DIGITALEUROPE

Umsetzung der EU-Richtlinie über die Sicherheit von Netzwerk- und Informationssystemen (NIS)

Brüssel, 5 Juli 2016

KURZDARSTELLUNG

Der Rat der Europäischen Union hat am 21. April 2016 die endgültige Version der Richtlinie über die Sicherheit von Netzwerk- und Informationssystemen (NIS) veröffentlicht. Während diese in diesem Sommer vom Europäischen Parlament noch formal zu unterzeichnen ist, haben sich die drei EU-Institutionen bereits auf den Wortlaut geeinigt, der voraussichtlich auch nicht mehr geändert wird. Die Mitgliedsstaaten müssen die Richtlinie innerhalb von 21 Monaten nach ihrer Annahme in nationales Recht umsetzen. Um diesen Prozess zu unterstützen, finden Sie beigefügt einen Leitfaden, wie die für die Technologiebranche relevanten Aspekte umgesetzt und die Absichten der Verfasser wirksam verankert werden können.

Die EU-Richtlinie über die Sicherheit von Netzwerk- und Informationssystemen ist die erste gesamteuropäische Gesetzgebung für Cybersicherheit, die den Schwerpunkt auf die Stärkung der zuständigen Behörden auf nationaler Ebene, eine verbesserte Koordination untereinander und die Einführung von Sicherheitsanforderungen für die wichtigsten Wirtschaftssektoren legt.

Die innerstaatlichen Durchführungsvorschriften dürfen die beiden Hauptziele der Richtlinie nicht aus den Augen verlieren: (1) ein hohes Maß an Cybersicherheit für die kritischen Infrastrukturen des Landes; (2) Einrichtung eines wirkungsvollen Kooperationsmechanismus innerhalb der EU-Mitgliedsstaaten, um dieses Ziel voranzutreiben. Die Ressourcen sollten in erster Linie dazu verwendet werden, diese zwei wichtigen Zielsetzungen zu erreichen.

Für die Technologiebranche sind die Bestimmungen im Hinblick auf die sogenannten Anbieter digitaler Dienste von besonderem Interesse. In der Richtlinie ist eindeutig festgelegt, dass es grundlegende Unterschiede zwischen den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste gibt. Tatsächlich sind Letztere nicht als kritische Infrastruktur an sich zu betrachten. Wie auch die Gesetzgebung anerkennt, bedeutet ein Ereignis, das Auswirkungen auf diese digitalen Dienste hätte, ein erheblich geringeres Risiko für die wirtschaftliche und öffentliche Sicherheit eines Landes. Es ist unverzichtbar, diese Unterscheidung beizubehalten, damit die knappen Ressourcen der Behörden, die für die Überwachung und Durchsetzung der Vorschriften zuständig sind, auch wirksam und effizient eingesetzt werden können.

Demzufolge empfehlen wir, den vorgesehenen Geltungsbereich der betreffenden Dienste genau zu beachten und ersuchen die politischen Entscheidungsträger, keine anderen Sektoren als diejenigen, die als Anbieter digitaler Dienste und Betreiber wesentlicher Dienste erfasst wurden, den Sicherheitsanforderungen im nationalem Recht zu unterwerfen.

Im Hinblick auf die rechtliche Zuständigkeit müssen die Anbieter digitaler Dienste in der Lage sein, sich auf das geltende Recht in dem Land ihrer Hauptniederlassung verlassen zu können, selbst in solchen Fällen, wenn zuständige Behörden aus mehr als einem Land beteiligt sind. Bei der Aufsicht sollten die zuständigen Behörden einen Ex-Post-Ansatz verfolgen, anstatt eine allgemeine Pflicht zur Beaufsichtigung der Anbieter digitaler Dienste aufzuerlegen. Ferner sollten sie sich auf die Ergebnisse konzentrieren und die Unterscheidung zwischen

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Mitglied des Transparenzregisters für die Kommission: 64270747023-20

Betreibern wesentlicher Dienste und Anbietern digitaler Dienste beibehalten, indem Letztere nicht Anforderungen unterworfen werden, die in der Richtlinie nicht vorgesehen sind, wie beispielsweise Prüfbefugnisse oder verbindliche Anweisungen.

Die Sicherheitsmaßnahmen für Anbieter digitaler Dienste müssen sich angesichts der in der Richtlinie getroffenen Aussage, dass diese ein erheblich geringeres Sicherheitsrisiko darstellen, von den Vorschriften für die Betreiber wesentlicher Dienste unterscheiden. Entscheidungsträger müssen das Ziel der Harmonisierung für diese Dienste erkennen, die bestehenden und von der Industrie getriebenen internationalen Standards anerkennen, Technologievorgaben vermeiden und das in der Richtlinie verankerte Recht des Anbieters digitaler Dienste, die für ihre Systeme am besten geeigneten Sicherheitsmaßnahmen zu definieren, respektieren. Die Meldung von Sicherheitsvorfällen muss auf europäischer Ebene ebenfalls möglichst einheitlich gestaltet sein, sich auf Vorfälle konzentrieren, die Auswirkungen auf die Kontinuität des Dienstes haben, die Flexibilität für den Zeitrahmen der Benachrichtigungen respektieren und ein vertrauensvolles Umfeld schaffen, das einen Austausch von Informationen befördert, ohne dass die benachrichtigende Partei dadurch einer erhöhten Haftung ausgesetzt wird.

Die den Betreibern wesentlicher Dienste auferlegten Maßnahmen werden sich auch auf andere Industriezweige auswirken, da die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen in die Vertragsbestimmungen einfließen werden. Dies gilt insbesondere für die sogenannten "Cloud"-Dienste. Infolgedessen können die Anbieter digitaler Dienste indirekt dem nationalen Recht ihrer Kunden unterliegen; folglich haben wir ein starkes Interesse daran, dass international anerkannte Sicherheitsmaßnahmen auf diese Dienste Anwendung finden. Wir schlagen ferner eine Koordinierung und höchstmögliche Synergien zwischen den Meldepflichten sowohl für die Betreiber wesentlicher Dienste als auch für die Anbieter digitaler Dienste vor, da Letztere voraussichtlich einer doppelten Benachrichtigungspflicht unterliegen werden.

In der Richtlinie wird das Bestreben deutlich, ein hohes gemeinsames Maß an Sicherheit für Netzwerk- und Informationssysteme zu erreichen, um das Funktionieren des Binnenmarktes zu verbessern. Um dieses hoch gesteckte Ziel zu erreichen, muss sich **die nationale Umsetzung auf einen risikobasierten, einheitlichen und internationalen Ansatz** konzentrieren, der den Akteuren aus dem Privatsektor die Flexibilität gibt, sich an eine ständig ändernde Bedrohungslage anzupassen, den zuständigen Behörden die Möglichkeit gibt, die beschränkten Ressourcen für die wichtigsten Herausforderungen einzusetzen und der anerkannt, dass die Lösung für ein grenzüberschreitendes Problem global sein muss. Wir hoffen, dass dieser Leitfaden hierfür ein nützliches Werkzeug liefert und stehen Ihnen bei Rückfragen gerne zur Verfügung.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Mitglied des Transparenzregisters für die Kommission: 64270747023-20

Anhang: Leitfaden für die Umsetzung der Richtlinie für Sicherheit in Netzwerk- und Informationssystemen (NIS)

1. Anbieter digitaler Dienste

a) Anwendungsbereich

- In der Richtlinie ist festgelegt, dass Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste als Anbieter digitaler Dienste zu betrachten sind und daher in den Geltungsbereich der Richtlinie fallen. Während es sich um eine Richtlinie mit Mindestharmonisierung (Artikel 2) handelt, ist es wichtig die Einheitlichkeit innerhalb Europas beizubehalten; daher sollten Mitgliedsstaaten - wie in Artikel 3 definiert - nicht andere Sektoren als diejenigen, die als Anbieter digitaler Dienste oder Betreiber wesentlicher Dienste erfasst wurden, den Sicherheitsanforderungen im nationalem Recht unterwerfen.

- Die Richtlinie besagt ausdrücklich, dass Hardware-Hersteller und Software-Entwickler nicht Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste sind und daher nicht den innerstaatlichen Gesetzen unterliegen, mit denen die Richtlinie umgesetzt wird (Erwägungsgrund 50).

- Vom Geltungsbereich der Online-Marktplätze ausdrücklich ausgenommen sind in der Richtlinie die Online-Dienste, die als Vermittler für Dienste Dritter agieren, , bei denen der Vertriebs- oder Dienstleistungsvertrag endgültig abgeschlossen wird (z. B. Vergleichsseiten) (Erwägungsgrund 15).

- Die Suchfunktionen, die auf den Inhalt einer bestimmten Website beschränkt sind, fallen nicht unter die Definition einer Online-Suchmaschine, selbst wenn sie einen externen Anbieter nutzen (Erwägungsgrund 16).

- Die Definition von Cloud-Computing-Diensten zielt laut der Richtlinie darauf ab, dass Rechenressourcen von mehreren Nutzern gemeinsam genutzt werden (Artikel 4 (19) und Erwägungsgrund 17). Angesichts der Tatsache, dass sich private Clouds (im Vergleich zu öffentlichen Clouds) einer einzelnen Organisation zugeordnet, sind sie nicht abgedeckt.

- In der Richtlinie wird betont, dass es grundlegende Unterschiede zwischen den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste gibt. Das ist auch der Grund, warum Anbieter digitaler Dienste anderen Richtlinien unterliegen (Erwägungsgrund 57). Bei der Umsetzung der Richtlinie sollte diese Unterscheidung beibehalten werden.

b) Rechtliche Zuständigkeit und Aufsicht

- Anbieter digitaler Dienste sollten nur der rechtlichen Zuständigkeit eines Mitgliedsstaates unterliegen, in dem der Betreiber seine Hauptniederlassung in der EU hat, was in der Regel dem Ort entspricht, wo er seinen Hauptgeschäftssitz in der EU hat (Artikel 18.1 und Erwägungsgrund 64). Wir sind hingegen der Auffassung, dass die Anbieter digitaler Dienste diese Entscheidung selbst treffen sollten und diese nur dann überprüft werden sollte, wenn zuständige Behörden sie im Rahmen nachträglicher Aufsichtstätigkeiten in Frage stellen.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Mitglied des Transparenzregisters für die Kommission: 64270747023-20

- Wenn Anbieter in anderen Ländern als an dem Standort ihrer Hauptniederlassung digitaler Dienste Netzwerk- und Informationssysteme betreiben, sieht Artikel 17.3 eine Zusammenarbeit der zuständigen Behörden vor. Aus Sicht der Anbieter digitaler Dienste ist es jedoch von Bedeutung, dass nur die Gesetze des Landes, in dem sie ihre Hauptniederlassung haben, Anwendung finden und dass sie einzig und allein dieser national zuständigen Behörde gegenüber verantwortlich sind, die als Ansprechpartner fungiert.

- In der Richtlinie wird hervorgehoben, dass die Anbieter digitaler Dienste einer reaktiven Ex-Post-Aufsicht unterliegen und die zuständigen Behörden daher keine allgemeine Aufsichtspflicht über die Anbieter digitaler Dienste haben. Somit müssen sie nur aktiv werden, wenn ihnen entsprechende Nachweise vorgelegt werden. (Artikel 17.1 und Erwägungsgrund 60). Diese Bestimmungen sollten bei der Umsetzung dieser Richtlinie respektiert werden.

- Im Gegensatz zu den Betreibern wesentlicher Dienste können die Behörden im Falle von Anbietern digitaler Dienste nur Informationen anfragen und verlangen, dass die Anbieter digitaler Dienste bei einem Versäumnis nachbessern. Die Richtlinie macht deutlich, dass Behörden keine Prüfbefugnisse haben und keine verbindlichen Anweisungen erteilen können. Diese Bestimmungen sollten auch auf nationaler Ebene respektiert werden.

c) Weitere Anforderungen

- Die Sicherheitsanforderungen und Meldepflichten der Anbieter digitaler Dienste unterliegen einer Vollharmonisierung(Artikel 16.10). Dieser Artikel ist demnach auf die Produkte, Dienste und Lösungen, aus denen sich ihre Netzwerk- und Informationssysteme zusammensetzen, anzuwenden. Demzufolge sollten zusätzliche Bestimmungen, wie beispielsweise Produktprüfungen, nicht vorgeschrieben werden, sofern die Produkte und Dienste in diesem Zusammenhang genutzt werden.

d) Sicherheitsmaßnahmen und Standards

- Die Sicherheitsmaßnahmen für Anbieter digitaler Dienste sollten weniger strikt als die für Betreiber wesentlicher Dienste sein. Es sollte den Anbietern digitaler Dienste freigestellt sein, wie sie für Sicherheit sorgen und je nach den vorliegenden Risiken einen angemessenen Schutz ihrer Netzwerk- und Informationssysteme gewährleisten wollen (Erwägungsgrund 49).

- Die Sicherheitsmaßnahmen sollten prozessbezogen sein und sich auf das Risikomanagement konzentrieren. Es sollte nicht vorgeschrieben werden, dass Produkte aus dem Bereich Informations- und Kommunikationstechnik in einer besonderen Weise konzipiert, entwickelt oder hergestellt werden (Erwägungsgrund 51).

- In der Richtlinie wird betont, dass Mitgliedsstaaten den Anbietern digitaler Dienste keine weiteren Sicherheitsanforderungen auferlegen sollen (Artikel 16.10).

- Dessen ungeachtet gehen wir davon aus, dass mehrere Akteure Leitlinien ausgeben werden. Mitgliedsstaaten müssen sicherstellen, dass die in der Richtlinie genannten Maßnahmen angenommen werden (Artikel 16.1). Sie können die Anwendung von Normen anregen, um diese umzusetzen (Artikel 19.1) und die Normen mit den europäischen Normungsorganisationen in der Kooperationsgruppe

diskutieren (Artikel 11.3 (h)). ENISA berät über die angemessenen Normen (Artikel 19.2) und die Europäische Kommission ist mit der Annahme von Durchführungsrechtsakten zu Sicherheitsmaßnahmen beauftragt (Artikel 16.8).

- Angesichts dieser Komplexität und der Vorteile der Harmonisierung empfehlen wir, die nationalen Verfahren im Wesentlichen den Durchführungsrechtsakten zwecks Genehmigung der angemessenen Maßnahmen unterzuordnen, die in jedem Fall innerhalb eines Jahres nach der Annahme der Richtlinie endgültig festzulegen sind. Die Durchführungsrechtsakte selbst sollten in keiner Weise der Fähigkeit der Anbieter digitaler Dienste entgegenstehen, die für ihre Systeme am besten geeigneten Sicherheitsmaßnahmen zu definieren.

- Der Artikel zu den Normen ermöglicht eine Bezugnahme auf die europäischen bzw. international anerkannten Normen (Artikel 19.1). Da es in diesem Bereich bereits bewährte internationale Normen gibt, empfehlen wir für den Fall, dass geeignete Normen existieren, eine Zertifizierung nach diesen Normen vorzunehmen (wie z. B. ISO 27001), die hinreichend sein müssten, um diesen Anforderungen gerecht zu werden.

- In jedem Fall sollte die Zertifizierung des Standards optional und nicht verpflichtend sein. In Artikel 19 wird hervorgehoben, dass jede Norm nur "gefördert" werden kann und dass dies "ohne Auferlegung oder Bevorzugung der Verwendung einer bestimmten Technologieart" erfolgen soll.

e) Meldung von Sicherheitsvorfällen

- Wie bei den Sicherheitsmaßnahmen sind mehrere Parteien daran beteiligt, die Meldung von Vorfällen gemäß der Richtlinie für die Sicherheit von Netzwerk- und Informationssystemen zu formulieren. Die Mitgliedsstaaten müssen sicherstellen, dass die Anbieter digitaler Dienste alle Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Bereitstellung der von ihnen angebotenen Dienste (die in den Geltungsbereich der Richtlinie fallen) haben (Artikel 16.3), wobei die Kooperationsgruppe für die Erörterung der Modalitäten für Benachrichtigungen (Artikel 11.3 (m)) und die Kommission für die Annahme der Durchführungsrechtsakte (Artikel 16.8 und 9) verantwortlich ist.

- Wieder lautet unsere Empfehlung, die nationalen Umsetzungen dem Verfahren der Durchführungsrechtsakte unterzuordnen, wobei der Durchführungsrechtsakt im Hinblick auf den Schwellenwert für Benachrichtigungen innerhalb eines Jahres nach der endgültigen Festlegung der Richtlinie angenommen werden muss.

- Im Hinblick darauf, welche Arten von Vorfällen gemeldet werden müssen, sind die Anbieter digitaler Dienste dafür verantwortlich, "jeden Vorfall zu melden, der erhebliche Auswirkungen auf die Bereitstellung [ihrer] Dienste hat" (Artikel 16.3). Was die Umsetzung der gleichwertigen Bestimmungen für Betreiber von Telekommunikationssystemen gemäß Artikel 13a der Rahmenrichtlinie betrifft, befürworten wir die Auslegung, dass sich diese auf die **Kontinuität (oder Verfügbarkeit)** der bereitgestellten Dienste konzentrieren sollten. Mit anderen Worten: es sollten eher Ausfälle, die einen bestimmten Grenzwert erreichen (der anhand der Durchführungsrechtsakte festzulegen ist) als andere Arten von Sicherheitsvorfällen gemeldet werden. Dies hat den Vorteil, dass man sich auf Vorfälle konzentrieren kann, die wahrscheinlich Auswirkungen auf die Wirtschaft oder Gesellschaft haben werden, während eine Überlappung mit den Meldepflichten bei Verletzungen des Schutzes der

personenbezogenen Daten gemäß der Datenschutzgrundverordnung minimiert (jedoch nicht vollständig vermieden) wird.

- Darüber hinaus ist in der Meldepflicht für "Betreiber wesentlicher Dienste" festgelegt, dass diese Betreiber „Vorfälle melden müssen, die erhebliche Auswirkungen auf die Kontinuität der von ihnen bereitgestellten wesentlichen Dienste haben", wobei hier erneut der eindeutige Schwerpunkt auf der Kontinuität (oder Verfügbarkeit) der Dienste liegt. Die Mitgesetzgeber haben vereinbart, dass die Verpflichtungen für die Anbieter digitaler Dienste geringer als die für die Betreiber wesentlicher Dienste sein müssen (siehe Erwägungsgrund 49). Die Meldepflicht von Vorfällen durch die Anbieter digitaler Dienste gemäß der Richtlinie für die Sicherheit von Netzwerk- und Informationssystemen darf daher nicht weiter gefasst sein als die für die Betreiber wesentlicher Dienste. Tatsächlich müsste sie im Hinblick auf Grenzwerte noch enger gefasst sein. Dies zeigt erneut, dass die Meldung von Vorfällen für Anbieter digitaler Dienste auf Vorfälle beschränkt werden sollte, die einen bestimmten Grenzwert erreichen und **Auswirkungen auf die Kontinuität/Verfügbarkeit des Dienstes haben** und nicht Vorfälle im Hinblick auf die Vollständigkeit oder Vertraulichkeit von Daten, die in hohem Maße bereits durch die damit im Zusammenhang stehenden Anforderungen gemäß den Datenschutzgrundverordnung (DSGVo) und der Verordnung über elektronische Identifizierung und Vertrauensdienste (elDAS) abgedeckt sind.

- Im Hinblick auf den Zeitrahmen für die Meldung begrüßen wir die in der Formulierung "unverzüglich" (Artikel 16.3) enthaltene Flexibilität. Die Umsetzung sollte nicht mit einer festen Meldefrist verbunden sein, da die Vorfälle in ihrer Komplexität sehr unterschiedlich sein können. Einheitliche Meldefristen könnten eine ungenaue Meldung zur Folge haben, wenn das anfängliche Ausmaß der betroffenen Systeme nicht eindeutig ist und somit die Fähigkeit der für die Meldung von Vorfällen verantwortlichen Fachleute, auf Vorfälle nach Priorität zu reagieren anstelle diese zu melden, beeinträchtigt werden könnte.

- Wie bereits erörtert, sind Sicherheitsvorfälle, die gemäß der Richtlinie gemeldet werden müssen, möglicherweise auch nach dem Datenschutzrecht meldepflichtig, falls der Schutz personenbezogener Daten verletzt wird. Dies bedeutet nicht nur, dass der gleiche Vorfall an unterschiedliche Behörden gemeldet werden muss, sondern auch, dass diese Behörden sogar in unterschiedlichen Mitgliedsstaaten ansässig sein können, je nachdem, welche rechtliche Zuständigkeit laut dieser beiden Gesetze für die Anbieter digitaler Dienste zutrifft. Wir empfehlen, dass Mitgliedsstaaten die Notwendigkeit erkennen und dafür Sorge tragen, dass nur eine einzige Meldung von Vorfällen erforderlich ist und sie sich ferner bemühen werden, Kommunikationskanäle zu schaffen, damit die relevanten Informationen unbeschadet von Geschäftsgeheimnissen untereinander geteilt werden können.

- Vor der Veröffentlichung von Informationen über Vorfälle, sollten die zuständigen Behörden den daraus resultierenden Konsequenzen für die Reputation und das Geschäft der Anbieter digitaler Anbieter Rechnung tragen. Noch wichtiger ist, dass die Bekanntgabe des Vorfalls das Sicherheitsrisiko verstärken könnte. Folglich ist vor der Veröffentlichung eine Koordination mit den betroffenen Akteuren wichtig.

- In der Richtlinie wird betont, dass als vertraulich eingestufte Informationen, auch als solche zu behandeln sind (Erwägungsgründe 41, 59, Artikel 1.5).

- In Artikel 16.3 wird unterstrichen, dass die meldende Partei durch die Meldung von Sicherheitsvorfällen keiner erhöhten Haftung ausgesetzt werden soll.

2. Wesentliche Betreiber

a) Übernahme der Bedingungen für Sicherheitsmaßnahmen

- Anbieter digitaler Dienste, die Betreiber wesentlicher Dienste als Kunden haben, unterliegen Sicherheitsmaßnahmen, die aus den gesetzlichen Verpflichtungen für wesentliche Betreiber in die Vertragsverhandlungen einfließen (Artikel 14.1). Demnach ist es möglich, dass sie, ungeachtet des für sie in dem Land ihres europäischen Hauptgeschäftssitzes geltenden Rechts, indirekt dem nationalen Recht ihrer Kunden unterliegen.

- Infolgedessen würden wir Bemühungen hinsichtlich einer Harmonisierung der Sicherheitsmaßnahmen für wesentliche Betreiber begrüßen. Während Mitgliedsstaaten das Recht haben, den wesentlichen Betreibern strengere Verpflichtungen aufzuerlegen als die, die in der Richtlinie vorgesehen sind (Artikel 3), lautet unsere Empfehlung, davon abzusehen und wir ermutigen die Mitgliedsstaaten, einen harmonisierten Ansatz zu erarbeiten. Dies könnte dadurch erreicht werden, dass zusätzliche Maßnahmen in der nationalen Umsetzung vermieden werden und man sich um die Festlegung angemessener Sicherheitsmaßnahmen in der Kooperationsgruppe bemüht, anstatt sich auf den innerstaatlichen Prozess zu konzentrieren.

- Die Sicherheitsanforderungen sollten weitestgehend auf internationalen Normen (wie z. B. die ISO-Normenreihe 27x) und den anerkannten bewährten Sicherheitsverfahren basieren.

- Die den Betreibern von wesentlichen Diensten auferlegten Sicherheitsmaßnahmen sollten auf keinen Fall vorschreiben, dass bestimmte Produkte aus dem Bereich Informations- und Kommunikationstechnik in bestimmter Weise konzipiert, entwickelt oder hergestellt werden (Erwägungsgrund 51).

b) Übernahme der Bedingungen für die Meldung von Vorfällen

- Die Betreiber wesentlicher Dienste sind verpflichtet, Sicherheitsvorfälle zu melden, die sich bei von ihnen beauftragen Anbietern digitaler Dienste ereignen und sich auf die Kontinuität ihrer wesentlichen Dienste auswirken(Artikel 16.5). Somit sind die Anbieter digitaler Dienste vertraglich verpflichtet, dem betreffenden wesentlichen Betreiber Sicherheitsvorfälle, die Auswirkungen auf ihn haben könnten, zu melden.

- Im Hinblick auf den Zeitrahmen der Benachrichtigung begrüßen wir die in der Formulierung "unverzüglich" enthaltene Flexibilität. (Artikel 14.3 - A. d. Ü.: Achtung: es müsste Artikel 16.3 heißen). Bei der Umsetzung auf nationaler Ebene sollten keine spezifischen Fristen eingeführt werden und falls die Betreiber wesentlicher Dienste aufgefordert werden, die für die Benachrichtigung in Anspruch genommene Zeit zu rechtfertigen, sollte der zu beurteilende Zeitraum immer ab dem Zeitpunkt beginnen, an dem die Betreiber wesentlicher Dienste, informiert wurde und nicht der Anbieter digitaler Dienste, von dem Vorfall Kenntnis erlangt hat.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Mitglied des Transparenzregisters für die Kommission: 64270747023-20

- Artikel 14.7 sieht vor, dass die Kooperationsgruppe - im Gegensatz zu der Harmonisierungsaufgabe der Kommission im Hinblick auf die Benachrichtigungen von Anbietern digitaler Dienste - Handlungshilfen ausarbeiten soll bzgl. der Umstände, unter denen eine Benachrichtigung erfolgen muss. Angesichts der doppelten Meldepflicht für Anbieter digitaler Dienste ist es wichtig, dass die jeweiligen Meldepflichten nicht widersprüchlich und weitestgehend angeglichen sind. Folglich sollte dieser Prozess auf dieses Ziel hin überprüft werden. Darüber hinaus sollten die Meldepflichten für Anbieter digitaler Dienste die Vertraulichkeitsverpflichtungen, die sie gegenüber den Betreibern wesentlicher Dienste als ihren Kunden haben, respektieren und sie nicht zur Weitergabe vertraulicher Geschäftsgeheimnisse auffordern.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Mitglied des Transparenzregisters für die Kommission: 64270747023-20

ÜBER DIGITALEUROPE

DIGITALEUROPE vertritt den Industriezweig Digitaltechnik in Europa. Zu unseren Mitgliedern gehören einige der weltweit größten Unternehmen aus den Bereichen IT, Telekommunikation und Verbraucherelektronik sowie Nationalverbände aus allen Teilen Europas. Es ist der Wunsch von DIGITALEUROPE, dass einerseits die Unternehmen und Bürger Europas in vollem Umfang von der Digitaltechnik profitieren und in Europa andererseits die weltbesten Unternehmen für Digitaltechnik wachsen, angezogen und erhalten werden.

DIGITALEUROPE gewährleistet, dass die Industrie an der Entwicklung und Umsetzung von EU-Richtlinien mitwirken kann. Zu den Mitgliedern von DIGITALEUROPE gehören 62 Unternehmen und 37 nationale Handelsverbände aus ganz Europa. Auf unserer Website http://www.digitaleurope.org finden sich weitere Informationen über unsere aktuellen Nachrichten und Aktivitäten.

MITGLIEDSCHAFT BEI DIGITALEUROPE

Mitgliedsunternehmen

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Nationale Handelsverbände

Belgien: AGORIA
Bulgarien: BAIT
Dänemark: DI Digital, IT-BRANCHEN
Deutschland: BITKOM, ZVEI
Estland: ITL
Finnland: FFTI
Frankreich: AFNUM, Force Numérique, Tech in France
Griechenland: SEPE
Großbritannien: techUK
Irland: ICT IRLAND
Italien: ANITEC
Litauen: INFOBALT
Niederlande: Nederland ICT, FIAR
Österreich: IOÖ
Polen: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Rumänien: ANIS, APDETIC
Schweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Schweiz: SWICO
Slowakei: ITAS
Slowenien: GZS
Spanien: AMETIC
Türkei: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
Ungarn: IVSZ
Weißrussland: INFOPARK
Zypern: CITEA