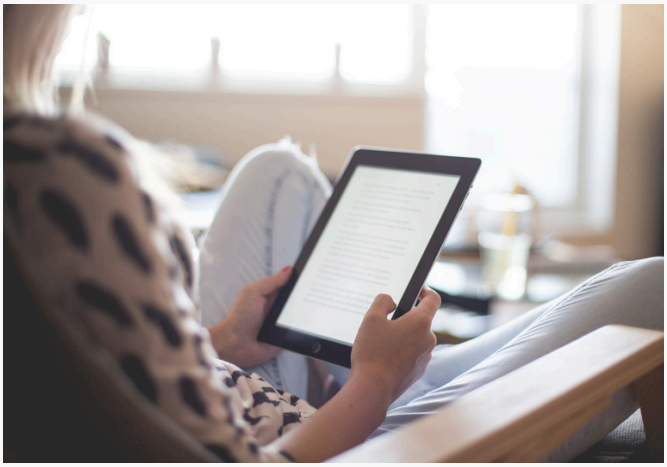
FORUM WISSEN, DAS ANKOMMT.


Leseprobe

Unsere Fachinhalte bieten Ihnen praxisnahe Lösungen, wertvolle Tipps und direkt anwendbares Wissen für Ihre täglichen Herausforderungen.

- **Praxisnah und sofort umsetzbar**: Entwickelt für Fach- und Führungskräfte, die schnelle und effektive Lösungen benötigen.
- **Fachwissen aus erster Hand**: Inhalte von erfahrenen Expertinnen und Experten aus der Berufspraxis, die genau wissen, worauf es ankommt.
- **Immer aktuell und verlässlich**: Basierend auf über 30 Jahren Erfahrung und ständigem Austausch mit der Praxis.

Blättern Sie jetzt durch die Leseprobe und überzeugen Sie sich selbst von der Qualität und dem Mehrwert unseres Angebots!

Merkblatt

Lieferkette

Ein adäquates Risikomanagement, insbesondere durch ein Informationsmanagementsystem, sichert Unternehmen vor Cyberangriffen oder reduziert jedenfalls deren Auswirkungen. Auch Sicherheitslücken in der Lieferkette können zu relevanten Auswirkungen bei den Unternehmen führen. Unternehmen sind zunehmend auf komplexe Netzwerke von Zulieferern und Dienstleistern angewiesen, um ihre Produkte und Dienstleistungen zu erbringen. Diese Vernetzung bringt erhebliche Risiken mit sich, auch im Bereich der Cybersicherheit. Dies gilt für Dienstleister, die unmittelbar in den Betrieb der IT-Infrastruktur oder relevanter Anwendungen, etwa als Auftragsverarbeiter, eingebunden sind. Dies gilt ebenfalls für Produkte, von der Soft- bis zur Hardware, die vom Unternehmen selbst betrieben werden. Schwachstellen in diesen Leistungen und Produkten können zu erfolgreichen Cyberangriffen auf das Unternehmen führen. Das gilt sowohl bei Angriffen auf die Lieferanten, die sich wegen Auswirkungen in den Leistungen und Produkten auf das Unternehmen auswirken, als auch, wenn ein Unternehmen gezielt über die Lieferkette attackiert wird.

Daher ist die „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern“ wesentlicher Baustein der nach Art. 21 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 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) verpflichtenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit. Auch der nationale Umsetzungsentwurf der NIS-2-Richtlinie in der Fassung vom 2. Oktober 2024 (BT-Drs. 20/13184, nachfolgend bezeichnet als „BSIG-E“) sieht diesen Punkt in § 30 vor. Die Absicherung der Lieferkette ist zudem seit Langem bekannt und verpflichtend für personenbezogene Daten verarbeitende Auftragsverarbeiter (Art. 28, 32 DSGVO).

Identifikation relevanter Berührungspunkte

Ausgangspunkt für die Absicherung der Lieferkette ist die Identifikation und das Mapping der relevanten Leistungen und Produkte sowie der Schnittstellen in personeller und technischer Sicht.

Produkte/Leistungen

Die Produkte und Leistungen in der Lieferkette, über die Cyberangriffe erfolgen könnten, müssen mit einer Risikopriorisierung identifiziert und gemappt werden. Dazu gehört auch, dass die Hersteller und Vertragspartner dokumentiert sind. Hierbei sollten zugleich die relevanten rechtlichen Anforderungen definiert werden, insbesondere neben dem allgemeinen IT-Sicherheitsrecht auch aus dem Datenschutzrecht.

Kritikalität bewerten

- Priorisieren Sie die Produkte und Leistungen entsprechend ihrer Bedeutung für den Geschäftsbetrieb.
- Bewerten Sie die möglichen negativen Auswirkungen auf Ihr Unternehmen oder Ihre Kunden.

Lebenszyklus überwachen

- Überwachen und dokumentieren Sie den Lebenszyklus der Produkte und Leistungen.
- Stellen Sie sicher, dass alle Änderungen und Aktualisierungen festgehalten werden.

Mitarbeitende

Alle Mitarbeitenden, die in Verbindung mit der Lieferkette stehen, sollten identifiziert werden. Die jeweiligen Rollen und Bezugspunkte in Bezug auf die Lieferkettensicherheit sind dabei zu bestimmen, Mitarbeitende sind über ihre spezifischen Aufgaben und Pflichten zu informieren.

Schnittstellen

Besonderes Augenmerk ist sodann auf die Schnittstellen personeller wie technischer Art zu legen, da an diesen Stellen zusätzliche Angriffsrisiken entstehen.

Dokumentation und Überwachung von relevanten Produkten und Leistungen

Die relevanten Produkte und Leistungen sind zu dokumentieren und zu überwachen. Die Absicherung der Lieferkette hat sodann auf mehreren Ebenen zu erfolgen, nämlich durch

- vertragliche Regelungen,
- Pflege von Lieferantenkontakten,
- Auditierung sowie
- Strukturierung in Richtlinien und Prozessen.

Die Verordnung (EU) 2024/2847, der sog. Cyber Resilience Act, wird zukünftig Hersteller digitaler Produkte, also etwa auch von Software, verpflichten, eine umfassende Sicherheitsdokumentation vorzuhalten (Software Bill of Materials, SBOM). Dies ermöglicht Unternehmen eine entsprechende Überprüfung und Bewertung der Cybersicherheit, wenn diese digitalen Produkte im eigenen Unternehmen eingesetzt werden. Die Verordnung gilt allerdings erst ab Ende 2027.

Vertragsgestaltung mit Sicherheitsanforderungen

Werden Produkte und Leistungen mit Cybersicherheitsrelevanz bezogen, sollte der Vertrag für ein angemessenes Cybersicherheitsniveau in der Lieferkette klare Sicherheitsanforderungen definieren, die im Einklang mit Standards wie der DIN ISO 27001 stehen. Neben der Definition der Sicherheitsstandards sind ihr Nachweis, die Überprüfung und Gewährleistung während des Lebenszyklus, Meldepflichten bei Sicherheitsvorfällen, Ansprüche auf Nachjustierungen und Regelungen zu Haftung und womöglich Vertragsstrafen bei Nichterfüllung zu bestimmen. Zunehmend verpflichten gesetzliche Vorgaben, etwa § 327f BGB oder künftig der Cyber Resilience Act, zur Bereitstellung von Sicherheitsupdates. Die Umsetzung sollte ebenfalls im Vertrag geregelt werden. All diese Vorgaben sind sowohl in der Vertragskette abzusichern als auch gegenüber Unterlieferanten. Die Details dazu sind im Merkblatt Vertragsgestaltung dargestellt.

Dies entspricht auch den Hinweisen in der Entwurfsbegründung zum BSIG-E, wie eine hinreichende Sicherheit der Lieferkette erreicht werden kann: Adressierte Einrichtungen sollten danach mit ihren Zulieferern und Dienstleistern vertragliche Vereinbarungen zu Risikomanagementmaßnahmen, der Bewältigung von Cybersicherheitsvorfällen und zum Patchmanagement treffen und festlegen, in welchem Umfang auch sie die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik zu ihren Produkten und Dienstleistungen zu berücksichtigen haben (BT-Drs. 20/13184, S. 140). Unter Umständen kann es angemessen sein, Zulieferer und Dienstleister zur Beachtung der Prinzipien „Security by Design“ und „Security by Default“ aufzufordern (BT-Drs. 20/13184, S. 140).

Pflege von Lieferantenkontakten

Transparenz schaffen

- Erlangen Sie ein tiefes Verständnis für Ihre Lieferkette und Ihre Zulieferer.
- Stellen Sie sicher, dass Sie wissen, welche Risiken sich aus den Beziehungen zu Ihren Zulieferern ergeben könnten.

Kommunikationspläne entwickeln

- Implementieren Sie Kontrollstrukturen und Kommunikationspläne.
- Stellen Sie sicher, dass Ihre Zulieferer über eine angemessene Sicherheitskultur verfügen.

Regelmäßiger Austausch

- Pflegen Sie regelmäßigen Kontakt zu Ihren Lieferanten.
- Führen Sie regelmäßige Meetings und Audits durch, um die Einhaltung der Sicherheitsstandards zu überprüfen.

Überprüfung von Sicherheitsmaßnahmen

Ziel der vertraglichen Absicherung von ausreichenden Cybersicherheitsanforderungen ist die tatsächliche Absicherung in der Lieferkette. Um dies zu erreichen, sollte die Einhaltung der vertraglichen Vorgaben kontinuierlich überprüft werden. Zentral sind daher:

- Regelmäßige Evaluation und Audits
- Entwicklung von Metriken, um die Effektivität zu messen
- Änderungen bei Bedarf umsetzen, um fortlaufend ein angemessenes Cybersicherheitsniveau zu gewährleisten
- Dokumentation der Ergebnisse der Audits, entwickelten Metriken und Änderungen

Plan – Do – Check – Act

Änderungen steuern

- Steuern Sie Änderungen bei der Bereitstellung von Dienstleistungen durch Lieferanten.
- Stellen Sie sicher, dass alle Änderungen dokumentiert und bewertet werden.

Risikobeurteilung

- Führen Sie bei Änderungen eine erneute Risikobeurteilung durch.
- Berücksichtigen Sie die Kritikalität der betroffenen Geschäftsinformationen und -systeme.

Entwicklung von Richtlinien und Prozessen

Die Absicherung der Lieferkette sollte in passenden Richtlinien und Prozessen strukturiert werden. Die Mitarbeitenden sind regelmäßig zu schulen.

WISSEN, DAS ANKOMMT.

Bestelloptionen

Cybersecurity speziell für KRITIS

Sie haben Fragen zum Produkt oder benötigen Unterstützung bei der Bestellung? Unser Kundenservice ist für Sie da:

08233 / 381-123 (Mo - Do 7:30 - 17:00 Uhr, Fr 7:30 - 15:00 Uhr)
service@forum-verlag.com

Oder bestellen Sie bequem über unseren Online-Shop:

Jetzt bestellen

FORUM VERLAG HERKERT GMBH, Mandichostraße 18, 86504 Merching,
Tel.: (08233) 381 123, E-Mail: service@forum-verlag.com, Web: shop.forum-verlag.com