DURCHFÜHRUNGSVERORDNUNG (EU) 2018/151 DER KOMMISSION

vom 30. Januar 2018

über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union ([1]), insbesondere auf Artikel 16 Absatz 8,

in Erwägung nachstehender Gründe:

(1) Gemäß der Richtlinie (EU) 2016/1148 steht es den Anbietern digitaler Dienste frei, technische und organisatorische Maßnahmen zu ergreifen, die sie zur Bewältigung der Risiken für die Sicherheit ihrer Netz- und Informationssysteme für angemessen und verhältnismäßig halten, sofern diese Maßnahmen ein angemessenes Sicherheitsniveau gewährleisten und den in der Richtlinie vorgesehenen Elementen Rechnung tragen.

(2) Bei der Ermittlung der angemessenen und verhältnismäßigen technischen und organisatorischen Maßnahmen sollten die Anbieter digitaler Dienste die Informationssicherheit systematisch nach einem risikobasierten Ansatz angehen.

(3) Zur Gewährleistung der Sicherheit der Systeme und Anlagen sollten die Anbieter digitaler Dienste Bewertungs- und Analyseverfahren durchführen. Diese Tätigkeiten sollten das systematische Management der Netz- und Informationssysteme, die physische Sicherheit und die Sicherheit des Umfelds, die Versorgungssicherheit und die Kontrolle des Zugangs umfassen.

(4) Bei der Durchführung einer Risikoanalyse im Rahmen des systematischen Managements der Netz- und Informationssysteme sollten Anbieter digitaler Dienste dazu angehalten werden, spezifische Risiken zu ermitteln und hinsichtlich ihrer Bedeutung zu quantifizieren, indem sie beispielsweise ermitteln, welche Gefährdungen für unentbehrliche Anlagen oder Wirtschaftsgüter bestehen und wie sich diese auf den Betrieb auswirken können, und indem sie bestimmen, wie diese Gefährdungen unter Berücksichtigung der vorhandenen Fähigkeiten und des Ressourcenbedarfs am besten eingedämmt werden können.

(5) Maßnahmen im Bereich Humanressourcen könnten das Kompetenzmanagement betreffen, darunter auch Aspekte der sicherheitsrelevanten Kompetenzentwicklung und Bewusstseinsbildung. Bei der Entscheidung über geeignete Maßnahmen für die Betriebssicherheit sollten die Anbieter digitaler Dienste dazu angehalten werden, die Aspekte des Änderungs- und des Schwachstellenmanagements, der Formalisierung betrieblicher und administrativer Verfahren und der Systemerfassung und -abbildung zu berücksichtigen.

(6) Die Maßnahmen im Bereich Sicherheitsarchitektur könnten insbesondere die Trennung von Netzen und Systemen sowie spezifische Sicherheitsvorkehrungen für unentbehrliche Tätigkeiten, wie beispielsweise administrative Tätigkeiten, umfassen. Die Trennung von Netzen und Systemen könnte die Anbieter digitaler Dienste in die Lage versetzen, zwischen Elementen wie Datenströmen und Rechenressourcen zu unterscheiden, die einem Kunden, einer Gruppe von Kunden, dem Anbieter digitaler Dienste selbst oder Dritten gehören.

(7) Die mit Blick auf die physische Sicherheit und die Sicherheit des Umfelds getroffenen Maßnahmen sollten die Sicherheit der Netz- und Informationssysteme einer Organisation vor Schäden durch Vorfälle wie Diebstahl, Brand, Überschwemmung oder andere Wettereinflüsse sowie Telekommunikations- oder Stromausfälle gewährleisten.

(8) Die Sicherheit der Versorgung, z. B. mit elektrischem Strom, Brenn- und Kraftstoffen oder Kühlung, könnte auch die Sicherheit der Lieferkette umfassen, darunter insbesondere die Sicherheit bei Dritten, die Auftragnehmer und Unterauftragnehmer sind, und deren Management. Die Rückverfolgbarkeit unentbehrlicher Güter oder Vorleistungen betrifft die Fähigkeit des Anbieters digitaler Dienste, die Herkunft dieser Güter oder Vorleistungen festzustellen und zu dokumentieren.

(9) Die Nutzer digitaler Dienste sollten natürliche und juristische Personen umfassen, die Kunden oder Teilnehmer eines Online-Marktplatzes oder eines Cloud-Computing-Dienstes sind, oder die die Website einer Online-Suchmaschine besuchen, um Stichwortsuchen durchzuführen.

([1]) ABl. L 194 vom 19.7.2016, S. 1.

(10) Bei der Definition der Erheblichkeit der Auswirkungen eines Sicherheitsvorfalls sollten die in dieser Verordnung genannten Fälle als nicht erschöpfende Liste erheblicher Sicherheitsvorfälle betrachtet werden. Es sollten Lehren aus der Durchführung dieser Verordnung und aus den Arbeiten der Kooperationsgruppe gemäß Artikel 11 Absatz 3 Buchstaben i und m der Richtlinie (EU) 2016/1148 in Bezug auf die Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen sowie in Bezug auf die Modalitäten für die Berichterstattung über die Meldung von Sicherheitsvorfällen gezogen werden. Hieraus könnten sich umfassende Leitlinien für quantitative Schwellenwerte für Meldungsparameter ergeben, die eine Meldepflicht von Anbietern digitaler Dienste gemäß Artikel 16 Absatz 3 der Richtlinie (EU) 2016/1148 auslösen können. Gegebenenfalls könnte die Kommission auch erwägen, die derzeit in dieser Verordnung festgelegten Schwellenwerte zu überprüfen.

(11) Damit die zuständigen Behörden über potenzielle neue Risiken auf dem Laufenden bleiben, sollten die Anbieter digitaler Dienste dazu angehalten werden, jeglichen Sicherheitsvorfall freiwillig zu melden, der ihnen zuvor unbekannte Merkmale wie neue Exploits, Angriffsvektoren oder Angreifer, Anfälligkeiten und Gefahren aufweist.

(12) Diese Verordnung sollte ab dem Tag gelten, der auf den Tag des Ablaufs der Frist für die Umsetzung der Richtlinie (EU) 2016/1148 folgt.

(13) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 22 der Richtlinie (EU) 2016/1148 eingesetzten Ausschusses für die Sicherheit von Netz- und Informationssystemen —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand

In dieser Verordnung werden die Elemente näher festgelegt, die die Anbieter digitaler Dienste zu berücksichtigen haben, wenn sie Maßnahmen ermitteln und ergreifen, die ein bestimmtes Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, die sie im Rahmen der Bereitstellung der in Anhang III der Richtlinie (EU) 2016/1148 genannten Dienste nutzen; ferner werden die Parameter näher festgelegt, die bei der Feststellung zugrunde zu legen sind, ob ein Sicherheitsvorfall erhebliche Auswirkungen auf die Bereitstellung dieser Dienste hat.

Artikel 2

Sicherheitselemente

(1) Die Sicherheit der Systeme und Anlagen gemäß Artikel 16 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/1148 bezeichnet die Sicherheit von Netz- und Informationssystemen und ihrer physischen Umgebung und umfasst die folgenden Elemente:

a) das systematische Management von Netz- und Informationssystemen, d. h. eine Erfassung und Abbildung der Informationssysteme und die Einführung einer Reihe von geeigneten Maßnahmen für das Management der Informationssicherheit, einschließlich Risikoanalyse, Humanressourcen, Betriebssicherheit, Sicherheitsarchitektur, Lebenszyklus-Management gesicherter Daten und Systeme sowie gegebenenfalls Verschlüsselung und Verschlüsselungsmanagement;

b) die physische Sicherheit und die Sicherheit der Umgebung, d. h. das Vorhandensein einer Reihe von Vorkehrungen zum Schutz der Sicherheit der Netz- und Informationssysteme von Anbietern digitaler Dienste vor Schäden anhand eines risikobasierten Allgefahrenansatzes, der beispielsweise Systemversagen, menschliche Fehler, böswillige Handlungen oder Naturereignisse berücksichtigt;

c) die Versorgungssicherheit, d. h. die Einführung und Aufrechterhaltung geeigneter Maßnahmen zur Gewährleistung der Zugänglichkeit und gegebenenfalls der Rückverfolgbarkeit unentbehrlicher Güter oder Vorleistungen, die für die Bereitstellung der Dienste genutzt werden;

d) die Kontrolle des Zugangs zu Netz- und Informationssystemen, d. h. das Vorhandensein einer Reihe von Vorkehrungen, die gewährleisten, dass der physische und logische Zugang zu Netz- und Informationssystemen, einschließlich der administrativen Sicherheit der Netz- und Informationssysteme, auf der Grundlage von Geschäfts- und Sicherheitsanforderungen genehmigt bzw. eingeschränkt wird.

(2) Mit Blick auf die Bewältigung von Sicherheitsvorfällen gemäß Artikel 16 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/1148 umfassen die von dem Anbieter digitaler Dienste getroffenen Vorkehrungen Folgendes:

a) Aufrechterhaltung und Erprobung von Erkennungsprozessen und -verfahren zur Gewährleistung einer rechtzeitigen und angemessenen Lageerfassung bei ungewöhnlichen Ereignissen;

b) Prozesse und Vorgaben für die Meldung von Vorfällen und die Feststellung von Schwachstellen und Anfälligkeiten in ihren Informationssystemen;

c) Reaktion gemäß den festgelegten Verfahren und Berichterstattung über die Ergebnisse der ergriffenen Maßnahme;

d) Bewertung der Schwere des Sicherheitsvorfalls mit einer Dokumentierung der Erkenntnisse aus der Vorfallanalyse und einer Sammlung relevanter Informationen, die als Nachweis dienen können und einen kontinuierlichen Verbesserungsprozess fördern.

(3) Das Betriebskontinuitätsmanagement („*Business continuity management*“) gemäß Artikel 16 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/1148 bezeichnet die Fähigkeit einer Organisation zur Aufrechterhaltung bzw. Wiederherstellung der Erbringung von Diensten auf einem zuvor festgelegten akzeptablen Niveau nach einer Störung und umfasst Folgendes:

a) die Erstellung und Anwendung von Notfallplänen auf der Grundlage einer Analyse der betrieblichen Auswirkungen zur Gewährleistung der Kontinuität der vom Anbieter digitaler Dienste erbrachten Leistungen, die regelmäßig bewertet und erprobt werden, z. B. anhand von Übungen;

b) Wiederherstellungskapazitäten, die regelmäßig bewertet und erprobt werden, z. B. anhand von Übungen.

(4) Die Überwachung, Überprüfung und Erprobung gemäß Artikel 16 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/1148 umfasst die Einführung und Aufrechterhaltung von Maßnahmen in folgenden Bereichen:

a) Durchführung einer planmäßigen Abfolge von Kontrollen oder Messungen, um zu beurteilen, ob die Netz- und Informationssysteme bestimmungsgemäß funktionieren;

b) Kontrolle und Überprüfung, um zu ermitteln, ob eine Norm oder ein Leitlinienkatalog befolgt wird, Aufzeichnungen korrekt sind und die Effizienz- und Wirksamkeitsvorgaben erfüllt werden;

c) Prozess zur Feststellung von Mängeln in den Sicherheitsmechanismen eines Netz- und Informationssystems, die Daten schützen und Funktionen aufrechterhalten sollen. Ein solcher Prozess erstreckt sich auf die technischen Verfahren und das Personal, die in den Betriebsablauf eingebunden sind.

(5) Internationale Normen im Sinne des Artikels 16 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/1148 sind Normen, die von einer internationalen Normungsorganisation im Sinne des Artikels 2 Absatz 1 Buchstabe a der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates [1] angenommen wurden. Gemäß Artikel 19 der Richtlinie (EU) 2016/1148 können auch europäische oder international anerkannte Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen sowie bestehende nationale Normen verwendet werden.

(6) Anbieter digitaler Dienste müssen sicherstellen, dass sie über eine angemessene Dokumentation verfügen, anhand derer die zuständige Behörde die Einhaltung der in den Absätzen 1, 2, 3, 4 und 5 genannten Sicherheitselemente überprüfen kann.

Artikel 3

Bei der Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls zu berücksichtigende Parameter

(1) Hinsichtlich der in Artikel 16 Absatz 4 Buchstabe a der Richtlinie (EU) 2016/1148 angesprochenen Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen, muss der Anbieter digitaler Dienste in der Lage sein, eine Schätzung einer der folgenden Zahlen vorzunehmen:

a) Zahl der betroffenen natürlichen und juristischen Personen, mit denen ein Vertrag über die Bereitstellung des Dienstes abgeschlossen wurde, oder

b) Zahl der betroffenen Nutzer, die den Dienst genutzt haben, wobei insbesondere frühere Verkehrsdaten zugrunde gelegt werden.

(2) Die Dauer eines Sicherheitsvorfalls im Sinne des Artikels 16 Absatz 4 Buchstabe b bezeichnet die Zeitspanne von der Unterbrechung der ordnungsgemäßen Bereitstellung des Dienstes in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit bis zum Zeitpunkt der Wiederherstellung.

(3) Was die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet im Sinne des Artikels 16 Absatz 4 Buchstabe c der Richtlinie (EU) 2016/1148 betrifft, muss der Anbieter digitaler Dienste in der Lage sein zu ermitteln, ob der Sicherheitsvorfall die Bereitstellung seiner Dienste in bestimmten Mitgliedstaaten beeinträchtigt.

(4) Das Ausmaß der Unterbrechung der Bereitstellung des Dienstes im Sinne des Artikels 16 Absatz 4 Buchstabe d der Richtlinie (EU) 2016/1148 wird anhand eines oder mehrerer der folgenden Merkmale beurteilt, die durch den Sicherheitsvorfall beeinträchtigt werden: Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten oder entsprechenden Dienste.

[1] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

(5) Was das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten im Sinne des Artikels 16 Absatz 4 Buchstabe e der Richtlinie (EU) 2016/1148 anbelangt, muss der Anbieter digitaler Dienste in der Lage sein, auf der Grundlage von Angaben wie der Art der vertraglichen Beziehungen mit dem Kunden oder gegebenenfalls der potenziellen Zahl der Nutzer festzustellen, ob der Sicherheitsvorfall zu erheblichen materiellen oder immateriellen Verlusten für die Nutzer geführt hat, beispielsweise in Bezug auf die Gesundheit, die Sicherheit oder die Beschädigung von Sachen.

(6) Anbieter digitaler Dienste sind nicht verpflichtet, zu den Zwecken der Absätze 1, 2, 3, 4 und 5 zusätzliche Informationen einzuholen, die ihnen nicht zugänglich sind.

Artikel 4

Erhebliche Auswirkungen eines Sicherheitsvorfalls

(1) Ein Sicherheitsvorfall gilt als mit erheblichen Auswirkungen verbunden, wenn mindestens einer der folgenden Fälle eingetreten ist:

a) der von einem Anbieter digitaler Dienste bereitgestellte Dienst war mehr als 5 000 000 Nutzerstunden lang nicht verfügbar, wobei sich der Begriff Nutzerstunde auf die Zahl der Nutzer in der Union bezieht, die während einer Dauer von sechzig Minuten betroffen waren;

b) der Sicherheitsvorfall hat zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der entsprechenden Dienste, die über ein Netz- und Informationssystem des Anbieters digitaler Dienste angeboten werden bzw. zugänglich sind, geführt, von dem mehr als 100 000 Nutzer in der Union betroffen sind;

c) durch den Sicherheitsvorfall ist eine öffentliche Gefahr oder ein Risiko für die öffentliche Sicherheit entstanden oder es sind Menschen ums Leben gekommen;

d) der Sicherheitsvorfall hat für mindestens einen Nutzer in der Union zu einem Sachschaden in Höhe von mehr als 1 000 000 EUR geführt.

(2) Auf der Grundlage der bewährten Verfahren, die die Kooperationsgruppe im Rahmen ihrer Aufgaben gemäß Artikel 11 Absatz 3 der Richtlinie (EU) 2016/1148 erarbeitet, und der Erörterungen gemäß Artikel 11 Absatz 3 Buchstabe m kann die Kommission die in Absatz 1 genannten Schwellenwerte überprüfen.

Artikel 5

Inkrafttreten

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Sie gilt ab dem 10. Mai 2018.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 30. Januar 2018

Für die Kommission

Der Präsident

Jean-Claude JUNCKER