computer-Notfallteam kommt insbesondere die Aufgabe zu, Handlungsempfehlungen über Risiken und Sicherheitsvorfälle auszugeben und Sicherheitsfälle zu beobachten. Computer-Notfallteams können auch private Einrichtungen sein. Sie werden vom Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres akkreditiert, sofern die bestimmten, gesetzlich[24] definierten Mindestanforderungen erfüllt sind. Unter anderem hat sich das heranzuziehende Personal einer Sicherheitsprüfung nach dem Sicherheitspolizeigesetz[25] zu unterziehen.

Das Bundesministerium für Inneres ist ermächtigt, technische Einrichtungen zu betreiben, die Unregelmäßigkeiten oder Störungen von Netz- und Informationssystem frühzeitig erkennen. Dabei soll es sich offenbar um eine Art nationales „Intrusion Prevention System" handeln, an welchem sich Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes kostenpflichtig beteiligen können[26]. Nachdem bei diesem „Frühwarnsystem" auch personenbezogene Daten (insbesondere Namen, Anschriften, Telefonnummern, E-Mail-Adressen und sonstige den Sachverhalt spezifizierende technische Daten wie zum Beispiel der IP-Adresse, verwendete Ports, Host-Namen, Hashes, URL, Domainnamen, Zugangsdaten (!), Log-Files[27]) verarbeitet werden, ist dabei ein hohes Maß an den Datenschutz zu legen. **Es ist unbedingt sicherzustellen, dass die in diesem Zusammenhang vom Bundesministerium verarbeiteten Daten ausschließlich für die erforderlichen Zwecke verarbeitet werden!** Offenbar soll es möglich sein[28], für Zwecke der Strafrechtspflege personenbezogene Daten an Sicherheitsbehörden, militärische Organe, die Datenschutzbehörde, an Staatsanwaltschaften und ordentliche Gerichte weiterzuleiten. Außerdem soll eine Datenübermittlung „an sonstige in- und ausländische Behörden oder Stellen" möglich sein, „soweit dies zur Aufgabenerfüllung erforderlich" ist. **Angesichts der hohen Brisanz einerseits und der Unbestimmtheit dieser Regelung andererseits, wird die Verfassungskonformität dieser Regelung in der derzeitigen Fassung in Frage gestellt.**

[23] § 12 Entwurf NISG.
[24] § 13 Entwurf NISG.
[25] §§ 55 ff SPG.
[26] § 9 Abs 1 Entwurf NISG.
[27] Erläuterungen zum Entwurf 78/ME XXVI. GP – Ministerialentwurf – Erläuterungen, S 11 f.
[28] § 11 Abs 4 Entwurf NISG.

TT, November 2018

Umsetzung dem Stand der Technik entsprechender Sicherheitsvorkehrungen

Betreiber wesentlicher Dienste[29] und Anbieter digitaler Dienste[30] haben geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zur Gewährleistung der Netz- und Informationssicherheit vorzusehen. Der Gesetzgeber verlangt den Betreibern wesentlicher Dienste und den Einrichtungen des Bundes dabei ein höheres Schutzniveau ab, als den Anbietern digitaler Dienste. Die zu ergreifenden Maßnahmen sollen in einem angemessenen Verhältnis zu den Risiken stehen[31]. Eine Risikoanalyse auf Grundlage der ISO 27001 bzw ISO 27005 ist daher empfehlenswert. Die Maßnahmen müssen dann dem *„neuesten Stand Rechnung"*[32] tragen. Betreiber wesentlicher Dienste haben die Erfüllung dieser Anforderung mindestens alle drei Jahre gegenüber dem Bundesminister für Inneres nachzuweisen. Diese aktive Nachweispflicht gilt hingegen nicht für Anbieter digitaler Dienste.

Anbieter digitaler Dienste müssen dabei Folgendem Rechnung tragen[33]:

- Sicherheit der Systeme und Anlagen,
- Bewältigung von Sicherheitsvorfällen,
- Betriebskontinuitätsmanagement,
- Überwachung, Überprüfung und Erprobung,
- Einhaltung der internationalen Normen.

Bei dieser Auflistung fühlt man sich an das Verzeichnis der Maßnahmen aus Anhang A der ISO 27001 Norm erinnert. Maßnahmenziel 9 („Physische und umgebungsbezogene Sicherheit") und Maßnahmenziel 10 jeweils der ISO-Norm („Betriebs- und Kommunikationsmanagement") decken weitestgehend das Sicherheitsziel „Sicherheit der Systeme und Anlagen" des NISG ab. „Bewältigung von Sicherheitsvorfällen" spiegelt sich in Maßnahmenziel 13 („Umgang von Informationssicherheitsvorfällen") wieder. „Betriebskontinuitätsmanagement" erinnert stark an Maßnahmenziel 14 („Sicherstellung des Geschäftsbetriebs (Business Continuity Management)"). „Überwachung, Überprüfung und Erprobung" ähnelt Maßnahmenziel 12 („Beschaffung, Entwicklung und Wartung von Informationssystemen"). Und „Einhaltung der internationalen Normen" – wobei dieser Punkt noch dringend durch den Gesetzgeber konkretisiert werden sollte – findet sich in Maßnahmenziel 15 („Einhaltung von Vorgaben (Compliance)") wieder. Daraus folgt, dass

[29] § 15 Entwurf NISG.
[30] § 18 Entwurf NISG.
[31] Vgl ErwGr 53 zur NIS-RL.
[32] Vgl ErwGr 53 zur NIS-RL.
[33] Zur Erfüllung dieser Ziele siehe ErwGr 69 der NIS-RL.

der Bedarf an ISO 27001-Zertifizierungen zunehmen wird. **Jedenfalls aber dient die ISO 27001[34]–Reihe als gute Orientierung, um das Unternehmen rechtskonform im Sinne des NISG aufzustellen**.

Meldepflichten

Im Falle eines Sicherheitsvorfalls müssen Betreiber wesentlicher Dienste und Anbieter digitaler Dienste unverzüglich Meldung[35] an das (noch einzurichtende) „nationale Computer-Notfallteam" erstatten. Diese Meldepflicht besteht bei Anbietern digitaler Dienste allerdings nur dann, wenn der Anbieter digitaler Dienste Zugang zu Informationen hat, die benötigt werden, um die Auswirkungen eines Sicherheitsvorfalles zu bewerten. Ein Sicherheitsvorfall ist dabei eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einem Ausfall oder einer Einschränkung der Verfügbarkeit des betriebenen wesentlichen oder digitalen Dienstes geführt hat[36]. Sofern eine Störung keine Intensität eines Sicherheitsvorfalles im eben dargestellten Sinn erreicht, können freiwillige Meldungen erfolgen[37]. Inwiefern eine solche freiwillige Meldung eine zivilrechtliche Haftung ausschließen kann, wird die Rechtsprechung zeigen. Sofern die Voraussetzungen des Art 33 DSGVO erfüllt sind, sollte im Falle eines Sicherheitsvorfalles auch die Datenschutzbehörde benachrichtigt werden. Auf diese Parallelmeldung ist insbesondere deshalb zu achten, weil die zuständigen IT-Sicherheitsbehörden mit der Datenschutzbehörde einen Informationsaustausch pflegen sollten[38]. Im Falle der Unterlassung einer Meldung wird die „vernachlässigte" Behörde somit durch die alarmierte Behörde „Wind bekommen".

Zu den möglichen Konsequenzen eines Verstoßes

Im Falle eines Zuwiderhandelns gegen das NISG kann die örtliche zuständige Bezirksverwaltungsbehörde eine Geldstrafe von EUR 50.000 im Wiederholungsfall bis zu EUR 100.000 verhängen[39]. Auch juristische Personen können für die Verstöße haftbar gemacht werden.

---

[34] *„Die Normung der Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang"*. Vgl ErwGr 66 zur NIS-RL.
[35] § 16 und 18 Entwurf NISG.
[36] § 3 Z 6 Entwurf NISG.
[37] § 20 Entwurf NISG.
[38] Vgl ErwGr 63 NIS-RL.
[39] § 23 Entwurf NISG.

TT, November 2018

Zusammenfassung und Ausblick

Die NIS-RL wird durch das NISG in das nationale Recht umgesetzt werden. Das nationale Gesetz entfernt sich in einigen Punkten weit von der unionsrechtlichen Vorgabe. Dieses Gesetz umfasst „Betreiber wesentlicher Dienste", „Anbieter digitaler Dienste" und „Einrichtungen des Bundes". ME fallen in der derzeitigen Fassung wohl auch Unternehmen in den Anwendungsbereich, die einen Online-Vertrieb eingerichtet haben und über 50 Mitarbeiter beschäftigen. Ob dies vom (Unions-)Gesetzgeber tatsächlich so gewollt ist, ist fraglich. „Betreiber wesentlicher Dienste", „Anbieter digitaler Dienste" und „Einrichtungen des Bundes" haben entsprechende Sicherheitsvorkehrungen zur Gewährleistung der Netz- und Informationssicherheit vorzusehen. Bei der Implementierung dieser Sicherheitsvorkehrungen kann eine Orientierung an der ISO-27001-Reihe Kosten und Mühen ersparen. Zusammenfassend ist das Gesetz – wie im sicherheitstechnischen Bereich üblich – generisch gehalten. In einem (Anwendungsbereich hinsichtlich „Anbieter digitaler Dienste") oder anderen (Einhaltung „internationaler Normen") Punkten wäre eine Konkretisierung durch den Gesetzgeber noch wünschenswert. Ein besonderes Augenmerk ist zudem auf die datenschutzkonforme Umsetzung des „nationalen Frühwarnsystems" des Bundesministeriums für Inneres zu richten. Die dadurch gewonnenen Daten dürfen keinesfalls zweckentfremdend missbraucht werden.

Zum Autor:

Dr. Tobias Tretzmüller, LL.M. ist Rechtsanwalt in ständiger Kooperation mit der Knyrim Trieb Rechtsanwälte OG, Wien. E-Mail: tt@kt.at. Er berät und vertritt Unternehmen in den Bereichen des Datenschutzrechts, Urheberrechts, IT-Rechts und streitigen Behörden- und Zivilverfahren. Regelmäßige Vortrags- und Veröffentlichungstätigkeit (ua imh speaker of the year 2017, Jahrbuch Datenschutzrecht 2017).