ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Barenkamp, Marco

Article — Published Version

Auswirkungen von NIS-2 für das Management von Unternehmen

Wirtschaftsinformatik & Management

Provided in Cooperation with:
Springer Nature

Suggested Citation: Barenkamp, Marco (2024) : Auswirkungen von NIS-2 für das Management von Unternehmen, Wirtschaftsinformatik & Management, ISSN 1867-5913, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 16, Iss. 2, pp. 70-78, https://doi.org/10.1365/s35764-024-00518-1

This Version is available at:
https://hdl.handle.net/10419/315854

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

http://creativecommons.org/licenses/by/4.0/deed.de

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

Auswirkungen von NIS-2 für das Management von Unternehmen

Marco Barenkamp

Wirtschaftsinformatik & Management 2024 • 16 (2): 70–78
https://doi.org/10.1365/s35764-024-00518-1
Angenommen: 2. April 2024
Online publiziert: 11. Juni 2024
© The Author(s) 2024

In der sich stetig wandelnden Welt der Technologie und Digitalisierung ist die Cybersicherheit zu einer zentralen Säule für das sichere und reibungslose Funktionieren von Unternehmen und sogar ganzen Volkswirtschaften geworden. Mit der zunehmenden Vernetzung und der Abhängigkeit von digitalen Infrastrukturen steigt jedoch auch das Risiko von Cyberangriffen, Datenlecks und anderen sicherheitsrelevanten Vorfällen. Das zeigt auch die Tatsache, dass täglich eine Vielzahl neuer Schadprogramm-Varianten entstehen (**Abb. 1**). Sie kommen auf unterschiedlichsten Wegen zum Einsatz, weshalb es auch so viele verschiedene Arten von Cyberangriffen gibt [1].

Um diesen Herausforderungen zu begegnen und ein hohes gemeinsames Niveau an Cybersicherheit in der Europäischen Union sicherzustellen, wurde die NIS-Richtlinie (Network and Information Security – Richtlinie über die Sicherheit von Netz- und Informationssystemen) eingeführt und später durch die überarbeitete Version, NIS-2, ergänzt und verstärkt.

Die NIS-2-Richtlinie zielt darauf ab, die Widerstandsfähigkeit (Resilienz) und Sicherheit kritischer und wichtiger Entitäten über eine breitere Palette von Sektoren hinweg zu verbessern. Sie bringt erweiterte Anforderungen und strenge Regeln mit sich, die vor allem auch das Management von Unternehmen direkt betreffen. Diese Entwicklungen erfordern eine umfassende Auseinandersetzung mit den neuen Vorschriften, um sowohl die Compliance sicherzustellen als auch die inhärenten Risiken zu minimieren, die mit der digitalen Transformation einhergehen [2].

Die Einführung dieser Richtlinie stellt Unternehmen vor die Aufgabe, ihre bestehenden Sicherheitspraktiken zu überdenken und anzupassen. Dies erfordert nicht nur eine technische Neuausrichtung, sondern auch ein Umdenken in der Unternehmenskultur und im Managementverhalten. Cybersicherheit wird nicht länger als eine isolierte IT-Aufgabe angesehen, sondern als eine zentrale Managementverantwortung, die wesentlich zur Wettbewerbsfähigkeit, zum Vertrauen der Stakeholder und zur langfristigen Nachhaltigkeit eines Unternehmens beiträgt.

Grundlagen von NIS-2

Angesichts wachsender Cyberbedrohungen hat die Europäische Union (EU) ihre Bemühungen intensiviert, ein einheitliches und hohes Sicherheitsniveau von Netz- und Informationssystemen über alle Mitgliedstaaten hinweg zu gewährleisten. Ein zentraler Baustein dieser Strategie ist die Überarbeitung der ursprünglichen NIS-Richtlinie (Direktive 2016/1148) zur NIS-2-Richtlinie. Diese Erweiterung reflektiert die Notwendigkeit, sowohl die Reichweite als auch die Tiefe der cybersicherheitsrelevanten Maßnahmen zu verstärken.

Die ursprüngliche NIS-Richtlinie, die erste EU-weite Cybersicherheitsvorschrift, trat 2016 in Kraft und zielte darauf ab, ein gemeinsames Niveau an Netz- und Informationssystemsicherheit innerhalb der EU zu etablieren [3]. Angesichts der dynamischen Cyberbedrohungslage, nicht zuletzt durch die Konflikte in der Ukraine, und der Erkenntnis, dass die ursprünglichen Maßnahmen nicht ausreichten, wurde die Notwendigkeit einer Überarbeitung deutlich.

Prof. Dr. Marco Barenkamp LL.M. *(✉) ist promovierter Wirtschaftsinformatiker und studierter Wirtschaftsjurist. Als Gründer der LMIS AG mit Hauptsitz in Osnabrück ist er im Aufsichtsrat der Gesellschaft tätig. Als Vorsitzender des wissenschaftlichen Beirats der Studiengesellschaft für Künstliche Intelligenz e. V. unterstützt er den öffentlichen Diskurs über Fragen der künstlichen Intelligenz, insbesondere zu den gesellschaftlichen, politischen, ökonomischen und sozialen Implikationen der Entwicklungen, basierend auf wissenschaftlichen Erkenntnissen der relevanten Fachdisziplinen. Als Mitglied der Bundesfachkommission Künstliche Intelligenz und Wertschöpfung 4.0 im Wirtschaftsrat Deutschland setzt er sich auf bundespolitischer Ebene für zukunftsorientierte Rahmenbedingungen für KI in Deutschland und der Europäischen Union ein. Für einen kontinuierlichen Austausch zwischen Wissenschaft und Wirtschaft lehrt Marco Barenkamp mit den Schwerpunkten Management & KI.*
Marco.Barenkamp@lmis.de

[1]Hochschule Osnabrück, Osnabrück, Deutschland

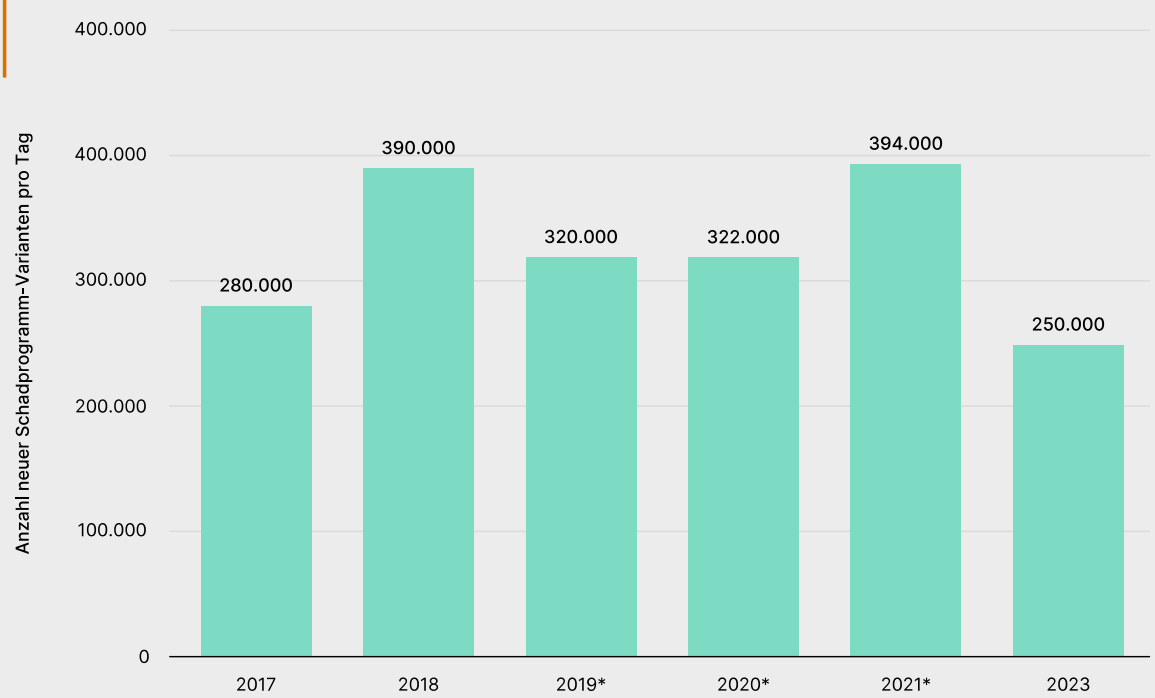
Zusammenfassung

- NIS-2 intensiviert die Sicherheits- und Meldeanforderungen, erweitert den Anwendungsbereich und stärkt die Cybersicherheitskultur in Unternehmen.
- Unternehmen stehen vor der Herausforderung, Ressourcen effizient einzusetzen, um Compliance zu erreichen, sehen sich aber auch mit Chancen für verbesserte Sicherheit und Wettbewerbsvorteile konfrontiert.
- Kontinuierliche Anpassung an die dynamische Cybersicherheitsumgebung und proaktive Reaktion auf neue regulatorische Anforderungen sind für die langfristige Resilienz entscheidend.

Die NIS-2-Richtlinie baut auf den Grundlagen von NIS auf und erweitert diese signifikant. Hierbei wird das primäre Ziel verfolgt, ein hohes gemeinsames Sicherheitsniveau der Netz- und Informationssysteme in der gesamten EU zu erreichen. Dies soll durch die Stärkung der Sicherheitsanforderungen, die Ausweitung des Anwendungsbereichs auf mehr Sektoren und Unternehmen sowie durch verbesserte Meldepflichten im Falle von Sicherheitsvorfällen erreicht werden.

Die Richtlinie stellt eine umfassende Erweiterung der Cybersicherheitsanforderungen innerhalb der Europäischen Union dar, die mehrere Schlüsselelemente beinhaltet, um die Resilienz gegenüber Cyberbedrohungen zu stärken. Ein wesentliches Merkmal ist die Ausweitung des Kreises der betroffenen Entitäten. Indem sie zusätzliche Sektoren und Dienste einschließt, die als kritisch für die Gesellschaft und Wirtschaft angesehen werden, zielt NIS-2 darauf ab, eine breitere und effektivere Sicherheitsbasis zu schaffen. Zu diesen Sektoren gehören beispielsweise Energie, Transport, Bankwesen, digitale Infrastruktur und öffentliche Verwaltung. Unternehmen, die unter diese erweiterte Definition fallen, sind nun angehalten, angemessene technische und organisatorische Maßnahmen zu ergreifen. Diese Maßnahmen sollen dazu dienen, Cyberrisiken zu managen und die Sicherheit ihrer Netz- und Informationssysteme zu gewährleisten, um so eine solide Verteidigungslinie gegen mögliche Cyberangriffe zu bilden – sowohl unternehmensintern als auch europaweit [4].

Abb. 1 Täglicher Zuwachs neuer Schadprogramme, * Erfassung inkl. PUA (Potentially unwanted application)



Zudem hat die Richtlinie die Anforderungen an die Meldung von Cybersicherheitsvorfällen verschärft. Dieser Schritt soll eine schnellere und stärker koordinierte Reaktion auf Sicherheitsbedrohungen ermöglichen, indem sicherheitsrelevante Informationen zeitnah geteilt werden, um potenzielle Schäden zu minimieren und die Reaktionsfähigkeit zu verbessern. Darüber hinaus schafft NIS-2 einen rechtlichen Rahmen, der alle Mitgliedstaaten dazu verpflichtet, nationale Strategien zur Cybersicherheit zu entwickeln [5]. Die Einrichtung nationaler Kompetenzzentren für Cybersicherheit wird vorangetrieben, um Fachwissen zu bündeln und die Effektivität der Maßnahmen zu steigern. Mitgliedstaaten müssen zudem Aufsichts- und Sanktionsregime einführen, die die Einhaltung der Richtlinie überwachen und durchsetzen, was die Verbindlichkeit und Wirksamkeit der Cybersicherheitsbemühungen innerhalb der EU insgesamt stärkt [6].

Auswirkungen auf das Management von Unternehmen

Diese erweiterten Anforderungen haben tiefgreifende Auswirkungen auf das Management von Unternehmen, insbesondere in Sektoren, die als wesentlich für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Aktivitäten angesehen werden. Die Richtlinie fordert eine proaktive und ganzheitliche Herangehensweise an die Cybersicherheit, die weit über die technischen Aspekte hinausgeht und strategische, organisatorische sowie compliancebezogene Maßnahmen umfasst.

Eine der signifikantesten Auswirkungen von NIS-2 ist die Notwendigkeit für das Management, Cybersicherheit als integralen Bestandteil der Unternehmensstrategie zu betrachten [7]. Führungskräfte müssen nun sicherstellen, dass Cybersicherheitsrisiken auf höchster Ebene bewertet und gesteuert werden. Dies erfordert eine enge Zusammenarbeit zwischen IT-Sicherheitsteams und der Geschäftsführung, um sicherzustellen, dass Cybersicherheitsstrategien mit den Geschäftszielen in Einklang stehen und angemessene Ressourcen für ihre Umsetzung bereitgestellt werden.

Die NIS-2-Richtlinie bringt erweiterte Complianceanforderungen mit sich, die Unternehmen dazu zwingen, ihre bestehenden Sicherheitspraktiken zu überprüfen und anzupassen. Das Management muss ein tiefgehendes Verständnis der rechtlichen Anforderungen entwickeln und sicherstellen, dass die Organisation diese erfüllt. Dies umfasst die Implementierung von Richtlinien und Verfahren für das Risikomanagement, die Sicherheitsüberprüfung und die Meldung von Sicherheitsvorfällen. Die Nichtbeachtung kann zu erheblichen finanziellen Strafen und Reputationsverlust führen [8].

Die Richtlinie erfordert die Einrichtung eines robusten Risikomanagementsystems und Governancestrukturen, die sicherstellen, dass Cybersicherheitsrisiken systematisch identifiziert, bewertet und gemindert werden [9]. Unternehmen müssen in der Lage sein, ihre Risikoexposition kontinuierlich zu überwachen und anzupassen, um auf sich ändernde Bedrohungslandschaften zu reagieren. Dies schließt die Entwicklung von Notfallplänen und Reaktionsstrategien für Sicherheitsvorfälle ein.

Kernthese 1

Eine agile Anpassung an die sich wandelnde Cybersicherheitslandschaft und zukünftige Gesetzgebung ist für Unternehmen essenziell.

Kernthese 2

Die Richtlinie stellt Herausforderungen dar, bietet aber auch Chancen zur Stärkung der Cybersicherheit und des Vertrauens.

Eine weitere wesentliche Auswirkung betrifft die Rolle der Mitarbeiter im Bereich der Cybersicherheit. Die NIS-2-Richtlinie betont die Notwendigkeit, das Bewusstsein und die Kompetenzen der Mitarbeiter in Bezug auf Cybersicherheitsrisiken zu erhöhen [10]. Dies erfordert regelmäßige Schulungen und Sensibilisierungsmaßnahmen, um sicherzustellen, dass alle Mitarbeiter die Sicherheitsrichtlinien verstehen und umsetzen können.

Während die Einhaltung der NIS-2-Richtlinie zunächst als Herausforderung erscheinen mag, bietet sie auch Chancen für Innovation und kann einem Unternehmen einen Wettbewerbsvorteil verschaffen. Unternehmen, die eine Vorreiterrolle in der Implementierung fortschrittlicher Cybersicherheitsmaßnahmen einnehmen, können das Vertrauen ihrer Kunden stärken und sich als vertrauenswürdige Partner auf dem Markt positionieren.

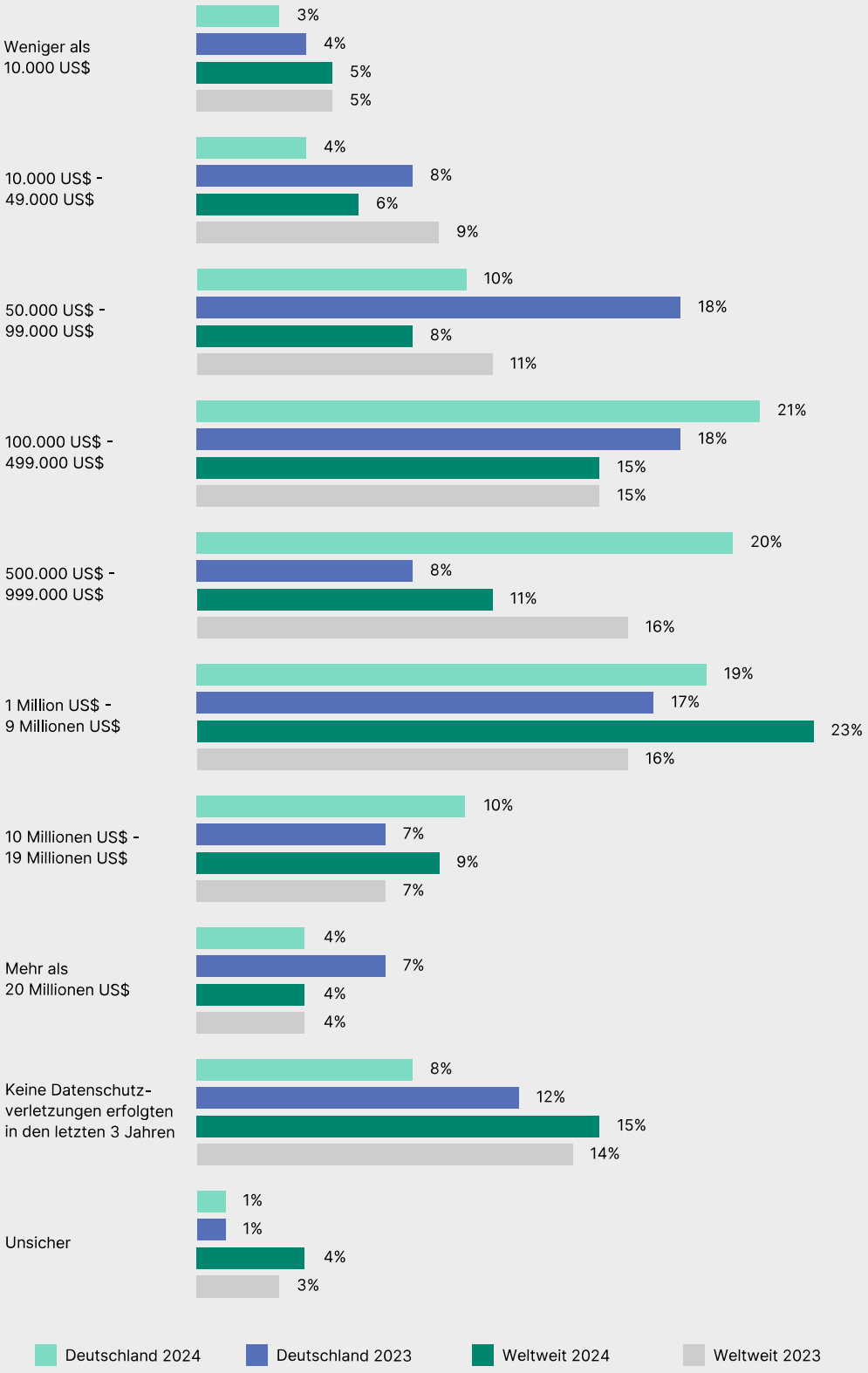
Herausforderungen und Chancen

Die Implementierung der NIS-2-Richtlinie stellt Unternehmen vor eine Vielzahl von Herausforderungen, bietet aber gleichzeitig auch bedeutende Chancen, ihre Cybersicherheitspraktiken zu verbessern und ihre Marktposition zu stärken.

Eine der größten Hürden ist die Schwierigkeit, die erweiterten und detaillierten Vorschriften einzuhalten. Unternehmen müssen ihre bestehenden Sicherheitspraktiken nicht nur überprüfen, sondern auch an die spezifischen Anforderungen der Richtlinie anpassen, was umfassende Kenntnisse der rechtlichen Rahmenbedingungen und eine kontinuierliche Anpassung an sich ändernde Vorschriften erfordert. Zusätzlich erfordert die Implementierung der durch NIS-2 geforderten Sicherheitsmaßnahmen und Governancestrukturen erhebliche Investitionen in Zeit, Personal und Finanzen. Insbesondere kleinere und mittlere Unternehmen könnten vor der Herausforderung stehen, die notwendigen Ressourcen bereitzustellen. Darüber hinaus verlangt die Richtlinie von den Unternehmen technische und organisatorische Anpassungen, was eine umfangreiche Neugestaltung bestehender Systeme erfordern kann. Angesichts der dynamischen Natur der Cyberbedrohungslandschaft müssen Unternehmen ihre Sicherheitsmaßnahmen zudem kontinuierlich evaluieren und aktualisieren, was nicht nur technologische Agilität, sondern auch eine Kultur der ständigen Wachsamkeit und des Lernens voraussetzt.

Trotz dieser Herausforderungen bietet NIS-2 den Unternehmen auch erhebliche Chancen. Die Richtlinie ermöglicht es ihnen, ihre Cybersicherheitspraktiken zu überprüfen und zu stärken, was zu einer erhöhten Widerstandsfähigkeit gegenüber Cyberangriffen führen kann. Dazu sind die aus Cyberangriffen hervorgehenden finanziellen Schäden erheblich. Eine weltweite Befragung von 3000 Führungskräften durch das Unternehmen PwC (**Abb. 2**) ergab, dass bei 70 % der deutschen Unternehmen, die Opfer von Cybervorfällen geworden sind, Kosten von 100.000 bis 20 Mio. US-Dollar entstanden [11]. Durch entsprechende Abwehrmaßnahmen, wie sie durch NIS-2 nun zur Pflicht werden, lassen sich solche finanziellen Schäden minimieren, wenn nicht sogar vermeiden.

Abb. 2 Geschätzte Kosten für die Organisation bei Cybervorfällen



Kernthese 3

NIS-2 verlangt eine Integration der Cybersicherheit in die Unternehmensführung durch erweiterte Sicherheitsanforderungen.

Unternehmen, die hohe Cybersicherheitsstandards nachweisen können, stärken außerdem das Vertrauen ihrer Kunden und Geschäftspartner, was besonders in datensensitiven Branchen einen wichtigen Wettbewerbsvorteil darstellen kann. Die Anforderungen von NIS-2 können zudem als Katalysator für die Entwicklung einer starken Cybersicherheitskultur innerhalb eines Unternehmens dienen und das Bewusstsein sowie die proaktive Haltung zur Risikominderung fördern. Schließlich kann die Notwendigkeit, sich an die Vorschriften anzupassen, Unternehmen dazu anregen, innovative Lösungen für Cybersicherheitsprobleme zu entwickeln. Das wiederum kann zu technologischen Fortschritten und einer Verbesserung der Effizienz und Effektivität von Cybersicherheitsmaßnahmen führen.

Fazit und Ausblick

Die Einführung und Implementierung der NIS-2-Richtlinie stellt einen bedeutenden Schritt in Richtung einer verstärkten Cybersicherheit und Resilienz digitaler Infrastrukturen dar. Durch die Erweiterung des Geltungsbereichs, die Verschärfung der Sicherheitsanforderungen und die Verbesserung der Meldepflichten bei Cybersicherheitsvorfällen wird das Bewusstsein für die Bedeutung einer robusten Cybersicherheit in Unternehmen und öffentlichen Einrichtungen signifikant erhöht. Diese Richtlinie fordert eine strategische Neuausrichtung, in der Cybersicherheit nicht nur als technische Notwendigkeit, sondern vor allem als integraler Bestandteil der Unternehmensführung und -kultur verstanden wird.

Die Anpassung an die beschriebenen Vorgaben bringt für Unternehmen selbstverständlich Herausforderungen mit sich, wie eine erhöhte Komplexität der Compliance, der Bedarf an zusätzlichen Ressourcen für die Implementierung der erforderlichen Maßnahmen und die Notwendigkeit, interne Prozesse und Systeme umfassend zu überdenken. Gleichzeitig eröffnet die Richtlinie aber auch bedeutende Chancen: Sie bietet die Möglichkeit, die eigene Cybersicherheit zu stärken, das Vertrauen von Kunden und Geschäftspartnern zu erhöhen und eine Kultur der Cybersicherheit zu fördern, die das Unternehmen gegenüber den sich ständig weiterentwickelnden Cyberbedrohungen sicherer macht.

Die kontinuierliche Anpassung und Verbesserung der Cybersicherheitsstrategien und -praktiken wird somit eine dauerhafte Aufgabe für Unternehmen sein. Die Cybersicherheitslandschaft gestaltet sich dynamisch und Bedrohungen entwickeln sich kontinuierlich weiter. Unternehmen müssen daher agil bleiben, ihre Sicherheitsmaßnahmen regelmäßig überprüfen und aktualisieren sowie in die Ausbildung und Sensibilisierung der Mitarbeiter investieren. Gleichzeitig ist zu erwarten, dass die Europäische Union ihre legislativen und regulativen Rahmenbedingungen weiterentwickeln wird, um auf neue Bedrohungen und technologische Entwicklungen zu reagieren. Dies könnte weitere Anpassungen der NIS-Richtlinie oder die Einführung neuer Vorschriften mit sich bringen.

Hinweis des Verlags
Der Verlag bleibt in Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutsadressen neutral.

Funding. Open access funding provided by Projekt DEAL.

Open Access. Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.
Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.
Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf http://creativecommons.org/licenses/by/4.0/deed.de.

Literatur

[1] BSI (2023). Die Lage der IT-Sicherheit in Deutschland 2023, (S. 12), Lagebericht, Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html. Zugegriffen: 15. März 2024.

[2] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/80 Abs. 1.

[3] Richtlinie (EU) Nr. 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABI. L 194/1 Abs. 4.

[4] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/108-111 Art. 2-3.

[5] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/115-116 Art. 7.

[6] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/134-139 Art. 30-33.

[7] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/88 Absatz 36.

[8] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/139 Art. 34.

[9] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/127 Art. 20.

[10] Richtlinie (EU) Nr. 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABI. L 333/80 Art. 7 Abs. 1f.

[11] PwC (2024). *Digital Trust Insights 2024. Die deutschen Ergebnisse einer weltweiten PwC-Befragung zum Thema Cyber Security,* PricewaterhouseCoopers GmbH. https://www.pwc.de/de/cyber-security/digital-trust-insights.html. Zugegriffen: 15. März 2024.

Springer Professional | **Mehr zum Thema finden Sie online**
www.springerprofessional.de/wum