

Lieferketten-Sicherheit: Warum die Pflicht auch die trifft, die nicht reguliert sind

Von Thomas Faß · 7. August 2026 · aktualisiert 9. September 2026

Lieferketten-Sicherheit adressiert das Risiko, dass Angreifer nicht die Organisation selbst kompromittieren, sondern ihre Lieferanten, Dienstleister oder Open-Source-Komponenten, um darüber Zugang zu erhalten. Die Sicherheitslage eines Unternehmens endet damit nicht an den eigenen Grenzen. Die Antwort ist keine einzelne Maßnahme, sondern Disziplin: abgesicherte Softwareentwicklung (DevSecOps, Software Bill of Materials), Zero-Trust-Architektur, phishing-resistente Authentifizierung und kontinuierliches Drittanbieter-Risikomanagement.

Das Wichtigste in Kürze

- Seit dem 6. Dezember 2025 ist Lieferkettensicherheit in Deutschland Gesetz: § 30 Absatz 2 Nummer 4 BSIG verlangt „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern“. Rund 29.500 Einrichtungen unterliegen direkt der BSI-Aufsicht – und geben die Anforderungen vertraglich an ihre Dienstleister weiter. Für Hersteller vernetzter Produkte beginnt am 11. September 2026 zusätzlich die CRA-Meldepflicht mit 24 Stunden Frist.
- Lieferketten-Sicherheit adressiert Angriffe, die nicht die Organisation selbst treffen, sondern ihre Lieferanten, Dienstleister oder Open-Source-Komponenten – der Zugang läuft über Dritte.
- Die Sicherheitslage endet nicht an den eigenen Grenzen: Angriffsvektoren sind kompromittierte Open-Source-Pakete, Drittanbieter/MSPs und Lücken in CI/CD-Pipelines.
- Es gibt keine Einzelmaßnahme, sondern Disziplin: DevSecOps mit Software Bill of Materials, Zero-Trust-Architektur, phishing-resistente Authentifizierung und kontinuierliches Drittanbieter-Risikomanagement.
- Die Bedrohung wächst messbar – Angriffe auf Software-Lieferketten und ihre Kosten steigen deutlich; TPRM und vertragliche Absicherung werden zur Pflicht.

Die moderne Unternehmenslandschaft ist untrennbar mit einem komplexen Geflecht aus Software-Lieferketten verbunden. Diese Vernetzung, die einst als reiner Effizienzgewinn betrachtet wurde, hat sich zu einer kritischen Angriffsfläche für Cyberkriminelle entwickelt. Die „Achillesferse“ der digitalen Welt liegt heute oft nicht mehr im Kern des eigenen Unternehmens, sondern in den scheinbar unscheinbaren Gliedern dieser weitläufigen Ketten. Ein umfassendes Verständnis der Bedrohungslandschaft und die Implementierung robuster Sicherheitsstrategien sind daher unerlässlich, um die Integrität und Resilienz der eigenen Lieferkette zu gewährleisten. Wir zeigen in diesem Artikel auf, wie die Lieferketten-Sicherheit in den Fokus von IT-Sicherheit und Co. rücken,

Einleitung: Die Lieferkette als neues Schlachtfeld der Cyberkriminalität

Die moderne Software-Lieferkette ist ein komplexes Geflecht aus internen Prozessen, externen Anbietern, Open-Source-Komponenten und Cloud-Diensten. Diese Vernetzung, die Effizienz und Innovation fördert, schafft gleichzeitig eine ausgedehnte Angriffsfläche, die Cyberkriminelle gezielt ausnutzen. Anstatt direkt gut verteidigte Unternehmensnetzwerke anzugreifen, suchen Angreifer den „Weg des geringsten Widerstands“ über weniger gesicherte Glieder in der Kette.

Die Ausnutzung von Vertrauensbeziehungen ist ein zentrales Element bei Lieferkettenangriffen. Die Sicherheitsposition einer Organisation wird nicht mehr nur durch ihre eigenen Grenzen definiert, sondern durch die kollektive Sicherheit all ihrer Drittpartner. Dies gilt insbesondere für Managed Service Provider (MSPs), die aufgrund ihres tiefen Zugriffs auf Kundennetzwerke eine häufige Angriffsfläche darstellen. Das implizite Vertrauen, das Unternehmen in ihre Partner setzen, wird so zu einer Schwachstelle. Traditionelle perimeterbasierte Sicherheitsansätze sind daher unzureichend, da Angriffe von „vertrauenswürdigen“ externen Quellen ausgehen können.

Die Häufigkeit und Schwere von Software-Lieferkettenangriffen hat in den letzten Jahren dramatisch zugenommen. Im Achten Jahresreport von 2022 wies Sonatype für den Zeitraum 2019 bis 2022 einen Anstieg dieser Angriffe um 742 Prozent aus; allein für 2021 nennt der Report über 600 Prozent gegenüber dem Vorjahr. Im Anchore-Report von 2022 gaben 62 Prozent der Organisationen an, im Jahr zuvor von einem Software-Lieferkettenangriff betroffen gewesen zu sein. In einer BlueVoyant-Befragung von 2021 sagten 93 Prozent der Unternehmen, sie hätten bereits eine direkte Sicherheitsverletzung aufgrund von Schwachstellen in ihrer Lieferkette erlitten. Juniper Research schätzte 2023, die Schäden würden von rund 46 Milliarden Dollar auf fast 81 Milliarden Dollar im Jahr 2026 steigen – ob die Schätzung eingetreten ist, lässt sich derzeit nicht belegen. Branchen wie das Gesundheitswesen, der Finanzsektor, Regierungen und die Automobilindustrie werden voraussichtlich den größten Teil dieser Kosten tragen.

Diese Zahlen weisen auf ein alarmierendes, exponentielles Wachstum hin, das eine systemische wirtschaftliche Bedrohung darstellt. Die Tatsache, dass viele dieser Angriffe über Monate unentdeckt bleiben, ist besonders besorgniserregend. Dies bedeutet, dass Angreifer ausreichend Zeit haben, Daten zu exfiltrieren, Persistenz zu etablieren und maximalen Schaden anzurichten, bevor sie entdeckt werden. Diese Angriffe sind oft „stille Killer“, die langfristige, heimtückische Schäden verursachen, anstatt sofortige, offensichtliche Störungen. Dies erfordert eine Abkehr von der reaktiven Erkennung hin zu einer proaktiven, kontinuierlichen Überwachung und Bewertung. Dass die Angreifer laut ENISA in rund 66 % der analysierten Vorfälle auf den Code der Softwareanbieter zielten und dabei das Vertrauen der Kunden in ihre Lieferanten ausnutzten, unterstreicht, dass genau die Mechanismen, die auf Effizienz ausgelegt sind, als Waffe eingesetzt werden. Dies deutet auf eine grundlegende Verschiebung der Angriffsmethodik von direkten zu indirekten, hebelbasierten Angriffen hin.

Die Evolution der Bedrohung: Zunehmende Angriffe auf Software-Lieferketten

Definition und Auswirkungen von Lieferkettenangriffen

Ein Lieferkettenangriff ist ein Cyberangriff, der darauf abzielt, die Lieferanten einer Organisation zu kompromittieren, um unbefugten Zugriff auf die Systeme oder Daten dieser Organisation zu erhalten. Angreifer nutzen Schwachstellen in den Systemen eines Unternehmens – sei es Software, Hardware oder

Netzwerkverbindungen –, um ein anderes Unternehmen, typischerweise einen Kunden oder Partner, anzugreifen. Dies ermöglicht es ihnen, ein viel größeres Netz auszuwerfen und potenziell mehrere Organisationen gleichzeitig zu betreffen.

Die Auswirkungen solcher Angriffe sind weitreichend und verheerend. Sie reichen von Betriebsunterbrechungen und der Offenlegung sensibler Daten wie Kreditkartendaten, Sozialversicherungsnummern und Gesundheitsinformationen bis hin zu Lecks von geistigem Eigentum und Problemen mit der Systemstabilität und -integrität. Das Opferunternehmen ist typischerweise für Daten haftbar, die aufgrund einer Verletzung des Lieferanten gestohlen wurden, selbst wenn der Verstoß bei einem Drittanbieter seinen Ursprung hatte.

Die Betriebsunterbrechungen können sich auf verschiedene Weisen manifestieren und zu erheblichen Konsequenzen für Organisationen und ihre Kunden führen. Ein Beispiel hierfür ist der groß angelegte Ransomware-Angriff auf Change Healthcare im Jahr 2024, eine medizinische Abrechnungsstelle. Dieser Angriff führte zu massiven Störungen für Gesundheitseinrichtungen, was den Patientenzugang und die operativen Abläufe erheblich beeinträchtigte, da viele Gesundheitsunternehmen keine Zahlungen mehr verarbeiten konnten. Ein solcher Vorfall verdeutlicht, wie ein einziger Ausfall bei einem kritischen Anbieter die Operationen einer ganzen Branche lahmlegen kann. Die Auswirkungen betreffen nicht nur das direkt betroffene Unternehmen, sondern das gesamte Netzwerk von Partnern und Kunden, was zu weit verbreiteter operativer Lähmung, massiven finanziellen Verlusten und schwerwiegenden Reputationsschäden führt.

Neben den direkten finanziellen und operativen Schäden ist das Reputationsrisiko ein weiterer kritischer Aspekt. Ein einziger Fehler eines Lieferanten kann schwerwiegende Folgen für den Ruf und die Glaubwürdigkeit eines Unternehmens haben. In Zeiten von Social Media verbreiten sich schlechte Nachrichten schneller und wirken sich härter aus als je zuvor.

Die rechtlichen Konsequenzen von Lieferkettenangriffen sind ebenfalls erheblich. Organisationen können für Schäden haftbar gemacht werden, selbst wenn die Verletzung bei einem Drittanbieter oder Lieferanten auftrat. Aufsichtsbehörden können Bußgelder und Strafen für die Nichteinhaltung relevanter Cybersicherheitsvorschriften verhängen. Beispielsweise können Bußgelder für die Nichteinhaltung der DSGVO bis zu 20.000.000 € oder 4 % des weltweiten Umsatzes betragen, je nachdem, welcher Betrag höher ist. Der California Consumer Privacy Act (CCPA) sieht ähnliche Gesetze vor, mit Bußgeldern von bis zu 7.500 US-Dollar pro vorsätzlichem Verstoß. Diese erheblichen behördlichen Bußgelder stellen eine doppelte Bestrafung dar, da sie zusätzlich zu den finanziellen Verlusten durch den Angriff selbst anfallen. Dies unterstreicht, dass die Einhaltung von Datenschutzgesetzen keine reine „Checkbox-Übung“ mehr ist, sondern eine kritische Notwendigkeit des Risikomanagements.

Was seit Dezember 2025 gilt: NIS2 und der Cyber Resilience Act

Lieferkettensicherheit war lange eine Frage der Sorgfalt. Seit dem **6. Dezember 2025** ist sie in Deutschland eine Frage des Gesetzes. An diesem Tag trat das NIS-2-Umsetzungsgesetz in Kraft; das BSI rechnet mit **rund 29.500 Einrichtungen**, die künftig direkt seiner Aufsicht unterliegen – zuvor waren es etwa 4.500.

Diese Einrichtungen haben nach Darstellung des BSI drei Pflichten: „Sie sind gesetzlich verpflichtet, sich als NIS-2-Unternehmen zu registrieren, dem BSI erhebliche Sicherheitsvorfälle zu melden und

Risikomanagementmaßnahmen zu implementieren und diese zu dokumentieren.“ Das Registrierungsportal des BSI ist seit dem 6. Januar 2026 freigeschaltet.

Für dieses Thema entscheidend ist die vierte der zehn Risikomanagementmaßnahmen aus **§ 30 Absatz 2 BSIG**. Sie lautet im Wortlaut: „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern.“ Lieferkettensicherheit steht damit nicht in einem Leitfaden, sondern in einem Gesetz – und sie ist zu dokumentieren.

Der Punkt, der den Mittelstand wirklich betrifft

Die meisten mittelständischen IT-Dienstleister werden jetzt nachsehen, ob sie zu den 29.500 gehören, feststellen, dass sie es nicht tun, und weiterarbeiten. Das ist der Fehler.

Das BSI formuliert es unmissverständlich: „Da die Sicherheit in der Lieferkette ein wichtiger Teil der Risikomanagementmaßnahmen ist, sind auch zahlreiche Dienstleister der direkt betroffenen Unternehmen indirekt betroffen.“ Und weiter: „Denn die betroffenen Unternehmen werden die Anforderungen aus dem BSIG an ihre Dienstleister weiterreichen. Dazu kann ebenfalls die nachweisliche Umsetzung der eigenen Risikomanagementmaßnahmen zählen.“

Übersetzt: Die Pflicht kommt nicht über die Aufsichtsbehörde, sie kommt über den Vertrag. Wer regulierte Unternehmen beliefert, wird die Anforderungen erfüllen müssen, ohne je einen Brief vom BSI bekommen zu haben – und wird sie **nachweisen** müssen, nicht nur zusichern.

Der Cyber Resilience Act: erster scharfer Termin am 11. September 2026

Der zweite Rechtsakt trifft die andere Seite: nicht die Betreiber, sondern die Hersteller. Der Cyber Resilience Act, Verordnung (EU) 2024/2847 vom 23. Oktober 2024, gilt für Produkte mit digitalen Elementen – und sein erster scharfer Termin ist der **11. September 2026**.

Ab diesem Tag unterliegen Hersteller vernetzter Produkte der Meldepflicht für Schwachstellen und Vorfälle. Das BSI beschreibt die Fristen so: „Bei aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen mit Auswirkung auf die Sicherheit von Produkten mit digitalen Elementen muss innerhalb von 24 Stunden eine initiale Meldung (Frühwarnung) erfolgen. Innerhalb von 72 Stunden sind weitere Informationen, soweit verfügbar, zu ergänzen.“ Gemeldet wird über eine zentrale Meldeplattform.

24 Stunden. Das ist kein Projektzeitraum, das ist eine Rufbereitschaft. Wer diese Meldung erst dann organisiert, wenn sie fällig wird, reißt die Frist.

Was	Rechtsgrundlage	Gilt seit / ab
NIS-2-Umsetzungsgesetz in Kraft	BSIG	6. Dezember 2025
BSI-Registrierungsportal offen	BSIG	6. Januar 2026
Verfahren für Konformitätsbewertungsstellen	CRA	11. Juni 2026

Was	Rechtsgrundlage	Gilt seit / ab
Meldepflicht der Hersteller (24 h / 72 h)	CRA	11. September 2026
Ausreichende Zahl notifizierter Stellen	CRA	11. Dezember 2026
Alle CRA-Anforderungen	CRA	11. Dezember 2027

Zum 11. Dezember 2027 folgen die grundlegenden Cybersicherheitsanforderungen vor dem Inverkehrbringen, die Schwachstellenbehandlung über den gesamten Lebenszyklus und die Transparenzpflichten gegenüber Nutzern.

Schlüssel-Angriffsvektoren

Kompromittierte Open-Source-Komponente

Die moderne Softwareentwicklung stützt sich stark auf Open-Source-Komponenten und Bibliotheken, um die Entwicklungszeiten zu beschleunigen. Diese Abhängigkeit erweitert jedoch die Angriffsfläche erheblich. Eine einzige kompromittierte Bibliothek kann Schwachstellen in jede Anwendung einschleusen, die sie verwendet, was zu einer weitreichenden und oft unsichtbaren Infektion führt.

Ein prominentes Beispiel hierfür ist die Log4j-Schwachstelle, auch bekannt als Log4Shell. Diese kritische Schwachstelle, die im November 2021 entdeckt wurde, betrifft ein weit verbreitetes Open-Source-Logging-Dienstprogramm in Java-basierten Software-Stacks. Sie ermöglichte Hackern die vollständige Kontrolle über ungepatchte Geräte und bedrohte Millionen von Anwendungen im Internet. Die Schwachstelle ist tief in Software-Lieferketten eingebettet, oft als indirekte Abhängigkeit, was die Erkennung erschwert. Selbst wenn eine Organisation Log4j nicht direkt verwendet, könnte sie über eine andere Anwendung, die Log4j nutzt, anfällig sein. Dies bedeutet, dass das Problem nicht nur die direkte Verwendung anfälliger Software betrifft, sondern auch transitive Abhängigkeiten, die versteckte Risiken schaffen und traditionelle Schwachstellen-Scans unzureichend machen. Die US-amerikanische Heimatschutzbehörde schätzt, dass es mindestens ein Jahrzehnt dauern wird, jede anfällige Instanz von Log4j zu finden und zu beheben.

Die Angreifer selbst nutzen ebenfalls Open-Source-Tools, um ihre Angriffs-Frameworks zu etablieren. Beispiele hierfür sind PoshC2, ein Open-Source-Angriffs-Framework, und Chisel, ein Open-Source-Tunneling-Dienstprogramm. Sie fälschen oft legitime Produkte oder signieren ihre Tools mit gestohlenen Signaturen, um die Erkennung zu umgehen. Dies verwischt die Grenzen zwischen legitimer und bösartiger Aktivität zusätzlich.

Angriffe über Drittanbieter und Managed Service Provider (MSPs)

Angreifer nutzen gezielt die Vertrauensbeziehungen zu Drittanbietern und Managed Service Providern (MSPs), um in Unternehmen einzudringen. MSPs sind aufgrund ihres tiefen Zugriffs auf Kundennetzwerke ein besonders attraktives Ziel. Angreifer nutzen die oft schwächere Sicherheit von MSPs aus, um sich auf die Netzwerke ihrer Kunden auszubreiten. Wenn Anbieter keine robusten Sicherheitsmaßnahmen

durchsetzen, werden ihre Schwachstellen schnell zu denen der Organisation, da Angreifer das schwächste Glied in der Kette ansteuern.

Ein prägnantes Beispiel für diese Art von Angriff ist der Kaseya-Lieferketten-Angriff. Hierbei manipulierte die Ransomware-Gruppe REvil die Software von Kaseya, einer IT-Management-Plattform, um Ransomware in die von der Plattform verwalteten IT-Umgebungen einzuschleusen. Dieser einzelne Plattform-Hack gefährdete über 1.500 Unternehmen. Der Vorfall verdeutlicht drastisch, wie die Kompromittierung eines einzelnen MSPs zu einer weit verbreiteten Ransomware-Bereitstellung in zahlreichen Kundenorganisationen führen kann. Dies unterstreicht, dass die „Achillesferse“ oft außerhalb der direkten Kontrolle des Opfers liegt, was das Management von Drittanbieterrisiken von größter Bedeutung macht.

Sicherheitslücken in CI/CD-Pipelines

Continuous Integration/Continuous Deployment (CI/CD)-Pipelines sind das Herzstück der agilen Softwareentwicklung und automatisieren den Prozess von der Codeerstellung bis zur Bereitstellung. Ihre Komplexität und die hohen Berechtigungen, mit denen sie oft arbeiten, machen sie jedoch zu einem attraktiven Angriffsvektor. Fehlkonfigurationen in CI/CD-Workflows und Source Code Management (SCM)-Plattformen bleiben oft unbemerkt und schaffen Sicherheitslücken.

Häufige Fehlkonfigurationen umfassen übermäßig permissive SCM-Repository-Zugriffe, ungeschützte Geheimnisse (wie API-Schlüssel oder Cloud-Anmeldeinformationen) in CI/CD-Workflows, fehlende Branch-Schutzregeln, übermäßige Runner-Privilegien und uneingeschränkten Artefaktzugriff. Wenn Angreifer diese Schwachstellen ausnutzen, können sie Quellcode kompromittieren, Geheimnisse exfiltrieren, Privilegien eskalieren und Build-Artefakte manipulieren, um Lieferkettenangriffe zu initiieren.

Dies führt zu einem „Automatisierungs-Paradoxon“: Die Geschwindigkeit und Automatisierung von CI/CD, wenn sie falsch konfiguriert ist, kann zu einem Beschleuniger für Angriffe werden, der böartigen Code schnell und weitreichend verbreitet. Die Lösung liegt im „Shift-Left“-Sicherheitsansatz. Hierbei wird Sicherheit frühzeitig in den Entwicklungsprozess integriert, anstatt sie nachträglich hinzuzufügen. Dies bedeutet, dass Sicherheit nicht nur ein Gate am Ende ist, sondern ein kontinuierlicher Bestandteil der automatisierten Pipeline, vom Code-Commit bis zur Bereitstellung.

Die Rolle der KI in modernen Cyberangriffen

KI verschiebt beide Seiten dieses Themas: Sie senkt die Kosten für Täuschung und sie beschleunigt die Ausführung. Beides ist für die Lieferkette relevant, gehört aber ausführlich woanders hin – wie Angreifer KI einsetzen, von Deepfakes bis zu adaptiver Malware, steht in [KI in der Cyberkriminalität](#); wie sich das Geschäftsmodell hinter den Angriffen professionalisiert hat, in [Ransomware 2.0](#).

Für die Lieferkette bleibt der Punkt, der beide verbindet: Der Einstieg erfolgt zunehmend über Menschen und Zugänge bei Dritten, nicht über eine technische Schwachstelle im eigenen Haus.

Aktuelle Statistiken zu Software-Lieferkettenangriffen

- >600% – Anstieg der Angriffe 2021 vs. Vorjahr
- 742% – Anstieg der Angriffe 2019-2022

- **62%** – Betroffene Organisationen laut Anchore-Report 2022
- **46 Mrd. US-Dollar** – Finanzielle Kosten 2023 (weltweit)
- **81 Mrd. US-Dollar** – Prognostizierte finanzielle Kosten 2026

Wenn der Angriff nicht über Code läuft: Coinbase

Wie ein solcher Angriff aussieht, wenn er ohne kompromittierte Komponente auskommt, zeigte Coinbase. Nach einer Erpressermail vom 11. Mai 2025 reichte das Unternehmen am 15. Mai 2025 eine Pflichtmitteilung (Form 8-K) bei der US-Börsenaufsicht ein, mit dem 14. Mai als Berichtsdatum. Angreifer hatten Support-Mitarbeiter bestochen – nicht Angestellte von Coinbase, sondern ausgelagerte Kräfte eines Dienstleisters. Die Erpresser forderten 20 Millionen Dollar; das Unternehmen bezifferte den erwarteten Sanierungsaufwand auf **180 bis 400 Millionen Dollar** (Quelle: Coinbase, Form 8-K bei der SEC, 2025). Betroffen war nach eigener Angabe weniger als ein Prozent der monatlich aktiven Nutzer.

Kein manipuliertes Update, keine Schwachstelle. Der Zugang war legitim – er gehörte nur einem Vertragspartner. Genau diese Beziehung meint § 30 Absatz 2 Nummer 4 BSIG mit „Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern“. Dieselbe Struktur aus der Zugangsperspektive beschreibt der Beitrag zu [Zero Trust](#).

Best Practices für das Management von Drittanbieter-Risiken

Umfassendes Third-Party Risk Management (TPRM)

Ein robustes Third-Party Risk Management (TPRM) ist unerlässlich, um die von externen Anbietern ausgehenden Risiken zu identifizieren, zu bewerten und zu mindern. Dies erfordert einen proaktiven und kontinuierlichen Ansatz, der über einmalige Bewertungen hinausgeht.

Die besten Praktiken für TPRM umfassen:

- **Proaktiver Ansatz:** Organisationen sollten einen nahezu Echtzeit-Einblick in die Sicherheitslage ihrer Lieferanten haben. Dies ermöglicht es Risikomanagern, Änderungen in den Sicherheitsbewertungen anhand etablierter Risikoschwellen zu messen und Neubewertungen durchzuführen, um zu verhindern, dass potenziell inakzeptable Risiken in das Drittanbieter-Ökosystem gelangen. Dies ist entscheidend, da sich die Bedrohungslandschaft ständig weiterentwickelt und eine statische Bewertung schnell veraltet ist.
- **Angepasste Bewertungen:** Bewertungen sollten auf jeden Lieferanten zugeschnitten werden, wobei mehr Zeit und Ressourcen für Lieferanten oder operative Bereiche aufgewendet werden sollten, die ein höheres Risiko darstellen.
- **Gestufte Bewertungsstruktur:** Lieferanten sollten nach dem Grad des Zugriffs auf sensible Daten kategorisiert werden. Dadurch können Risikomanagementteams mehr Zeit für die Bewertung von Hochrisikolieferanten aufwenden und weniger Zeit für solche, die aufgrund ihres Geschäftsszenarios weniger potenziellen Schaden verursachen.

- **Objektiver Kontext für Selbstbewertungen:** Risikomanager sollten Daten aus der kontinuierlichen Überwachung nutzen, um den von Lieferanten ausgefüllten Selbstbewertungen einen objektiven Kontext hinzuzufügen. Dies hilft, die Genauigkeit ihrer Antworten zu bestimmen und festzustellen, ob ihre Selbstbewertung ihre Sicherheitslage wahrheitsgemäß widerspiegelt.
- **Nutzung eines Vendor Security Assessment Frameworks:** Ein solches Framework, das auf dem NIST Cybersecurity Framework basiert, hilft Organisationen, die Cybersicherheitslage, Schwachstellen und Minderungsmaßnahmen von Anbietern zu verstehen. Es umfasst die Bereiche Identifizierung, Schutz, Erkennung und Reaktion.

Die kontinuierliche Überwachung im TPRM umfasst die fortlaufende Bewertung von Drittanbietern und die Überprüfung ihrer Aktivitäten, Leistungen und Compliance-Status. Dies stellt eine Verschiebung von statischen Momentaufnahmen zu einer dynamischen Risikoüberwachung dar, was angesichts der sich ständig ändernden Bedrohungslandschaft von großer Bedeutung ist.

Vertragliche Absicherungen und Compliance-Anforderungen

Verträge sind ein entscheidendes Instrument zur Festlegung der Sicherheitsanforderungen und zur Zuweisung von Verantwortlichkeiten bei der Zusammenarbeit mit Drittanbietern. Sie müssen detaillierte Bestimmungen enthalten, die die Einhaltung von Sicherheitsstandards und Datenschutzvorschriften gewährleisten.

Wichtige vertragliche Sicherheitsklauseln für Drittanbieter-Vereinbarungen umfassen :

- **Standard-Drittanbieter-Vereinbarungsklausel:** Erfordert die vorherige schriftliche Zustimmung der anderen Partei, bevor eine Vereinbarung mit einem Drittanbieter getroffen wird, und stellt sicher, dass diese Vereinbarung den ursprünglichen Bedingungen entspricht.
- **Klausel mit Abtretungsbeschränkung:** Verhindert, dass eine Partei Rechte oder Pflichten ohne vorherige schriftliche Zustimmung an einen Drittanbieter abtritt.
- **Klausel mit Freistellungsverpflichtung:** Stellt sicher, dass die Parteien sich gegenseitig von Ansprüchen oder Schäden freistellen, die sich aus der Leistung oder dem Verhalten des Drittanbieters ergeben.
- **Klausel mit Mitteilungspflicht:** Erfordert eine schriftliche Mitteilung an die andere Partei, bevor eine Vereinbarung mit einem Drittanbieter getroffen wird, einschließlich Details zum Umfang und den Bedingungen.
- **Klausel zur Beschränkung der Rechte Dritter:** Begrenzt die Rechte von Drittanbietern unter der Hauptvereinbarung, es sei denn, dies ist ausdrücklich schriftlich genehmigt.
- **Klausel zur Leistungsüberwachung:** Verpflichtet die Parteien, die Leistung von Drittanbietern zu überwachen und zu überprüfen, um die Einhaltung der vereinbarten Bedingungen sicherzustellen.
- **Klausel zum Vertraulichkeitsschutz:** Erfordert, dass Drittanbieter-Vereinbarungen Bestimmungen zum Schutz vertraulicher Informationen enthalten.
- **Klausel mit Compliance-Anforderungen:** Verlangt, dass jede Drittanbieter-Vereinbarung alle anwendbaren Gesetze, Vorschriften und Industriestandards einhält.

- Klausel mit Genehmigung für Subunternehmer: Erfordert die vorherige schriftliche Zustimmung des Kunden, bevor ein Teil der Arbeit an einen Subunternehmer vergeben wird.
- Klausel mit Recht zur Prüfung: Gewährt den Parteien das Recht, Drittanbieter-Vereinbarungen zu prüfen und zu überprüfen, um die Einhaltung sicherzustellen.

Der Rechtsrahmen dient als erste Verteidigungslinie im Management von Drittanbieter-Risiken. Durch die explizite Aufnahme umfassender Sicherheits- und Compliance-Klauseln können Organisationen Erwartungen rechtlich definieren, Haftung zuweisen und die Einhaltung von Standards durchsetzen. Dies verwandelt rechtliche Vereinbarungen in proaktive Sicherheitsinstrumente, die Unklarheiten reduzieren und im Falle von Verstößen Abhilfe schaffen. Die schiere Anzahl spezifischer Klauseln, die in den Forschungsergebnissen erwähnt werden, unterstreicht die Komplexität und Notwendigkeit eines detaillierten rechtlichen Ansatzes.

Absicherung der eigenen Lieferkette

Sichere Softwareentwicklung (DevSecOps)

DevSecOps ist eine Softwareentwicklungsmethodik, die Sicherheit in jede Phase des Software Development Lifecycle (SDLC) integriert. Im Gegensatz zu traditionellen Ansätzen, bei denen Sicherheit oft erst am Ende des Entwicklungsprozesses berücksichtigt wird, zielt DevSecOps darauf ab, Sicherheitsmaßnahmen von Anfang an einzubetten. Dies wird als „Shift-Left“-Sicherheit bezeichnet und ermöglicht es, Schwachstellen frühzeitig im Entwicklungsprozess zu erkennen und zu beheben, was die Kosten reduziert und die Bereitstellung von Software beschleunigt.

Zu den Schlüsselpraktiken von DevSecOps gehören:

- Automatisierte Sicherheitstests: Der Einsatz von Tools für Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) und Interactive Application Security Testing (IAST) ermöglicht die kontinuierliche Überwachung und Erkennung potenzieller Bedrohungen. SAST-Tools analysieren den Quellcode, um Schwachstellen wie SQL-Injection oder Cross-Site Scripting (XSS) frühzeitig zu finden.
- Kontinuierliche Überwachung: Die Überwachung von Codeänderungen und Systemverhalten in Echtzeit hilft, Probleme frühzeitig zu erkennen und zu beheben.
- Schwachstellenmanagement und Zugriffssteuerung: Implementierung von Maßnahmen zur Identifizierung, Priorisierung und Behebung von Schwachstellen sowie zur Beschränkung des Zugriffs auf sensible Informationen und Ressourcen.
- Sichere Codierungspraktiken: Entwickler müssen in sicheren Codierungspraktiken geschult werden, um die Einführung von Schwachstellen von vornherein zu minimieren.

- **Software Bill of Materials (SBOM):** Die Verwendung von SBOMs, einer umfassenden Bestandsaufnahme aller Softwarekomponenten und Abhängigkeiten, erhöht die Transparenz und hilft, potenzielle Schwachstellen zu identifizieren. Was hier als gute Praxis steht, ist inzwischen vorgeschrieben. Das BSI dazu: „Der CRA erfordert die Erstellung einer SBOM durch die Hersteller mit dem Ziel, dass sie im Schwachstellenhandling genutzt wird. Die SBOM muss nicht veröffentlicht werden.“ Der zweite Satz ist der praktisch wichtigere: Die Sorge, mit einer Stückliste die eigene Architektur offenzulegen, ist der häufigste Einwand gegen SBOMs – und sie geht ins Leere. Erstellt werden muss sie, veröffentlicht nicht.
- **Code-Signierung:** Die digitale Signierung von Anwendungscode und ausführbaren Dateien stellt sicher, dass Änderungen nach der Signierung erkannt werden können, wodurch die Softwareintegrität gewahrt bleibt.

DevSecOps verbessert die Zusammenarbeit zwischen Entwicklungs-, Betriebs- und Sicherheitsteams, was zu einer höheren Effizienz und Produktqualität führt. Der kulturelle Wandel hin zu einer gemeinsamen Verantwortung für Sicherheit ist dabei von grundlegender Bedeutung. Ohne diese Verschiebung der Denkweise bleiben selbst die besten Tools ineffektiv. Dies erfordert ein starkes Engagement der Führungsebene und Investitionen in kontinuierliche Schulungen und Anpassungsfähigkeit.

Implementierung von Zero Trust-Architekturen

Zero Trust ist ein Sicherheitsrahmen, der auf dem Prinzip „niemals vertrauen, immer überprüfen“ basiert. Es eliminiert das implizite Vertrauen, das in traditionellen perimeterbasierten Sicherheitsmodellen angenommen wird, und erfordert eine kontinuierliche Authentifizierung und Autorisierung für jede Zugriffsanfrage, unabhängig davon, ob sie innerhalb oder außerhalb des Netzwerks erfolgt. Dieses Modell ist in modernen, verteilten Umgebungen, die von Remote-Arbeit, Cloud-Diensten und komplexen Bedrohungen geprägt sind, unerlässlich.

Die Kernprinzipien der Zero Trust-Architektur umfassen:

- **Kontinuierliche Verifizierung:** Jede Zugriffsanfrage, sei es von einem Benutzer, einem Gerät oder einer Anwendung, muss streng und kontinuierlich überprüft werden. Dies beinhaltet die Implementierung einer Multi-Faktor-Authentifizierung (MFA), die resistent gegen Phishing-Angriffe ist, wie z. B. Passkeys. Passkeys nutzen Public-Key-Kryptographie und sind domänenspezifisch, was sie extrem phishing-resistent macht. Die Einführung von Passkeys durch große Technologieunternehmen wie Apple, Google und Microsoft markiert einen wichtigen Schritt zur Stärkung der Identität als Sicherheitsanker. Dies bedeutet auch eine Abkehr von weniger sicheren MFA-Methoden wie SMS-OTPs, die anfällig für Abfangen sind.
- **Geringstes Privileg (Least Privilege Access):** Benutzern und Geräten wird nur der absolut notwendige Zugriff gewährt, um ihre Aufgaben zu erfüllen – nicht mehr und nicht weniger. Dies minimiert den potenziellen Schaden im Falle einer Kompromittierung.
- **Mikrosegmentierung:** Das Netzwerk wird in kleinere, isolierte Segmente unterteilt, um die laterale Bewegung von Angreifern zu begrenzen und den „Blast Radius“ eines potenziellen Verstoßes zu minimieren.

- **Kontinuierliche Überwachung und Analysen:** Das System überwacht kontinuierlich das Benutzerverhalten, den Gerätezustand und den Netzwerkverkehr, um Anomalien und potenzielle Bedrohungen in Echtzeit zu erkennen.
- **Annahme einer Kompromittierung (Assume Breach):** Zero Trust geht davon aus, dass Sicherheitsverletzungen unvermeidlich sind. Der Fokus liegt daher darauf, die Auswirkungen einer Kompromittierung zu minimieren.

Die Integration von Zero Trust mit Legacy-Systemen stellt eine Herausforderung dar, da ältere Infrastrukturen oft grundlegende Sicherheitsfunktionen vermissen (z. B. MFA, API-Sicherheitskontrollen, moderne Verschlüsselung) und flache Netzwerkdesigns die Mikrosegmentierung erschweren. Lösungen umfassen den Einsatz von API-Gateways, Identitätsproxy-Diensten und virtuellen Patching-Methoden, um die Sicherheit zu verbessern, ohne den Legacy-Code zu ändern. Auch die Verbesserung der Überwachung durch Netzwerktraffic-Analyse und Log-Aggregation ist entscheidend.

Zero Trust kann auch dazu beitragen, Qualifikationslücken im Cybersicherheitsbereich zu schließen, indem es Sicherheitsmanagement vereinfacht und Aufgaben automatisiert, wodurch die Abhängigkeit von tiefem, spezialisiertem Wissen in jedem Bereich reduziert wird.

Cloud-Native Sicherheitsstrategien

Cloud-Native ist ein Ansatz zur Entwicklung und Bereitstellung skalierbarer Anwendungen, die die vollen Vorteile von Cloud-Umgebungen nutzen. Dies beinhaltet den Einsatz von Containern, Kubernetes, Microservices, unveränderlicher Infrastruktur und deklarativen APIs. Cloud-Native-Anwendungen bieten Vorteile wie eine reduzierte Angriffsfläche, einfachere Bedrohungserkennung und -reaktion sowie verbesserte Compliance.

Wichtige Komponenten und Praktiken umfassen:

- **Containerisierung und Orchestrierung (Kubernetes):** Container verpacken Anwendungen mit all ihren Abhängigkeiten in einer einzigen ausführbaren Einheit, – Bereitstellungen werden damit konsistent, portabel und skalierbar. Kubernetes, als führende Container-Orchestrierungsplattform, automatisiert die Bereitstellung, Skalierung und das Selbst-Healing von containerisierten Anwendungen.
- **Microservices-Architektur:** Anwendungen werden in kleine, unabhängige Dienste zerlegt, die über APIs kommunizieren. Dies fördert Agilität, Ausfallsicherheit und unabhängige Skalierung.
- **Unveränderliche Infrastruktur (Immutable Infrastructure):** Anstatt bestehende Server oder Container zu modifizieren, werden bei Updates neue Instanzen bereitgestellt, die die alte ersetzen. Dies sorgt für Konsistenz, Zuverlässigkeit und verbesserte Sicherheit durch Reduzierung von Konfigurationsabweichungen und vereinfachtes Patching.
- **Infrastructure as Code (IaC):** Die Bereitstellung und Verwaltung der IT-Infrastruktur erfolgt über Code, – das bringt Automatisierung, Konsistenz, weniger Fehler und schnellere Bereitstellungen.
- **Policy as Code (PaC):** Sicherheitsrichtlinien werden als Code definiert, automatisiert, durchgesetzt und verwaltet. Dies gewährleistet konsistente Durchsetzung, Agilität und Compliance-Prüfungen in CI/CD-Pipelines.

- **Observability (Logs, Metriken, Traces):** Bietet tiefe Einblicke in den internen Zustand und die Leistung von Systemen durch die Sammlung und Analyse von Logs (detaillierte Ereignisaufzeichnungen), Metriken (numerische Messungen der Systemgesundheit) und Traces (End-to-End-Karten von Anfragen). Dies ermöglicht proaktive Problemlösung und schnelle Fehlerbehebung.
- **Service Meshes:** Eine dedizierte Infrastrukturschicht, die die Kommunikation zwischen Microservices steuert, Sicherheit (z. B. gegenseitige TLS-Authentifizierung, Zugriffssteuerung), Observability und Traffic-Management bietet, ohne Anwendungsänderungen zu erfordern.
- **Serverless Computing:** Ein Cloud-Native-Entwicklungsmodell, das es Entwicklern ermöglicht, Anwendungen zu erstellen und auszuführen, ohne Server verwalten zu müssen. Der Cloud-Anbieter übernimmt die Bereitstellung, Wartung und Skalierung der Serverinfrastruktur, wodurch Entwickler sich auf den Code konzentrieren können.

Die Cloud-Native-Einführung führt zu einer erheblichen Komplexität, da eine Vielzahl von Microservices, Tools und dynamischen Umgebungen verwaltet werden müssen. Diese Komplexität ist jedoch auch die treibende Kraft hinter Innovationen, insbesondere bei der Integration von KI/ML. Der Schlüssel liegt darin, diese Komplexität durch Standardisierung, Automatisierung (IaC, PaC) und zentralisierte Observability zu managen, anstatt von ihr überwältigt zu werden. Dies erfordert einen kulturellen Wandel hin zu kontinuierlichem Lernen und Anpassung.

Multi-Cloud- und Hybrid-Cloud-Strategien

Eine Multi-Cloud-Strategie bedeutet, Cloud-Computing-Dienste von mindestens zwei Cloud-Anbietern zu nutzen, um Anwendungen auszuführen. Eine Hybrid-Cloud-Strategie hingegen kombiniert eine private Cloud oder On-Premises-Infrastruktur mit einer oder mehreren Public Clouds.

Die wichtigsten Treiber für Multi-Cloud- und Hybrid-Cloud-Strategien sind:

- **Vermeidung von Herstellerbindung (Vendor Lock-in):** Durch die Verteilung von Workloads auf mehrere Anbieter wird die Abhängigkeit von einem einzigen Anbieter reduziert, was Flexibilität und Verhandlungsspielraum erhöht.
- **Erhöhte Zuverlässigkeit und Redundanz:** Die Verteilung von Workloads und Daten auf mehrere Cloud-Umgebungen minimiert das Ausfallrisiko und gewährleistet die Geschäftskontinuität, selbst wenn ein Anbieter ausfällt. Dies ist besonders wichtig für Disaster Recovery und Ransomware-Schutz, da Daten über verschiedene Umgebungen repliziert werden können.
- **Kostenoptimierung:** Organisationen können wettbewerbsfähige Preismodelle verschiedener Anbieter nutzen, um die Gesamtkosten zu senken und Ressourcen effizienter zuzuweisen.
- **Best-of-Breed-Dienste:** Die Möglichkeit, die besten Tools und Funktionen von verschiedenen Anbietern auszuwählen (z. B. Google Cloud für KI/ML, AWS für Rechenleistung, Azure für Unternehmenslösungen), optimiert die Workloads und fördert Innovationen.
- **Compliance und Datenresidenz:** Multi-Cloud-Strategien erleichtern die Einhaltung regionaler Compliance-Anforderungen, indem Daten in spezifischen geografischen Regionen gespeichert werden können.

- **Verbesserte Latenz für globale Zielgruppen:** Durch die Bereitstellung von Diensten näher an den Endbenutzern wird die Latenz reduziert und die Benutzererfahrung verbessert. Edge Computing spielt hierbei eine wichtige Rolle.

Trotz der Vorteile bringen Multi-Cloud-Umgebungen auch Herausforderungen mit sich, darunter die Komplexität des Managements, inkonsistente Sicherheitsrichtlinien, Datenintegration und Netzwerkprobleme sowie Qualifikationslücken.

Zur Minderung dieser Herausforderungen werden folgende Strategien empfohlen:

- **Vereinheitlichte Management-Plattformen („Single Pane of Glass“):** Diese Plattformen bieten eine zentrale Übersicht über alle Cloud-Ressourcen und -Anbieter, was das Management und die Überwachung erheblich vereinfacht.
- **Automatisierung:** Der Einsatz von Infrastructure as Code (IaC) und CI/CD-Pipelines automatisiert Bereitstellungen, Skalierung und Wartung über verschiedene Cloud-Anbieter hinweg.
- **Zero Trust-Sicherheitsansatz:** Gewährleistet, dass jede Zugriffsanfrage überprüft wird, unabhängig von ihrem Ursprung, und schützt Daten und Workloads, die über verschiedene Anbieter verteilt sind.
- **Standardisierung von Daten:** Die Standardisierung von Datenformaten und -modellen über verschiedene Cloud-Plattformen hinweg ist entscheidend für eine reibungslose Datenintegration und -konsistenz.
- **FinOps-Kultur:** Fördert die finanzielle Verantwortung und Optimierung der Cloud-Kosten.

Die strategische Diversifizierung durch Multi-Cloud ist mehr als nur die Nutzung mehrerer Anbieter; es ist ein strategischer Schritt zur Risikostreuung und Vermeidung von Herstellerbindung. Dies ermöglicht Organisationen, „Best-of-Breed“-Dienste von verschiedenen Anbietern auszuwählen, Leistung und Kosten für spezifische Workloads zu optimieren und Disaster Recovery sowie Geschäftskontinuität zu verbessern. Die Implementierung erfordert jedoch ein sorgfältiges Management der inhärenten Komplexität.

Cloud-Kostenoptimierung (FinOps)

Cloud-Kostenoptimierung, auch bekannt als FinOps (Financial Operations), ist eine kulturelle Praxis, die Finanz-, Technologie- und Geschäftsteams zusammenbringt, um Cloud-Ausgaben zu verwalten und den Geschäftswert zu maximieren. Sie ist unerlässlich, da Cloud-Kosten aufgrund von Überprovisionierung, Unterauslastung, unerwarteten Gebühren, mangelnder Transparenz, Shadow IT, Multi-Cloud-Komplexität und Qualifikationslücken schnell außer Kontrolle geraten können.

Die besten Praktiken für FinOps umfassen:

- **Transparenz und Sichtbarkeit:** Eine der größten Herausforderungen ist der Mangel an Transparenz bei den Cloud-Ausgaben. FinOps erfordert eine kontinuierliche Überwachung und detaillierte Kostenanalyse in Echtzeit. Dies beinhaltet das Tagging von Ressourcen nach Kostenstellen oder Projekten, um die Kostenzuordnung zu verbessern. Warnmeldungen bei Kostenüberschreitungen oder ungewöhnlichen Nutzungsmustern sind ebenfalls entscheidend.

- **Ressourcenoptimierung:** Dies ist ein Kernaspekt zur Reduzierung unnötiger Ausgaben.
- **Rightsizing:** Anpassung der Cloud-Ressourcen (z. B. VMs, Speicher) an den tatsächlichen Workload-Bedarf, um Überprovisionierung zu vermeiden.
- **Eliminierung ungenutzter Ressourcen:** Identifizierung und Abschaltung von Leerlauf- oder verwaisten Ressourcen (z. B. ungenutzte Instanzen, Speicher).
- **Auto-Scaling:** Automatische Anpassung der Ressourcen an den Bedarf, um Engpässe zu vermeiden und Kosten zu senken.
- **Nutzung von Rabattmodellen:** Strategischer Einsatz von Reserved Instances (RIs), Savings Plans und Spot Instances für vorhersehbare bzw. unterbrechbare Workloads.
- **Automatisierung:** Automatisierung von Kostenkontrollen, geplanten Abschaltungen und dem Datenlebenszyklus-Management reduziert den manuellen Aufwand und gewährleistet eine kontinuierliche Optimierung.
- **Kollaboration und Kultur:** FinOps fördert die Zusammenarbeit zwischen Finanz-, Engineering- und Produktteams, um Cloud-Ausgaben zu optimieren und den Geschäftswert zu maximieren. Jedes Team sollte die Verantwortung für seine Cloud-Nutzung übernehmen.

FinOps wandelt das Cloud-Kostenmanagement von einem technischen Overhead in einen strategischen Wettbewerbsvorteil um. Durch die Förderung der Zusammenarbeit und die Bereitstellung von Echtzeit-Transparenz können Organisationen datengestützte Entscheidungen treffen, die Ausgaben optimieren und gleichzeitig Innovationen beschleunigen. Diese finanzielle Agilität ermöglicht es Unternehmen, selbstbewusst zu skalieren, ausufernde Kosten zu vermeiden und Einsparungen in strategische Initiativen umzulenken, was direkt zum Geschäftswert und zur Marktreaktionsfähigkeit beiträgt. Dies ist in einem Markt, in dem Cloud-Ausgaben schnell untragbar werden können, von entscheidender Bedeutung.

Fazit und Empfehlungen

Die zunehmende Komplexität und Vernetzung moderner Software-Lieferketten hat diese zu einer primären Angriffsfläche für Cyberkriminelle gemacht. Die Bedrohungen reichen von kompromittierten Open-Source-Komponenten und Drittanbietern bis hin zu hochentwickelten KI-gestützten Angriffen wie Deepfakes und adaptiver Malware. Das rapide Wachstum und die finanziellen Auswirkungen dieser Angriffe, gepaart mit der Industrialisierung der Cyberkriminalität durch RaaS, erfordern einen fundamentalen Wandel in der Sicherheitsstrategie von Organisationen.

Um die eigene Lieferkette effektiv abzusichern und den Herausforderungen der vernetzten Achillesferse zu begegnen, sind folgende Empfehlungen von entscheidender Bedeutung:

- **Priorisierung des Risikomanagements von Drittanbietern:** Organisationen müssen ein umfassendes und kontinuierliches Third-Party Risk Management (TPRM) implementieren. Dies geht über einmalige Bewertungen hinaus und erfordert eine proaktive, nahezu Echtzeit-Überwachung der Sicherheitslage von Lieferanten. Vertragliche Absicherungen mit detaillierten Sicherheits- und Compliance-Klauseln sind unerlässlich, um Verantwortlichkeiten festzulegen und rechtliche Risiken zu minimieren.

- **Integration von Sicherheit in den Entwicklungszyklus (DevSecOps):** Sicherheit darf kein nachträglicher Gedanke sein. Die Einführung von DevSecOps-Prinzipien, die Sicherheit von Anfang an in CI/CD-Pipelines integrieren, ist entscheidend. Dies beinhaltet automatisierte Sicherheitstests (SAST, DAST), die Nutzung von SBOMs für Transparenz und die Implementierung sicherer Codierungspraktiken, um Schwachstellen frühzeitig zu erkennen und zu beheben. Ein kultureller Wandel hin zu einer gemeinsamen Sicherheitsverantwortung ist hierfür die Grundlage.
- **Einführung von Zero Trust-Architekturen:** Das Prinzip „niemals vertrauen, immer überprüfen“ muss in der gesamten IT-Infrastruktur verankert werden. Dies bedeutet die Implementierung kontinuierlicher Verifizierung für jeden Benutzer und jedes Gerät, die Anwendung des Prinzips des geringsten Privilegs und die Nutzung von Mikrosegmentierung. Die Einführung phishing-resistenter Authentifizierungsmethoden wie Passkeys ist dabei ein wichtiger Schritt, um die Identität als robusten Sicherheitsanker zu etablieren.
- **Strategische Nutzung von Cloud-Technologien:** Cloud-Native-Architekturen mit Containern, Microservices und unveränderlicher Infrastruktur ermöglichen Agilität, Skalierbarkeit und Resilienz. Multi-Cloud- und Hybrid-Cloud-Strategien bieten die Möglichkeit, Herstellerbindung zu vermeiden, die Zuverlässigkeit zu erhöhen und „Best-of-Breed“-Dienste zu nutzen. Die Komplexität dieser Umgebungen muss durch Automatisierung (IaC, PaC) und zentralisierte Management-Plattformen beherrscht werden.
- **Etablierung von FinOps:** Um die Vorteile der Cloud voll auszuschöpfen und gleichzeitig die Kosten zu kontrollieren, ist die Implementierung einer FinOps-Kultur unerlässlich. Dies fördert die finanzielle Verantwortung über alle Teams hinweg, verbessert die Transparenz der Cloud-Ausgaben und ermöglicht eine kontinuierliche Optimierung der Ressourcen durch Rightsizing, Automatisierung und die Nutzung von Rabattmodellen.
- **Kontinuierliche Schulung und Bewusstseinsbildung:** Der menschliche Faktor bleibt eine kritische Schwachstelle. Regelmäßige, realistische Schulungen zu Phishing, Social Engineering und den neuesten Bedrohungen sind unerlässlich, um die Mitarbeiter als erste Verteidigungslinie zu stärken. Dies muss durch eine Kultur des kontinuierlichen Lernens und der Anpassung an die sich ständig weiterentwickelnde Bedrohungslandschaft ergänzt werden.

Die Absicherung der Lieferkette ist keine einmalige Aufgabe, sondern ein fortlaufender Prozess, der eine übergreifende Strategie, technologische Innovation und einen tiefgreifenden kulturellen Wandel erfordert. Nur durch die proaktive Stärkung jedes Glieds in der Kette kann die „vernetzte Achillesferse“ in eine Quelle der Stärke und Resilienz verwandelt werden.

Ihr nächster Schritt

Ob Sie unter NIS2 fallen, entscheidet ein Blick ins Gesetz. Ob Ihre Auftraggeber die Anforderungen an Sie weiterreichen, entscheidet sich im nächsten Rahmenvertrag – und zwar unabhängig davon. Wir prüfen mit Ihnen, welche Nachweise Sie führen müssen und welche Sie heute schon führen könnten, und verankern sie in [Cloud-Governance und Compliance](#) – mit deutschsprachigen Senior-Teams und Steuerung in Deutschland.

Häufige Fragen

Was ist ein Lieferkettenangriff?

Ein Angriff, der nicht direkt auf das Zielunternehmen zielt, sondern auf einen seiner Lieferanten, Dienstleister oder auf eine genutzte Software-Komponente. Über dieses kompromittierte Glied verschaffen sich Angreifer Zugang – oft über ein vertrauenswürdiges Software-Update, dem das Ziel arglos vertraut.

Warum sind Open-Source-Komponenten ein besonderes Risiko?

Weil moderne Software zu großen Teilen aus fremden Bausteinen besteht, deren Schwachstellen man erbt. Die Log4Shell-Schwachstelle in der weit verbreiteten Java-Bibliothek Log4j (CVE-2021-44228, Dezember 2021) zeigte das drastisch: eine einzige Komponente, Millionen betroffener Anwendungen. Ohne Überblick über die eigenen Abhängigkeiten bleibt dieses Risiko blind.

Was schützt die eigene Lieferkette?

Ein Bündel aus Disziplinen: sichere Entwicklung nach dem Shift-Left-Prinzip mit automatisierten Tests und einer Software Bill of Materials (SBOM), eine Zero-Trust-Architektur (niemals vertrauen, immer prüfen), phishing-resistente Authentifizierung wie Passkeys und ein kontinuierliches Risikomanagement für alle Drittanbieter.

Warum sind Managed Service Provider (MSPs) ein bevorzugtes Angriffsziel?

MSPs haben tiefen Zugriff auf die Netzwerke vieler Kunden gleichzeitig. Wer einen MSP kompromittiert, erreicht über dessen Vertrauensbeziehungen zahlreiche Unternehmen auf einmal. Der Kaseya-Angriff ist das prägnante Beispiel: Die Ransomware-Gruppe REvil manipulierte die IT-Management-Software, um Ransomware in die verwalteten Kundenumgebungen auszurollen.

Wo liegen die Risiken in CI/CD-Pipelines?

CI/CD-Pipelines automatisieren den Weg von der Codeerstellung bis zur Bereitstellung und arbeiten mit hohen Berechtigungen. Typische Schwachstellen sind zu permissive Repository-Zugriffe, ungeschützte Geheimnisse wie API-Schlüssel in Workflows, fehlende Branch-Schutzregeln und übermäßige Runner-Privilegien. Falsch konfiguriert wird die Automatisierung zum Beschleuniger für Angriffe – das Automatisierungs-Paradoxon.

Wie verändert KI die Angriffe auf Lieferketten?

Generative KI macht täuschend echte Deepfakes einfach herstellbar und ermöglicht hochpersonalisierte Social-Engineering-Angriffe; adaptive Malware passt ihr Verhalten an, und Ransomware-as-a-Service senkt die Einstiegshürde für Angreifer. Für die Lieferkette zählt vor allem, dass der Einstieg damit häufiger über Menschen und Zugänge bei Dritten läuft als über eine technische Schwachstelle.

Was gehört zu einem wirksamen Third-Party Risk Management (TPRM)?

Ein umfassendes TPRM bewertet Lieferanten und Dienstleister kontinuierlich statt einmalig beim Onboarding, sichert Anforderungen vertraglich ab und prüft Compliance-Nachweise. Ergänzt wird es durch DevSecOps mit einer Software Bill of Materials für die eigene Lieferkette, Zero-Trust-Architektur und phishing-resistente Authentifizierung.

Thematische Vertiefungen

[Cybersecurity-Expertise](#)[Zero Trust](#)[Ransomware 2.0](#)

Quellen

- BSI: Cybersicherheitsrecht – NIS-2-Umsetzungsgesetz ab morgen in Kraft, Pressemitteilung vom 5. Dezember 2025. Belegt: Inkrafttreten am 6. Dezember 2025, rund 29.500 beaufsichtigte Einrichtungen (zuvor etwa 4.500), die drei Pflichten Registrierung, Meldung und Risikomanagement, Registrierungsportal ab 6. Januar 2026. – https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251205_NIS-2-Umsetzungsgesetz_in_Kraft.html
- BSI: #nis2know – NIS-2-Risikomanagementmaßnahmen. Belegt den Wortlaut der vierten Maßnahme aus § 30 Absatz 2 BSIG, die Zahl von ca. 29.500 direkt verpflichteten Unternehmen sowie die indirekte Betroffenheit der Dienstleister und die vertragliche Weitergabe der Anforderungen. – <https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Risikomanagementmassnahmen/NIS-2-Risikomanagementmassnahmen.html>
- BSI: Cyber Resilience Act. Belegt die Termine 11. Juni 2026, 11. September 2026 (Meldepflicht der Hersteller), 11. Dezember 2026 und 11. Dezember 2027, die Fristen von 24 und 72 Stunden sowie den Satz „Die SBOM muss nicht veröffentlicht werden“. – https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html
- Verordnung (EU) 2024/2847 (Cyber Resilience Act) vom 23. Oktober 2024, im Amtsblatt verkündet am 20. November 2024. – <https://eur-lex.europa.eu/eli/reg/2024/2847/oj?locale=de>
- Coinbase Global, Inc.: Pflichtmitteilung Form 8-K, bei der SEC eingereicht am 15. Mai 2025 (Berichtsdatum 14. Mai 2025). Belegt Bestechung von Support-Mitarbeitern eines Drittdienstleisters, 20 Mio. USD Lösegeldforderung, 180 bis 400 Mio. USD erwarteter Sanierungsaufwand, weniger als 1 % der monatlich aktiven Nutzer betroffen. – <https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=0001679788&type=8-K&dateb=&owner=include&count=40>
- CISA: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities (AA21-356A) – <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a>
- NIST SP 800-218: Secure Software Development Framework (SSDF) – <https://csrc.nist.gov/News/2022/nist-publishes-sp-800-218-ssdf-v11>
- Sonatype: 8th Annual State of the Software Supply Chain Report (2022) – +742 % Angriffe 2019–2022 – <https://www.sonatype.com/press-releases/2022-software-supply-chain-report>
- ENISA: Threat Landscape for Supply Chain Attacks (2021) – ~66 % der Vorfälle zielten auf Anbieter-Code – <https://enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks>

- **Anchore: 2022 Software Supply Chain Security Report (62 % betroffene Organisationen)** – <https://anchore.com/press/anchore-continues-expansion-into-software-supply-chain-security-market/>
- **BlueVoyant: Global Third-Party Cyber Risk Study 2021 (93 % erlitten Breach über die Lieferkette)** – <https://www.prnewswire.com/news-releases/bluevoyant-research-reveals-rise-in-supply-chain-cybersecurity-breaches-as-firms-struggle-to-effectively-monitor-third-party-cyber-risk-301397733.html>
- **Juniper Research (via Cybersecurity Dive, 2023): Kosten von Software-Lieferkettenangriffen ~46 Mrd. USD 2023 → ~81 Mrd. USD 2026** – <https://www.cybersecuritydive.com/news/software-supply-chain-attacks/650148/>