Transkript Podcastfolge: Mehr Cybersicherheit durch die NIS-2-Richtlinie?

Ein Beitrag von Johannes Müller, Nicolas John, Ole-Christian Tech und Klaus Palenberg, 21. Juni 2023

Beschreibung:

Regelmäßige Cyberangriffe auf IT-Infrastrukturen sind zum Alltag einer digitalisierten Welt geworden. Hiermit steigt auch das Bedürfnis nach einem rechtlichem Rahmen, der zur Cybersicherheit verpflichtet. In dieser Folge informieren die wissenschaftlichen Mitarbeiter Nicolas John und Johannes Müller über die EU-Gesetzgebung zur Herstellung eines einheitlichen Niveaus der IT-Sicherheit. Hierbei wird insbesondere der Inhalt der noch jungen NIS 2-Richtlinie diskutiert.

Einen Beitrag zu der Thematik findet sich in der hier verlinkten Ausgabe des DFN-Infobrief Recht 04/2023.

Transkript

00:00:06 Palenberg

Weggeforscht. Der Podcast der Forschungsstelle Recht im DFN.

00:00:13 John

Hallo und herzlich Willkommen zu einer neuen Folge von unserem Podcast. Heute geht es um die NIS 2 Richtlinie und dafür stehen für Sie mein lieber Kollege Johannes Müller und ich, Nicolas John, für Sie am Mikrofon.

00:00:24 Müller

Auch von mir ein Hallo und ein herzliches Willkommen.

00:00:26 John

Ja, was genau diese sogenannte NIS Richtlinie überhaupt regelt, was das juristische Update der eben jetzt in Kraft getretenen NIS 2 Richtlinie bedeutet und welcher Umsetzungsbedarf davon in Deutschland zu erwarten ist, das wird dann heute das Thema sein. Aber zuerst wie immer, was gibts neues?

00:00:43 Tech

Datenleck bei Tesla. Bei dem US-Automobilhersteller Tesla kam es zu einem großen Datenleck. Ein Informant hat dem Handelsblatt insgesamt 100 GB von vertraulichen Daten zugespielt. Dabei handelt es sich um 23.000 Dateien, die personenbezogene Daten enthalten, unter anderem Gehälter und Privatanschriften von mehr als 100.000 aktuellen und ehemaligen Mitarbeitern. Daneben sind mutmaßlich auch Dokumente zu technischen Problemen veröffentlicht worden. Auch die Politik und verschiedene Behörden haben nun die Frage stellt, ob Informationen von Mitarbeitern und Kunden nicht ausreichend geschützt werden.

Selbstverpflichtung als Provisorium. Aufgrund der öffentlichen Warnungen vor Risiken durch KI drängt die EU auf eine sogenannte freiwillige Selbstkontrolle. Die KI Regulierung durch die EU in Form des AI-Acts wird voraussichtlich erst in mehreren Jahren in Kraft treten. Daher soll nun möglichst schnell eine Selbstverpflichtung der Unternehmen erarbeitet werden, um die Risiken des Einsatzes dieser Technologie zu reduzieren. Die Ausarbeitung soll dabei in enger Kooperation mit der Industrie erfolgen.

00:01:43 John

Ja, und damit ist zum Hauptthema. Hackerangriff auf Krankenkassen, Hackerangriff auf Webseiten des Landes Mecklenburg-Vorpommern, bundesweite Cyberattacke auf Ministerien und Behörden, Cyberangriff auf ATU-Kette und Medienportale. Ja, das sind alles Nachrichten über Hackerangriffe und Cyberattacken aus den vergangenen 5 Monaten dieses Jahres, also nur 5 Monate. Teil der Aufzählungen sind hier ausschließlich größere Angriffe und nur solche, die sich unmittelbar in Deutschland ereignet haben. Es zeigt sich also, Europa und weltweit häufen sich die Hacker und Cyberangriffe immer weiter und mit der zunehmenden Digitalisierung der alltäglichen Welt steigen die natürlich weiterhin auch. Laut Studien tatsächlich kommt es zu hochgerechnet 17.000 Hackerangriffen pro Sekunde auf Unternehmen weltweit, also eine unfassbar hohe Zahl. Der europäische Gesetzgeber jedenfalls hat sich deswegen dazu berufen gefühlt, in der Europäischen Union natürlich auch ein höheres und harmonisiertes Niveau an IT-Sicherheit zu schaffen. Zu diesem Zweck trat schon 2016 die Netz- und Informationssicherheitsrichtlinie, kurz die NIS Richtlinie, in Kraft. Johannes und ich, wir haben uns da mal mit auseinandergesetzt, weil jetzt gab es hierzu ein kleines Update mit der NIS 2 Richtlinie, dazu kommen wir später, und wir haben uns das alles mal genauer angeschaut. Deswegen, ja kommen wir erstmal zu NIS Richtlinie.

00:02:58 Müller

Also, vielleicht fangen wir am besten chronologisch an. Möchtest du einmal sagen, was die 1. Richtlinie geregelt hat, also was genau die Inhalte von der Richtlinie waren und vor allem durch die Richtlinie verpflichtet wurde?

00:03:08 John

Ja klar. Zum einen würden dadurch die Mitgliedstaaten verpflichtet, eine nationale Strategie für die Sicherheit von Netz und Informationssystemen festzulegen. Außerdem müssen Sie für Notfälle ein Netzwerk an Computer-Notfallteams einrichten, welches dann die effiziente Zusammenarbeit zwischen den verschiedenen EU Mitgliedstaaten fördern soll und auch das Vertrauen zwischen den Staaten stärken soll. Und zum anderen werden natürlich auch die Betreiber wesentlicher Dienste verpflichtet.

00:03:34 Müller

Wer sind denn diese Betreiber? Also was versteht die Richtlinie unter dem Begriff und vor allem, welche Pflichten kommen auf die Betreiber zu?

00:03:41 John

Ja, also zuerst einmal werden unter Betreiber eines wesentlichen Dienstes aus einem kritischen Versorgungssektor solche IT-Dienste gefasst, welche bei einem Sicherheitsvorfall das öffentliche Leben erheblich einschränken würden. Also dann für die Aufrechterhaltung diese Dienste tatsächlich unerlässlich sind. Erfasst werden zum Beispiel Energieversorger, Gesundheitsdienstleister, Krankenhäuser oder Betreiber von wesentlichen digitalen Infrastrukturen. Zusätzlich werden aber

auch Anbieter digitaler Dienste, wie zum Beispiel Online-Suchmaschinen oder Cloud-Computing Dienste, erfasst, weil auch die eine sehr hohe Kritikalität bezüglich der Datensicherheit z. B. haben. Nicht erfasst werden hingegen Anbieter sozialer Netzwerke oder kleine Unternehmen. Jetzt ist es so, dass die Richtlinie diese Betreiber dann zu verschiedenen Sicherheitsanforderungen und Meldeauflagen verpflichtet und es müssen dazu dann zum Beispiel Maßnahmen ergriffen werden, um diese Sicherheitsrisiken auch zu bewältigen. Im Falle eines Sicherheitsvorfalls mit den erheblichen Auswirkungen auf die Verfügbarkeit des Dienstes, also es muss auch schon ein gewisser Grad erreicht werden, muss dann zum Beispiel auch eine Meldung an die zuständige Behörde erfolgen.

00:04:42 Müller

Also wurden durch die ursprüngliche Fassung der NIS Richtlinie einerseits die Mitgliedstaaten, aber auch andererseits Betreiber selbst von wesentlichen Diensten verpflichtet. Und wie der Name selbst schon ziemlich klar sagt, handelt es sich bei der NIS Richtlinie um eine Richtlinie, also nicht um eine Verordnung, wie es zum Beispiel bei der Datenschutzgrundverordnung der Fall ist.

00:05:00 John

Ja genau. Also europäische Richtlinien haben, im Gegensatz zu der eben, wie zum Beispiel von dir schon genannten Verordnung DSGV, wie auch immer, in den Mitgliedstaaten keine unmittelbare Rechtswirkung. Also das bedeutet, die müssen zuerst durch den nationalen Gesetzgeber, bei uns natürlich durch den deutschen Gesetzgeber, in nationales Recht umgesetzt werden. Und das bedeutet, dass die europäischen Vorgaben in das nationale Recht integriert werden oder neu eingeführt werden müssen. Und durch die NIS Richtlinie wurde eine sogenannte Mindestharmonisierung festgelegt, sprich die Richtlinie legt Mindestanforderungen fest, aber darüberhinausgehende Regelungen für ein höheres Schutzniveau sind durchaus in den einzelnen Ländern zulässig.

00:05:36 Müller

Und wie genau sah dann die Umsetzung der Richtlinie in Deutschland aus?

00:05:39 John

In Deutschland gab es schon vor dem Inkrafttreten der Richtlinie seit 2015 das sogenannte IT-Sicherheitsgesetz. Damit waren schon ziemlich viele Anforderungen der NIS Richtlinie in Deutschland abgedeckt. Festgelegt wurden dort insbesondere die Pflichten von Unternehmen im Bereich kritischer Infrastruktur.

00:05:56 John

Es gab aber damals auch noch ein paar andere Bereiche, in denen die Richtlinie deutlich über den damaligen status quo des IT-Sicherheitsgesetzes hinausging. Vor allem Regelungen zu den Anbietern digitaler Dienste fanden sich dort dann noch nicht, das hatte damals der deutsche Gesetzgeber noch nicht für regelungswürdig erachtet oder hatte einen anderen Sicherheitsmaßstab angesetzt. Und 2017 wurden deshalb die fehlenden Anpassungen vorgenommen, sodass dann 2018 das Umsetzungsgesetz der NIS Richtlinie in Deutschland in Kraft getreten ist.

00:06:22 Müller

OK, also als vielleicht eine kleine Zusammenfassung zur ersten NIS Richtlinie. Die war damals eine Reaktion auf die immer höher werdende Zahl von Cyberangriffen und sollte dafür sorgen, dass in den

Mitgliedstaaten einheitliche Mindestanforderungen für die IT Sicherheit gelten. Und in Deutschland wurden ein paar Bereiche noch angepasst. Bereits davor gab es schon einen recht hohen IT-Sicherheitsschutz. Und jetzt wollen wir vor allem mit der zweiten Richtlinie, der NIS 2 Richtlinie, beschäftigen. Was genau regelt die denn jetzt und wieso war sie eigentlich noch nötig?

00:06:51 John

Ja, tatsächlich war es so, dass nach Ablauf der Umsetzungsfrist sich ziemlich schnell gezeigt, dass auf europäischer Ebene noch weiterer Anpassungsbedarf besteht. Mit der NIS Richtlinie sollte eine Mindestharmonisierung erreicht werden, allerdings wurde die Richtlinie den Mitgliedstaaten sehr unterschiedlich umgesetzt. Jetzt haben wir eben schon darüber gesprochen, dass mit der Richtlinie zum Beispiel die Betreiber wesentlicher Dienste in die Pflicht genommen wurden. Aber was genau ein wesentlicher Dienst ist, wurde dann in den Mitgliedstaaten wieder sehr unterschiedlich definiert, sodass es da bis heute eben keinen einheitlichen Adressatenkreis gab. Und zum anderen wurden auch zum Beispiel Umsetzungen der Pflichten nicht überwacht, was die Wirkung der Richtlinie in der Praxis tatsächlich ziemlich geschwächt hat. Also was bringt eine Regelung, wenn sie nicht durchgesetzt wird. Und daran hat sich dann gezeigt, dass eben die NIS-Richtlinie zwar grundsätzlich gut war, aber das Sicherheitsniveau bislang einfach noch zu niedrig war. Und genau deshalb hat die Europäische Kommission dann die NIS 2 Richtlinie auf den Weg gebracht, und die ist jetzt nun im Januar 2023 in Kraft getreten und muss von den Gesetzgebern der Mitgliedstaaten, also auch in Deutschland, bis Oktober 2024 in nationales Recht umgesetzt werden.

00:07:51 Müller

Okay und was sind jetzt die maßgeblichen neuen Änderungen, also die neuen Regelungen?

00:07:57 John

Ja, im Endeffekt soll die NIS 2 Richtlinie die Cybersicherheit noch mal modernisieren und dann auch erweitern. Konkret beinhaltet das zunächst einmal eine deutliche Erweiterung des Anwendungsbereichs. Bisher wurde ja wie gesagt zwischen wesentlichen und digitalen Diensten differenziert. Jetzt werden wesentliche Dienste von wichtigen Diensten unterschieden, also das heißt, damit werden alle bisherigen Adressaten auch als neue Adressaten erfasst. Welche Dienste und Einrichtungen in welche Kategorien allerdings fallen, ergibt sich dann aus den Anhängen der Richtlinie. Danach sind wesentliche Dienste solche mit hoher Kritikalität. Zum Beispiel Anbieter von Rechenzentrums-Diensten oder öffentliche Kommunikationsnetze. Oder auch eben die öffentliche Verwaltung. Wichtige Einrichtungen sind dagegen solche, die zwar grundsätzlich wesentliche Dienste sind, aber aufgrund ihrer Größe nicht wesentlich sind. Also da gibt es doch bestimmte Größenvorgaben. Beispiele sind zum Beispiel Online-Marktplätze, Suchmaschinen oder nun auch soziale Netzwerke, das ist ein klarer Unterschied zur alten NIS 1 Richtlinie. Interessant ist aber insbesondere die sogenannte Size Cap Rule, also dass nun allgemein alle großen und mittelgroßen Unternehmen, die in einem der genannten Sektoren tätig sind, von der Regelung erfasst sind. Konkret sind das also alle Unternehmen mit mindestens 50 Mitarbeiter:innen oder einer Jahresbilanz von über 10.000.000€. Damit wird dann der Adressatenkreis der Richtlinie eindeutiger und es soll verhindert werden, dass die Mitgliedstaaten den Begriff der wesentlichen Dienste so unterschiedlich definieren, wie es bisher der Fall ist. Und das war ja eben eines der größten Probleme in der NIS Richtlinie.

00:09:21 Müller

OK, also haben wir nun einen festen Adressaten Kreis, und an den müssen sich jetzt alle Mitgliedstaaten halten?

00:09:26 John

Ja, nicht ganz. In bestimmten Bereichen lässt der Richtliniengeber weiterhin Ausnahmen zu, aber im Grundsatz hast du da völlig recht. Ja, damit würde auf jeden Fall eine einheitlichere Grundlage geschaffen.

00:09:36 Müller

Und zu der Erweiterung und zu der klaren Ausgestaltung des Anwendungsbereichs kommen mit der NIS 2 Richtlinie aber auch noch andere Änderungen hinzu. Zum Beispiel hast du eben gesagt, dass auch das Sicherheitsniveau in der NIS Richtlinie generell noch zu niedrig angesetzt war. Hat sich da etwas bei der neuen Richtlinie geändert?

00:09:53 John

Ja absolut, sogar ziemlich viel. Also zum Beispiel werden jetzt auch die Pflichten der betroffenen Unternehmen erneuert. Diese müssen weiterhin die bisherigen Präventionsmaßnahmen wie eben Backups oder Verschlüsselungstechnologien vornehmen und haben umfangreichere Meldepflichten jetzt aber bei erheblichen Sicherheitsvorfällen. Das gilt auch für die Lieferketten. Außerdem werden die Vorgaben bezüglich der Meldepflichten detaillierter ausgestaltet.

00:10:13 Müller

Das heißt für die Unternehmen selbst gibt es zukünftig strengere und detailliertere Vorgaben. Und wie sieht es mit den Mitgliedstaaten aus? Bleibt da alles beim Alten?

00:10:22 John

Ja, also auch da sie die NIS 2 Richtlinie im Vergleich zur NIS 1 Richtlinie eine Vertiefung der Pflichten vor. Z. B. sollen die Computer-Notfallteams, die auch schon von der NIS 1 Richtlinie angesprochen wurden, auf Anfrage nun auch proaktiv Schwachstellen-Scans vornehmen. Außerdem soll eine Schwachstellen Datenbank in Europa aufgebaut werden, damit die Mitgliedstaaten schneller Zugang zu den erforderlichen Informationen zu bestimmten Sicherheitsvorfällen bekommen können, also hier soll einfach ein verbesserter Datenaustausch passieren. Und außerdem werden auch die Aufsichts- und Durchsetzungsbefugnisse der nationalen Behörden verschärft. Also es gibt nun die Möglichkeit, zum Beispiel Bußgelder zu verhängen.

00:10:55 Müller

Also hat sich doch nochmal einiges getan im Vergleich zur ersten Richtlinie. Und bis Oktober 2024 hat jetzt der deutsche Gesetzgeber Zeit, die NIS 2 Richtlinie in das nationale Gesetz umzusetzen. Und was genau muss jetzt konkret angepasst werden?

00:11:10 John

Tatsächlich ist es gar nicht so viel, wie man nach unserem Gespräch gerade denken könnte. Weil tatsächlich ist der deutsche Gesetzgeber der Kommission, wie schon damals bei der NIS 1 Richtlinie, teilweise zuvorgekommen und hat das IT-Sicherheitsgesetz schon mit dem IT-Sicherheitsgesetz 2.0, umgangssprachlich gesagt, 2021 überarbeitet und dieses knüpft an die Eigenschaft als Unternehmen der kritischen Infrastruktur an. Es müssen daher nur geringe Anpassungen im Grunde vorgenommen werden.

00:11:36 Müller

OK, und die neue Richtlinie sieht für ihren Anwendungsbereich vor, dass zum einen Verwaltungseinrichtungen, Forschungseinrichtungen, aber auch Bildungseinrichtungen vom Anwendungsbereich teilweise umfasst sind, teilweise auch nicht, teilweise besteht Umsetzungsspielraum für die Mitgliedstaaten. Müssen wir vielleicht ganz kurz einen Ausblick geben, wie sich die Umsetzung der NIS Richtlinie, der NIS 2 Richtlinie, für die Forschungseinrichtungen und Universitäten auswirken könnte.

00:12:00 John

Ja klar. Einerseits ist es da wichtig zu sehen, dass mit Sicherheit nicht alle Forschungsbereiche mit der Erweiterung des Anwendungsbereichs, auf die zum Beispiel öffentliche Verwaltung und Forschung, sich konfrontiert sehen werden. Man muss jetzt natürlich sagen, bislang hat der Gesetzgeber hierzu noch keine Stellung gegeben, wie sich das genau auswirken wird, da werden wir den ersten Gesetzentwurf des neuen IT-Sicherheitsgesetzes dann sehen müssen. Auf alle Fälle sind auf der anderen Seite manche Bereiche schon längst einbegriffen. Zum Beispiel Universitätskliniken sind vom IT-Sicherheitsgesetz schon längst erfasst, als eben Krankenhäuser. Sprich also, es ist hier noch überhaupt nicht klar, was am Ende dann eben von den Sektoren der öffentlichen Verwaltung oder Forschung erfasst wird, auch zum Beispiel bei den jetzt angesprochenen Bildungseinrichtungen hat der deutsche Gesetzgeber dann gewissen Spielraum, und da müssen wir jetzt einfach die Umsetzung abwarten und dann tatsächlich schauen, was dann faktisch umgesetzt werden muss.

00:12:47 Müller

OK, also können wir zusammenfassend ein bisschen sagen, dass in Deutschland zumindest der theoretische Umsetzungsbedarf eher gering ausfällt. Wenn man sich dann die praktischen Auswirkungen anschaut, dass da schon erhebliche Änderungen auf uns zu kommen können.

00:13:00 John

Ja absolut, es werden viel mehr Unternehmen jetzt eingebunden und die Pflichten sind auch deutlich erweitert worden.

00:13:05 Müller

Genau also darf man die Änderungen auf jeden Fall nicht unterschätzen, die durch die neue Richtlinie auf uns zukommen werden. Und ja, deshalb danke ich dir, lieber Nicolas, dafür, dass du uns diesen guten Überblick über die neuen Änderungen gegeben hast, über die neue Richtlinie, und ich danke Ihnen, liebe Hörerinnen und Hörer, für Ihre Aufmerksamkeit und ich würde sagen, wir haben heute mal wieder richtig was weggeforscht.

00:13:24 John

Ja, absolut.

00:13:25 Müller

Und in diesem Sinne bis zur nächsten Folge. Ja, Tschüss.