Wie sich Lieferketten vor Angriffen schützen lassen

SUPPLY CHAIN SECURITY

Supply-Chain-Angriffe sind eine akute Bedrohung für jedes Unternehmen. Einen Softwarelieferanten auszunutzen, um eine große Anzahl seiner Kunden zu erreichen, ist eine ausgeklügelte und erfolgreiche Methode der derzeit agierenden Hacker. Die Spezialisierung der Unternehmen auf ihre Kernkompetenzen, die Globalisierung der Lieferketten (Supply Chain), sowie die Digitalisierung entlang der Wertschöpfungskette sind nur einige Beispiele, wieso Angreifer vermehrt die Vertrauensbeziehung zwischen Kunden und Lieferanten für Angriffe ausnutzen. Dieser Artikel erläutert Cyberangriffe in Bezug auf eine Supply Chain und zeigt Sicherheitsmechanismen für die erfolgreiche Verteidigung.

Seit vielen Jahren ist ein deutlicher Anstieg der digitalen Vernetzung zwischen Kunden und Lieferanten erkennbar. Genau diese stetig zunehmende Vernetzung von Soft- und Hardwarebereitstellung im B2B Bereich ist sehr attraktiv für Hacker. Anstatt jede Organisation einzeln anzugreifen, wird die Organisation am Beginn der Supply Chain attackiert. So kann beispielsweise ein einziges infiziertes IT-System alle damit verknüpften Organisationen, IT-Systeme und Prozesse infizieren. Diese Attraktivität spiegelt sich in der Anzahl der Cyberangriffe auf Supply Chains wider. Bei einem Supply-Chain- oder Lieferketten-Angriff ist die prinzipielle Idee, dass ein vertrauenswürdiger Dienst (Software), der seit längerer Zeit bei einer Organisation/einem Unternehmen in Einsatz ist, irgendwann für einen Angriff verwendet wird. Hierfür missbraucht der Angreifer beispielsweise ein legitimiertes Software-Update, das der vertrauenswürdige Softwarehersteller zur Verfügung stellt, um Organisationen/Unternehmen anzugreifen (Angriffsvektor).

Um diesen Angriff durchführen zu können, dringt der Angreifer zuerst in das IT-System des Dienstleisters (Supplier) – dem vertrauenswürdigen Softwarehersteller – ein und infiltriert zum Beispiel das Software-Update mit Malware. Dieser Angriff wird in der Regel als Advanced Persistent Threat (APT) – mehrstufiger Angriff auf die IT-Infrastruktur von Unternehmen – durchgeführt. Voraussetzung für die weiteren Schritte des Angriffs ist, dass dieser Vorgang unbemerkt bleibt. Von daher muss er an einer bestimmten Prozessstelle umgesetzt werden. Nur so lässt sich sicherstellen, dass das manipulierte Software-Update offiziell als Hersteller-Update digital signiert und somit als autorisierter Code vom Kunden akzeptiert und eingespielt wird. Darauf basierend kann in einem zweiten Schritt, der Angreifer die Software des Herstellers bei mehreren Tausend Organisationen gleichzeitig nutzen, um die eigentlichen Angriffe umsetzen.

Während 2020 insgesamt 694 Organisationen betroffen waren, stieg die Zahl der betroffenen Organisation im Jahr 2021 allein durch einen einzigen erfolgreichen Angriff auf über 1.500 Organisationen an. Dabei wurde über ein Update eines Software-Produkts, welches von zahlreichen Unternehmen und Organisationen genutzt wurde, verheerender Schaden angerichtet. Zuvor hatten Hacker eine Schwachstelle bei einem international tätigen IT-Dienstleister entdeckt und ausgenutzt. Bei den kompromittierten Organisationen wurden sämtliche Rechner verschlüsselt und der durchschnittliche Schaden pro betroffener Organisation belief sich auf ungefähr 6,1 Millionen US-Dollar.

Um diesem enormen Schaden zu entgehen, reicht es für die Unternehmen nicht aus, sich beim Thema Cybersicherheit auf ihre Lieferanten oder Kunden zu verlassen. Jeder Teilnehmer der Wertschöpfungskette ist selbst dafür verantwortlich, dass die Schnittstellen zu seinen Kunden und den Lieferanten technischen und organisatorischen Anforderungen der Cybersicherheit und des Risikomanagements genügen.

SUPPLY CHAIN IM SINNE DER CYBERSICHERHEIT

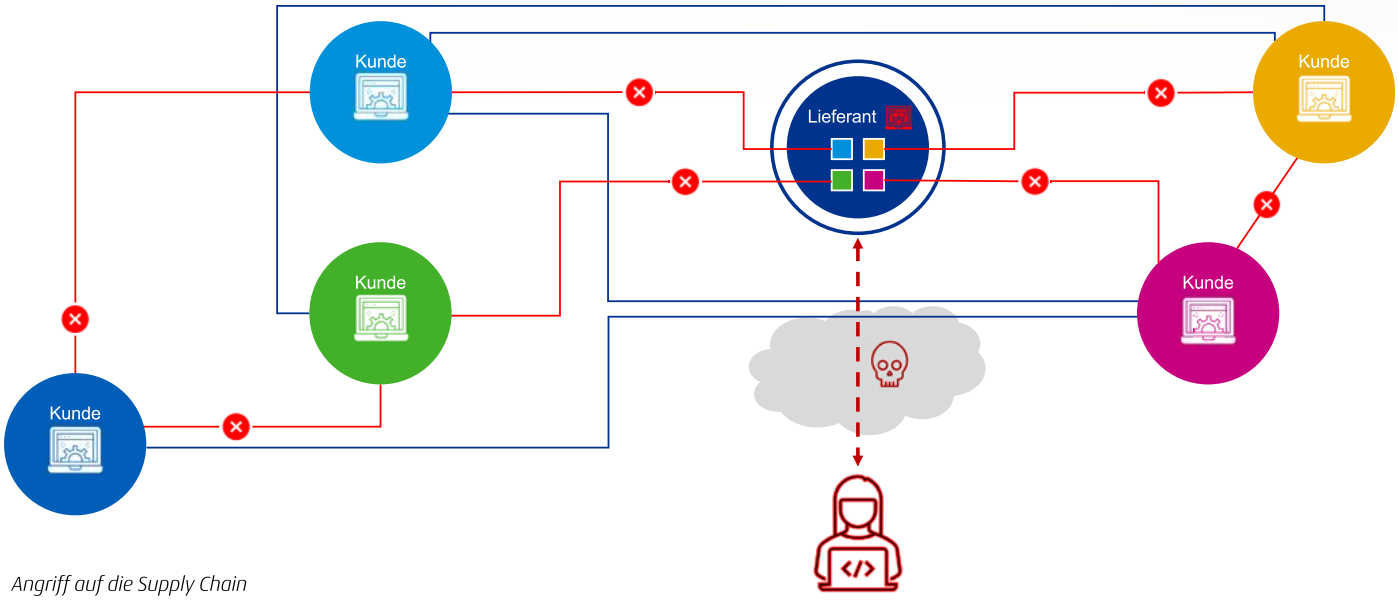
Was genau ist eigentlich eine Supply Chain? Eine Supply Chain umfasst zum Beispiel ein breites Spektrum an Ressourcen, bestehend aus Hardware und Software, Speicher (Cloud oder lokal), Vertriebsmechanismen (Webanwendungen, Onlineshops) und Verwaltungssoftware. Sie kann in unterschiedlichen Größenordnungen und Umfängen existieren. Kleine Mittelständler sowie Konzerne können ein Teil einer Supply Chain sein, sowohl als Kunde als auch als Lieferant oder sogar beides. Im Sinne der Cybersicherheit besteht eine Supply Chain aus den vier Kernelementen: Lieferant, Assets des Lieferanten, Kunde und Assets des Kunden.[1]

- ***Lieferant***
  Ein Unternehmen, das ein Produkt oder eine Dienstleistung für eine andere Organisation bereitstellt.

- ***Assets des Lieferanten***
  Wertvolle Elemente, die der Lieferant zur Herstellung des Produkts oder der Dienstleistung verwendet.

- ***Kunde***
  Eine Organisation, die das vom Lieferanten produzierte Produkt oder die Dienstleistung konsumiert.

- ***Assets des Kunden***
  Wertvolle Elemente, die sich im Besitz des Kunden befinden. Dies kann eine Einzelperson, eine



Angriff auf die Supply Chain

Gruppe von Personen oder eine Organisation sein. Bei den Vermögenswerten kann es sich um Personen, Software, Dokumente, Finanzmittel, Hardware oder andere Werte handeln.

Wie schon erwähnt, kostet es die Angreifer weniger, eine einzelne Organisation anzugreifen und die Supply Chain für sich arbeiten zu lassen, als jeden Kunden dieser Organisation einzeln anzugreifen. Die Angreifer können die Daten von mehreren Kunden der Organisation in einem Angriff erbeuten. So gibt es zum Beispiel Unternehmen A, die Cloud-Lösungen verkaufen, auf denen andere Unternehmen B ihre Software hosten. Für die Hacker ist es nun einfacher, Unternehmen A anzugreifen und durch die Verbindung ohne großen Aufwand an die Daten von Unternehmen B zu gelangen. Aufgrund der exponentiellen Verteilung der Supply Chains, bieten Angriffe auf Supply Chains eine attraktive Grundlage für Angreifer, verhältnismäßig kostengünstig eine hohe Reichweite und einen hohen Schaden zu erzielen. Folglich sollten Organisationen zu ihrer eigenen Sicherheit, in ihre Cybersicherheit investieren. Dies beginnt damit, die Vorgehensweise bei Angriffen auf die Supply Chain zu kennen und zu verstehen. Als weiteres muss die Organisation verstehen, welche Sicherheitsmaßnahmen diesen Angriffen entgegenwirken können.

Hier kommt die Supply Chain Security ins Spiel. Die Supply Chain Security befasst sich mit Maßnahmen und Konzepten zur Prozessabsicherung und Risikominimierung bei solchen Wertschöpfungsketten und hebt die Angriffssicherheit in den Fokus.

KUNDE/LIEFERANT-BEZIEHUNG

Für den Aufbau einer adäquaten Cybersicherheit ist es wichtig zu verstehen, dass Kunden sich nicht ausschließlich auf die Sicherheit der Lieferanten verlassen können – vielmehr sind sie selbst für ihre Sicherheit verantwortlich. Dabei kann mit Vorsichtsmaßnahmen zur Prävention von Angriffen über den Lieferanten begonnen werden, um Angriffen über die Supply Chain entgegenzuwirken. Jede von Lieferanten bezogene Hard- und Software und/oder Dienstleistung muss durch den Kunden auf ihr Risiko für die Cybersicherheit überprüft werden. Jeder Kunde ist selbst dafür verantwortlich festzustellen, ob ihre Lieferanten und deren Produkte und/oder Dienstleistungen als vertrauenswürdig eingestuft und die regulatorischen Anforderungen der Cybersicherheit und des Risikomanagements eingehalten werden. Dazu ist es wichtig, die Erfassung der Risiken durch eine Kooperation mit einem Lieferanten einzurichten. Zudem sollte mit diesem vorher festgelegt werden, welche Sicherheitsmaßnahmen und Regelungen während der Kooperation einzuhalten sind und welche Verpflichtungen für den Lieferanten entstehen.[2]

ANGRIFFE AUF SUPPLY CHAINS

Wogegen sollen sich Unternehmen nun genau schützen? Für die Antwort ist es essenziell zu verstehen, wie Angriffe auf Supply Chains ablaufen und welche Formen solcher Angriffe existieren. Dazu ist der erste Schritt, die Ziele und Angriffswege eines Angriffs zu ermitteln. Hierbei wird zwischen den Angriffsvektoren und -zielen auf Lieferanten und Kunden unterschieden. Bei den Lieferanten werden bei einem Supply-Chain-Angriff die Angriffsvektoren eines „gewöhnlichen" Cyberangriffs genutzt. Die Kunden werden anschließend in einem Folgeangriff über die Infrastruktur des Lieferanten attackiert. Es kann außerdem vorkommen, dass mehr als eine Angriffsart verwendet wird. In vielen Fällen wissen die Unternehmen und Kunden nicht, wie sich die Angreifer Zugang zu ihrer Infrastruktur verschafft haben und was die Ziele waren. Häufig werden diese Informationen von den Organisationen nicht weitergegeben oder nicht ordnungsgemäß gemeldet. In Tabelle 1 sind die häufigsten Angriffswege und Angriffsziele dargestellt.

Die Vektoren der Angriffe können variieren. So ist es möglich, dass zum Beispiel nach einem Social-Engineering-Angriff auf den Lieferanten eine Malware in der Software vom Kunden als Folgeangriff heruntergeladen wird. Somit werden sowohl Malware-Infektion als auch Trusted Relationship als Angriffsmethoden beim Kunden angewandt.

Um sich gegen Angriffe zu wappnen, ist es für Unternehmen essenziell zu verstehen, welche Angriffsvektoren und -ziele ein potenzieller Hacker hat. Wie in der Tabelle zu sehen ist, können die Ziele von Personendaten über den Code bis hin zur kompletten Software gehen. Ein Hacker kann folglich alles, was elektronisch verarbeitet und gespeichert wird, als Ziel haben. Zudem gibt es verschiedenste Arten von Angriffen, sowohl auf Lieferanten- als auch auf Kundenseite.

Somit kann ein Lieferant beispielsweise von einer Malware infiziert oder durch eine Schwachstelle in der Konfiguration angegriffen werden. Aber auch Angriffe, die auf menschliches Fehlverhalten oder Social Engineering abzielen, sind äußerst gefährlich und führen sehr häufig zu einem erfolgreichen Eindringen in die betroffenen Systeme.

	Lieferant	Kunde
Angriffsvektoren	▪ Malware-Infektion ▪ Social Engineering ▪ Brute-Force-Angriff ▪ Ausnutzung von Schwachstellen in der Software ▪ Ausnutzung von Schwachstellen in der Konfiguration ▪ Open-Source Intelligence	▪ Trusted Relationship ▪ Drive-by Compromise ▪ Phishing ▪ Malware-Infektion ▪ Physische Angriffe oder Manipulation ▪ Fälschung
Angriffsziele	▪ Daten ▪ Bereits existierende Software ▪ Softwarebibliotheken ▪ Code ▪ Konfigurationen ▪ Prozesse ▪ Hardware ▪ Personen	▪ Daten ▪ Persönliche Daten ▪ Software ▪ Prozesse ▪ Bandbreite ▪ Finanzen ▪ Personen

Tabelle 1: Supply-Chain-Attacken: Angriffswege und -ziele

Kunden hingegen werden meistens durch einen Trusted-Relationship-Angriff attackiert; Organisationen gewähren ihren Lieferanten häufig einen erweiterten Zugang sowie weitreichende Berechtigungen, um ihnen die Verwaltung interner Systeme oder cloudbasierter Umgebungen zu ermöglichen. Dieser Zugang kann jedoch von Angreifern kompromittiert und missbraucht werden. Auch Software-Updates, welche von Kunden der Softwarelieferanten heruntergeladen werden, können mit Schadsoftware zur Kompromittierung der Kunden versehen werden. Klassische Angriffsvektoren wie Phishing- oder Malware-Infektionen kommen ebenfalls häufig zum Einsatz.

Das Vorgehensmodell der beiden Angriffe, also dem Erstangriff auf den Lieferanten und den Folgeangriff auf den Kunden, folgt häufig einem vergleichbaren, siebenstufigen Ablauf (siehe Tabelle 2).

Bei Lieferanten wird häufig bereits existierende Software kompromittiert. Darunter fällt sämtliche Software von Drittanbietern, die der Lieferant verwendet, wie zum Beispiel Anwendungen, Webserver oder Firmware. Informationen über den Lieferanten, Werte von Sensoren, Zertifikate und persönliche Daten von Kunden oder vom Lieferanten sind ebenfalls gefährdet und somit besonders schützenswert. Weitere beliebte Ziele von Cyberangriffen auf Lieferanten können sein: Konfigurationen (Passwörter, URLs, Firewall Rules etc.), Softwarebibliotheken, Prozesse, Hardware, Personen mit Zugriff auf Daten des Unternehmens oder auch Quellcodes. Der Haupttunterschied zu klassischen Cyberangriffen ist, dass ein erfolgreicher Angriff auf einen Lieferanten das Schadenspotenzial exponentiell steigert.

Das Haupt- und Endziel der Angreifer und somit der Grund eines Supply-Chain-Angriffs sind in der Regel die Assets der Kunden. Diese Assets können je nach Branche und Art der angebotenen Dienstleistung variieren. Bestimmte Assets könnten von den Angreifern direkt ins Visier genommen worden sein, während andere unbeabsichtigt betroffen sein könnten. Es ist außerdem möglich, dass der Kunde das Ziel des Angreifers nicht kennt, weil der Angriff zum Beispiel erfolglos war oder schnell entdeckt wurde.

Mögliche Assets des Kunden sind ebenfalls persönliche Daten oder Geld. Hacker sperren den Computer und erpressen ihre Opfer für eine Lösegeldsumme oder zielen direkt auf Quellcodes und Prozesse ab.

Phase	Lieferantenangriff	Kundenangriff
Reconnaissance	▪ Ermittlung der relevanten Lieferanten und deren Schwachstellen ▪ Definition von Angriffsvektoren und Angriffszielen bei Lieferanten und Kunden ▪ Erstellung eines Angriffsplans	▪ Evaluierung von Angriffsvektoren und Angriffszielen beim Kunden ▪ Anpassung von Angriffsvektoren und/oder Angriffszielen, falls notwendig
Weaponize	▪ Bereitstellung von benötigten Werkzeugen und Informationen für den Lieferanten- und Kundenangriff	▪ Anpassung der Cyberwaffe gemäß den Anpassungen in der Reconnaissance-Phase
Deliver	▪ Einschleusung der Cyberwaffe in das System des Lieferanten	▪ Einschleusung der Cyberwaffe in das System des Kunden unter Ausnutzung der Malware im System des Lieferanten
Exploit	▪ Ausnutzung der Schwachstelle im System des Lieferanten ▪ Installation der Malware	▪ Ausnutzung der Schwachstelle im System des Kunden ▪ Installation der Malware
Control	▪ Aufbau eines Befehls- und Kontrollkanals zum Angreifer ▪ Ausbreitung der Infektion	▪ Aufbau eines Befehls- und Kontrollkanals zum Angreifer ▪ Ausbreitung der Infektion
Execute	▪ Die Vorbereitung ist abgeschlossen, und der Angriff kann durchgeführt werden.	▪ Ausführung des Angriffs auf den Kunden zum Erreichen des Ziels
Maintain	▪ Der Zugang zum Lieferanten soll erhalten bleiben, bis das Ziel beim Kunden erfolgreich erreicht wurde.	▪ Erhaltung des Zugangs zum Kunden (langfristig oder bis zum Erreichen des Ziels)

Tabelle 2: Phasen des Angriffs

WIE SICH ORGANISATIONEN GEGEN SOLCHE CYBERANGRIFFE SCHÜTZEN KÖNNEN

Je besser Kunden vor Cyberangriffen geschützt sind, desto mehr rückt die Aufmerksamkeit der Angreifer auf die Zulieferer. Ein Interessenkonflikt entsteht, wenn Kunden von den Lieferanten eine hohe Cybersicherheit erwarten und gleichzeitig nicht bereit sind, entsprechend kalkulierte Produktpreise zu akzeptieren.

Die Lieferanten müssen bereits bei der Softwareentwicklung gewährleisten, dass ihre eigene Software frei von Schwachstellen und Malware ist, um eine Infektion ihrer Kunden durch die eigene Software zu vermeiden. Dazu müssen neben der Gewährleistung einer sicheren Entwicklungsumgebung vor Verwendung die verwendete Drittanbieter-Software und -bibliotheken überprüft werden. Weiterhin müssen sämtliche Veränderungen an der Software dokumentiert und kontinuierlich überwacht werden. Bei der Herausgabe der Software an Kunden sollten schließlich die Integrität und Echtheit durch Prüfsummen und Signaturen gewährleistet werden, um eine nachträgliche Manipulation durch Angreifer leichter erkennen zu können.

Werden bei einem Supply-Chain-Angriff die Kunden eines Lieferanten in einem Folgeangriff über die Infrastruktur des Lieferanten angegriffen, können die üblichen Schutzmaßnahmen unzureichend sein. Dementsprechend müssen bei einer Lieferanten-Kunden-Beziehung weitere Vorsichtsmaßnahmen zur Prävention von Angriffen über den Lieferanten vorgenommen werden.

Im Folgenden werden wesentliche Handlungsmaßnahmen und Methoden erläutert, wie ein

genereller Schutz erreicht werden kann. Die Maßnahmen beinhalten sowohl technische als auch organisatorische Maßnahmen mit Fokus auf Third-Party-Management. Selbstverständlich ist diese Liste nicht vollständig und die Maßnahmen sollten auch nicht isoliert voneinander betrachtet werden. Vielmehr erhöht erst das Zusammenspiel zwischen technischen und organisatorischen Maßnahmen unter Einbindung der Lieferanten den Sicherheitsgrad des Unternehmens.

Schutz fängt immer mit Transparenz an – nur Bekanntes lässt sich schützen. Jedem Unternehmen sollten seine Verbindungen zu anderen Unternehmen bewusst sein. Die Verbindung muss nicht nur bekannt, sondern auch aus Risikosicht bewertet sein. Das bedeutet, dass bewertet wird, wie kritisch die Dienstleistung/das Produkt oder Ähnliches für das eigene Unternehmen ist. Die Kritikalität steigt beispielsweise, wenn der Lieferant nicht schnell ersetzt werden kann oder er über ein hohes Maß an weitreichenden Zugriffsberechtigungen auf die eigene Infrastruktur verfügt. Im nächsten Schritt muss für die als kritisch erkannten Lieferanten ein Mindestmaß von Anforderungen an die Cybersicherheit definiert werden. Dieses Mindestmaß sollte nicht von den eigenen Mindestanforderungen abweichen, da ansonsten mögliche Hintertüren offenbleiben.

Wichtig ist, dass die gemeinsamen Maßnahmen, Standards, Übungen etc. von Anfang an in den Verträgen und SLAs enthalten sind, sodass sich jederzeit darauf berufen werden kann.

Der Schutz sollte – ebenso wie die Angriffsmöglichkeiten – breit gefächert sein. Viele Organisationen denken zuerst an technische Maßnahmen, doch der Schutz beginnt bereits mit einem kontinuierlich und in Echtzeit geführten Asset-Management. Zudem ist es wichtig, ein Identity- und Access-Management sowie ein Patch-Management zu pflegen. Des Weiteren sollten die Mitarbeiter über das Thema aufgeklärt, geschult und sensibilisiert werden. Für den Fall der Fälle sollte jede Organisation ein klar definiertes und abgestimmtes Notfallmanagement haben.

Auf technischer Ebene ist es beispielsweise möglich, verschiedene Teilnetze in einer Organisation durch Gateways logisch zu segmentieren, um kritische Daten besonders zu schützen und die Ausbreitung von Angriffen einzuschränken. Gateways können einen Angriff aus einem anderen Teilnetz blockieren und somit weitere Kompromittierungen verhindern.

Das Aufrechterhalten des Vertrauens zwischen Lieferanten und Kunden in einer Supply Chain ist unverzichtbar [2]. Im Sinne der Cybersicherheit kann das Vertrauen zu den Lieferanten dagegen von Angreifern ausgenutzt werden, um über den Weg des Lieferanten einen Angriff auszuführen. Aus diesem Grund sollte der Datenzugriff von Lieferanten auf die Daten der Kunden nur in limitierter Form erlaubt werden. Weiterhin sollte die Beziehung zum Lieferanten und vor allem der Datenaustausch sowie die Kommunikation mit diesem geregelt und geschützt werden (siehe auch [3]).

Organisationen sollten zudem ein Konzept zur Zusammenarbeit mit ihren Lieferanten und Kunden erarbeiten, indem eine Risikobewertung, Rollen und Verantwortlichkeiten sowie notwendige Sicherheitsmaßnahmen und Anforderungen vereinbart werden. Folglich sollten Kunden und Lieferanten nur den absolut nötigsten Zugriff bekommen. Hier hilft die möglichst genaue Zeichnung der Bedrohungslandschaft für die Partnerunternehmen.

RESUMÉE

Bevor von einem Lieferanten Software bezogen oder diesem Zugriff auf die Infrastruktur der eigenen Organisation gewährt wird, sollte erst einmal dessen Rahmenwerk für die Cybersicherheit betrachtet und Awareness geschaffen werden.

Der Schutz vor Supply-Chain-Angriffen aufgrund der zunehmenden Vernetzung und den dadurch entstehenden Abhängigkeiten der Organisationen untereinander wird somit immer wichtiger. Bei einem erfolgreichen Angriff ist nicht nur das eigene Unternehmen gefährdet, sondern auch Kundenunternehmen. Dies kann zu enormen Kosten und zum Verlust von Ansehen und Vertrauen der Kunden in den Lieferanten führen.

Um einen einwandfreien Regelbetrieb gewährleisten zu können, müssen Handlungsempfehlungen und Maßnahmen auf jeden Fall berücksichtigt und nicht aufgrund von Ressourcenersparnissen oder Zeitdruck ausgelassen werden. Hierbei muss jedoch für jedes Unternehmen individuell entschieden werden, welche Maßnahmen umgesetzt werden sollen, um einen effektiven Schutz leisten zu können. ■

Literatur

[1] *European Union Agency for Cybersecurity (ENISA): „Threat Landscape for Supply Chain Attacks", 2021*

[2] *U. Coester, N. Pohlmann: „Mit Vertrauenswürdigkeit in eine sichere Zukunft – Warum im Cyber-Raum ein technisches Pendant zur menschlichen Empathie nötig ist", IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 6/2021*

[3] *N. Pohlmann: „Cybersicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cybersicherheitssystemen in der Digitalisierung", 2. Auflage, Springer Vieweg Verlag, Wiesbaden 2022*

JÜRGEN CHRISTL
studierte Informatik an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen seiner Abschlussarbeit mit Supply Chain Security.

NORBERT POHLMANN,
Informatikprofessor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit - TeleTrusT und im Vorstand des Internetverbandes - eco.

ANDRZEJ WOZNICZKA
ist Senior Manager Cyber Security bei der KPMG AG Wirtschaftsprüfungsgesellschaft und hat die Abschlussarbeit von Herrn Jürgen Christl mit betreut