Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Cloud Supply Chain Security

Leitfaden für Schutzmaßnahmen

2023

Danksagung

Diese Publikation wurde in der TeleTrusT-Arbeitsgruppe "Cloud Security" erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung sowie für die aktive Mitgestaltung dieses Positionspapieres.

Projektleitung
Oliver Dehning, Leiter der TeleTrusT-AG "Cloud Security"

Autorenliste (Auszug)

Buck, Konrad - asvin
Cink, Stefan - Net at Work
Demand, Marion - BSI
Dubbel, Sascha - Lacework
Geißler, Yvonne - eperi
Gora, Stefan - secorvo
Graf, Stefan - TÜV Rheinland
Hartmann, Florian - CrowdStrike
Lawicki, Tomasz - Capgemini
Miether, Raphael - BSI
Oppelland, Vincent - DCSO
Pache, Thomas - Aon
Probst, Dr. Christian - RMTP
Rost, Peter - secunet
Schubert, Jonas - M&H
Schütz, Anna Katharina - esatus
Siebert, Gunnar - Aon
Sinnwell, Thomas - consistec

Redaktion

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Mühlbauer, Dr. Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)

In dieser Publikation werden zahlreiche Anglizismen verwendet, da sie sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Des Weiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
https://www.teletrust.de

Inhalt

Zusammenfassung

Supply-Chain-Attacken haben in letzter Zeit deutlich zugenommen und betreffen auch bekannte Anbieter. Die Attacken erfolgen über vertrauenswürdig eingestufte Komponenten und IT-Services Dritter und sind daher von Anwendern schwer zu verhindern.

In der IT ist die Supply Chain die Lieferkette aller Teilprodukte und Lieferungen, aus denen sich ein IT-Service oder eine Anwendung zusammensetzt. Für jede Art von Software, aber insbesondere für Cloud-Dienste, besteht eine solche Lieferkette aus unzähligen Lieferanten und Produkten, die entweder direkt oder indirekt genutzt werden, oder zur Erstellung oder Ausführung der Teile beitragen. Im besten Fall wird der Produzent oder Anbieter der Teile die direkt genutzten Komponenten selbst auf Sicherheitseigenschaften überprüfen. Der Anwender hat aber normalerweise weder die Möglichkeit, die Nutzung einer betroffenen Komponente festzustellen, noch auf eine Behebung von Schwachstellen hinzuwirken - ein inakzeptabler Zustand. Um das Problem der mangelnden Transparenz zu lösen, führt der Weg über die Software Bill of Materials (SBOM). Eine SBOM ist eine Aufstellung aller Komponenten, die in einer Software-Anwendung enthalten sind. Wenn neue Erkenntnisse zu Fehlern und Schwachstellen in diesen Komponenten auftauchen, können Anwender schnell ermitteln, ob sie möglicherweise betroffen sind und die von ihnen genutzten Anwendungen gefährdet sind. Es wird erwartet, dass sich die Bereitstellung von SBOMs durch Lieferanten und Betreiber von Software und Services zum Marktstandard entwickelt.

Der Leitfaden beschreibt neben SBOMs noch weitere Schutzmaßnahmen, die von Anwenderunternehmen zur Verbesserung der Cloud Supply Chain Security getroffen werden können.

Summary

Supply chain attacks have increased significantly and also affect well-known providers. The attacks are carried out via trusted third-party components and IT services and are therefore difficult for users to prevent. In IT, the supply chain is the supply chain of all sub-products and deliveries that make up an IT service or application. For any type of software, but especially for cloud services, such a supply chain consists of countless suppliers and products that are either used directly or indirectly, or contribute to the creation or execution of the parts. In the best case scenario, the producer or supplier of the parts will check the directly used components for security properties themselves. However, the user usually has neither the possibility to determine the use of an affected component nor to work towards the elimination of vulnerabilities - an unacceptable situation. It is difficult for users to assess risks in the supply chain, and usually impossible for small and medium-sized companies. Users therefore rely on risk assessments and protective measures from providers without being able to assess and understand these in detail or even come to their own current assessment. As a result, they are almost completely dependent on the provider in the event of attacks.

The way to solve the problem of a lack of transparency is via a software bill of materials (SBOM). An SBOM is a list of all components contained in a software application. It thus creates transparency with regard to the software components used in an application. When applied to other elements of the supply chain (i.e. extended to hardware, cloud services, etc.), the concept allows complete transparency of all components used. If new findings emerge regarding errors and gaps in these components, users can quickly determine whether they are potentially affected and whether the applications they are using are at risk. If necessary, they can then take their own measures or decide not to use them temporarily. However, the static provision of SBOMs, for example at the time the contract is concluded, is not sufficient. Instead, providers need to provide this information dynamically. This means that this information must be up-to-date at all times, even after updates. Providers must also receive up-to-date information on the components they use and pass it on to their users. This type of provision of SBOMs does not yet exist. Approaches exist, but are incompatible with each other in parts.

Users can make a significant contribution to improving security in the supply chain if they include the provision of SBOMs by providers in their catalog of requirements. For their part, providers should make this information available to their users. The transparency gained will enable providers and users to actively manage cyber security rather than just reacting to incidents.

This guide describes protective measures that user companies can take to improve IT security despite a lack of transparency and the inability to directly influence elements of the supply chain. It also contains a suggestion on how transparency about the supply chain and the elements used can be improved, even when using cloud services.

1 Einleitung und Motivation

Supply Chain Attacken sind in letzter Zeit verstärkt in den Fokus geraten. Im Dezember 2020 sorgte eine Attacke auf das Network Management System Orion des Anbieters SolarWinds für Aufmerksamkeit. Die Attacke wurde als Teil eines Updates von SolarWinds eigenen Servern verbreitet, unter Nutzung eines validen Zertifikats. Leidtragende der Attacke waren Zehntausende von Organisationen, darunter viele Managed Service Provider und deren Kunden.

Eine weitere prominente Attacke betraf Kaseya, Anbieter für IT-Management-Lösungen, die ebenfalls von vielen Systemhäusern und MSPs bei Kunden eingesetzt werden. Kaseya meldete den Angriff Anfang Juli 2021. Schätzungen gehen von ca. 800 bis 1.500 betroffenen Unternehmen aus, bei denen durch die Attacke Ransomware aktiviert wurde.

Die Angriffe auf SolarWinds und Kaseya sind prominente, aber bei Weitem nicht die einzigen Beispiele für Supply Chain Attacken in jüngerer Zeit. Auch der Log4J Exploit, der Ende 2021 publik wurde, macht die Verwundbarkeit der IT über die Supply Chain deutlich. Ein weiteres Beispiel ist eine Attacke auf die 3CX Desktop App aus dem Frühjahr 2023, bei der über eine Kette von DLLs Malware auf betroffene Systeme geladen wurde.

Laut dem 2022 Annual Data Breach Report[1] waren im Jahr 2022 deutlich mehr Menschen von Angriffen auf die Lieferkette betroffen als von direkten Angriffen per Malware. Die zunehmende Zahl von Supply-Chain-Angriffen ist eine logische Konsequenz der zunehmenden Nutzung von Cloud Services. Da Supply-Chain-Angriffe nicht direkt die eigene IT-Infrastruktur von Unternehmen attackieren, sondern über als vertrauenswürdig eingestufte IT-Services Dritter eingeschleust werden, sind übliche Schutzmaßnahmen der Anwenderunternehmen gegen diese Attacken oft wirkungslos.

Der vorliegende Leitfaden beschreibt Schutzmaßnahmen, die Anwenderunternehmen ergreifen können, um trotz mangelnder Transparenz und mangelnden direkten Einflussmöglichkeiten auf die Elemente der Supply Chain die IT-Sicherheit zu verbessern. Er enthält außerdem einen Vorschlag, wie die Transparenz über die Supply Chain und die verwendeten Elemente auch bei Nutzung von Cloud Services verbessert werden kann.

[1] Identity Theft Resource Center: 2022 Annual Data Breach; www.idtheftcenter.org, January 2023

2 Definition: Cloud Supply Chain

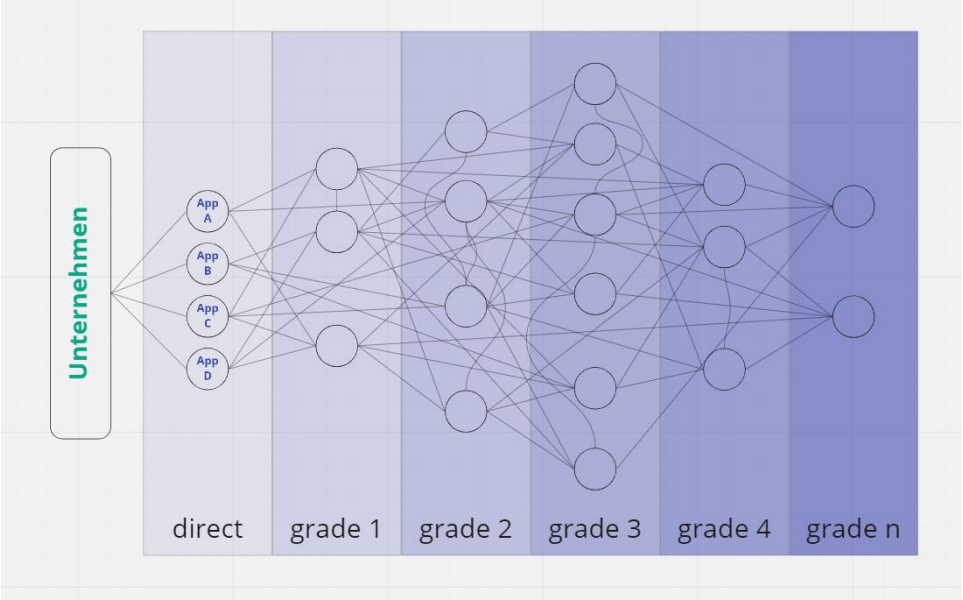

Abbildung 1: Schematische Darstellung von Abhängigkeiten in der Supply Chain

Generell beschreibt der Ausdruck Supply Chain die Lieferkette aller Teilprodukte und Lieferungen, die zu weiteren Teilprodukten und damit dem endgültigen Produkt beitragen. Für jede Art von Software, aber insbesondere für Cloud-Dienste besteht eine solche Lieferkette aus unzähligen Lieferanten und Produkten, die entweder direkt oder indirekt in dem Dienst genutzt werden, oder zur Erstellung oder Ausführung der Teile beitragen.

Die Liste der zur Cloud Supply Chain beitragenden Produkte reicht so von der eingesetzten Hardware über Betriebssysteme und Software-Komponenten des eigentlichen Dienstes, über Software und Komponenten, die direkt (Bibliotheken) oder indirekt (Datenbanken oder andere Cloud Dienste) eingebunden werden, bis zu Software und Komponenten, die wiederum zu diesen beitragen. In der Grafik (Abbildung 1) sind die von einem Unternehmen direkt genutzten Dienste von einer Anzahl Komponenten abhängig, die wiederum von anderen Komponenten abhängig sind und so weiter. Es ist hierbei häufig der Fall, dass dieselbe Komponente in verschiedenen Versionen genutzt wird.

Im besten Fall wird der Produzent oder Anbieter einer solchen Komponente die direkt genutzten Komponenten selbst auf Sicherheitseigenschaften überprüfen. Eine solche Überprüfung sollte auch umfassen, ob der Anbieter der Komponente selbst solche Überprüfungen vornimmt und regelmäßig über Sicherheitslücken informiert (und diese dann auch behebt). Häufig werden Komponenten allerdings vorwiegend nach funktionalen Anforderungen ausgewählt und Sicherheit spielt höchstens eine Nebenrolle.

Die große Verflechtung von Abhängigkeiten in einer typischen Cloud Supply Chain bedeutet auch, dass es lange dauern kann, bis eine gefundene Sicherheitslücke in allen Komponenten behoben ist - im schlimmsten Fall erst nachdem sie ausgenutzt wurde. Der Anwender hat hier normalerweise weder die Möglichkeit, die Nutzung der betroffenen Komponente festzustellen, noch auf eine Behebung der Schwachstelle hinzuwirken - ein inakzeptabler Zustand.

3 Elemente der Cloud Supply Chain

Nachfolgend werden Elemente der Cloud Supply Chain aufgeführt und beschrieben.

3.1 Infrastruktur

Auch wenn für das nutzende Unternehmen der jeweilige Cloud-Dienst im Vordergrund steht, muss dieser natürlich auf einer Maschine ausgeführt werden. Zu der hierzu notwendigen Infrastruktur gehört zunächst ein Rechenzentrum (Data Center), das üblicherweise eine große Anzahl von Servern und Speicherkapazität beherbergt. Die Server und Datenspeicher in Rechenzentren sind intern mit Netzwerkkomponenten verbunden und kommunizieren über einen oder mehrere Anschlüsse mit dem Internet.

Diese Infrastruktur wird von einem Rechenzentrumsbetreiber bereitgestellt und gewartet, der auch selbst Cloud-Dienste bereitstellen kann, aber meist insbesondere die Rechen- und Speicherkapazität weiterverkauft. Der Betreiber hat in der Regel direkten Zugriff auf die Infrastrukturkomponenten und damit auf die in der Infrastruktur von Nutzern gespeicherten oder verarbeiteten Daten. Das gilt naturgemäß gleichermaßen für Dritte, die sich unberechtigt Zugang zu Komponenten dieser Infrastruktur verschaffen. Jede Schwachstelle in der Infrastruktur wirkt sich dadurch direkt auf die Sicherheit der, diese Infrastruktur nutzenden, Services oder Anwendungen aus. Einige Beispiele hierfür sind:

- Hardware interne Schwachstellen (z.B. Spectre / Meltdown)
- Schwachstellen in der Firmware (z.B. SolarWinds)
- Physische Vektoren (z.B. physischer Zugriff auf die Geräte)
- Versorgungs- und Betriebsvektoren (z.B. Stromversorgung, Kühlung, Brandschutz).

Die Bedeutung der physischen Sicherheit hat z.B. der Großbrand im Rechenzentrum von OVH in Straßburg gezeigt, durch den insgesamt 3,6 Millionen Webseiten auf mehr als 460.000 Domains offline gewesen sein sollen.

3.2 Systemsoftware

Die Infrastruktur in Rechenzentren stellt die Plattform für die Ausführung von Diensten bereit. Im Unterschied zu üblichen Arbeitsplatzrechnern werden hier aber auf jedem Server eine Vielzahl von virtuellen Maschinen ausgeführt.

Auf der reinen Hardware läuft hierzu ein Betriebssystem, das Host OS. Dieses Betriebssystem führt eine Virtualisierungsschicht aus, die die Verwaltung der virtuellen Maschinen ermöglicht, also das Anlegen neuer virtueller Maschinen, das Starten und Stoppen und Verschieben virtueller Maschinen zwischen Hostsystemen und auch das Löschen virtueller Maschinen. In jeder virtuellen Maschine wird ein weiteres Betriebssystem ausgeführt (Gast OS).

Eine der Virtualisierung ähnliche Konfiguration ist die Nutzung sog. "Container" (Docker, Kubernetes, LXC oder Ähnliches). Container sind Softwarepakete, die alle notwendigen Elemente enthalten, um in jeder Umgebung ausgeführt werden zu können. Auf diese Weise virtualisieren Container das Betriebssystem. Die große Problematik bei diesen Containern ist, dass oft nicht nachvollzogen werden kann, welche Komponenten innerhalb des Containers verwendet werden. Die Angriffsfläche des Host-Systems (z.B. Docker Host oder Kubernetes Cluster) erweitert sich um die Schwachstellen der im Container verwendeten Komponenten.

Während Virtualisierung große Vorteile in Hinblick auf Flexibilität bietet, stellt es auch wesentliche Risiken für die Sicherheit dar. Host OS und Virtualisierungsschicht haben prinzipiell Zugriff auf die Daten des Gast OS, sowohl über die ebenfalls virtualisierten Speichermedien als auch über den Netzwerkverkehr. Das Gast OS muss, ebenso wie Host OS und Virtualisierungsschicht, so konfiguriert werden, dass unautorisierte Zugriffe verhindert und Sicherheitslücken zeitnah geschlossen werden.

3.3 Eingebundener Software-Code

Praktisch alle aus der Cloud angebotenen Dienste nutzen breit verfügbare Software-Bibliotheken. Oft sind diese Bibliotheken Open Source und werden von der Open Source Community entwickelt und gepflegt. Diese Bibliotheken nutzen wiederum andere Bibliotheken, so dass sich ein tiefes Netz von Abhängigkeiten ergibt. Durch die weite

Verbreitung mancher Bibliotheken wirken sich Fehler sehr breit aus. Software Dritter wird oft eingebunden, ohne Reflektion der Risiken durch die Einbindung dieser Software. Dadurch gerät auch deutlich fehlerhafte, schlecht geschriebene oder schlecht gewartete Software in Produktionssysteme, ohne dass Betreiber oder Nutzer sich dessen bewusst sind.

Es besteht auch die Gefahr, dass Software-Bibliotheken vorsätzlich manipuliert werden, um über gezielt eingebrachte Schwachstellen ("Hintertüren") später Zugriff auf die Bibliothek nutzende Anwendungen und Dienste zu erlangen. Die Log4J-Schwachstelle, die 2022 entdeckt wurde, zeigt die Problematik dieser vermaschten Abhängigkeiten sehr gut auf. Eine einzelne Schwachstelle in einer weit verbreiteten Softwarekomponente betraf plötzlich weltweit viele Services und es war sehr schwer festzustellen, ob eine eingesetzte Software betroffen war oder nicht.

3.4 Sicherheitssoftware

Oberhalb des Betriebssystems - oder auch eingebunden in das Betriebssystem - wird auch bei Cloud-Anbietern zum zusätzlichen Schutz der Kundendaten weitere Sicherheitssoftware wie AV- und EDR-Produkte und weitere Tools eingesetzt. Diese werden vom Cloud Provider ausgesucht und genutzt, der Kunde sollte aber generell sicherstellen, dass die Systeme nach dem aktuellen Stand der Technik auch geschützt werden.

Diese Sicherheitssoftware kann je nach Produkt tief in das Betriebssystem eingreifen und auf der einen Seite Angriffe erkennen, könnte aber ggf. auch zur Änderung von Daten oder gar dem Löschen von Daten genutzt werden. Hierzu gab es auch jüngst Tests von Sicherheitsforschern, die es geschafft haben, EDR-Software als Schadsoftware zu nutzen und Dateien auf Systemen zu löschen.[2]

Zusätzlich bringen diese Produkte für den Endgeräteschutz sowie auch andere Sicherheitssoftware der Cloud-Anbieter weitere Funktionen mit, von Erkennungen von Fehlkonfigurationen bis hin zu virtuellen Firewalls, die in das System eingreifen und ggf. Änderungen an Verbindungen zulassen. Auch die oben erwähnte Kategorie der EDR-Produkte bietet Funktionen zum Remote Zugriff an, die je nach Anbieter zum Systemvollzugriff genutzt werden könnten.

Es steht außer Frage, dass Sicherheitssoftware wie moderner Endgeräteschutz oder auch NG-Firewalls und mehr im eigenen Unternehmen und auch bei den Cloud-Anbietern zum Einsatz kommen müssen um die eigenen Daten im Unternehmen, aber auch die bei Cloud-Anbietern gelagerten Daten zu schützen. Unternehmen sollten sich jedoch bewusst sein, dass diese oft im Betriebssystem verankerten Produkte höhere Berechtigungen haben und somit unter Umständen auch zu Bedrohungen in Form von Zugriffen Externer oder Datenveränderung oder gar Verlust führen könnten.

Ein zusätzlicher Ansatz bei eingesetzten Cloud Applikationen ist die konsequente Nutzung von Verschlüsselung der Daten während des Transports (Encryption at Transit, zum Beispiel TLS-Verschlüsselung, HTTPS) und auch die Verschlüsselung der Daten auf virtuellen Festplatten, eingebundenen Datenbanken und weiteren Speichermöglichkeiten bei der Speicherung (Encryption at Rest).

Vorzugsweise sollte die Verschlüsselung mit eigenen Zertifikaten erfolgen, um so die Daten auch vor dem Betreiber des Cloud-Dienstes und eventuell eingebundenen weiteren Dienstleistern (Third-party Subprocessors) zu schützen.

3.5 Cloud Subservices / Cloud APIs

Wie bei jeder Software basieren auch Cloud Services auf dem Prinzip, dass einzelne Dienste oder Komponenten miteinander kommunizieren müssen. Dieser Datenaustausch funktioniert über APIs (Application Programming Interface). Je nach Aufbau können Daten von einer API geholt oder an eine API übergeben werden. Die Bedienoberfläche (UI), über die der Benutzer Einstellungen oder Daten an die jeweilige App übergibt, ist ein offensichtliches Beispiel für den Austausch von Daten, sofern eine Client/Server-Architektur oder Webseiten für den Zugriff genutzt werden. Die Bedienoberfläche holt Daten von der API und zeigt sie dem Benutzer an. Änderungen werden dann wiederum von der Bedienoberfläche über die API an die App übergeben.

Bei der Betrachtung von Risiken und Bedrohungen muss zunächst unterschieden werden, ob eine API nur von anderen Programmkomponenten erreicht werden kann oder ob auch ein Netzwerkzugriff möglich ist. Die Angriffsfläche

[2] Siehe https://i.blackhat.com/EU-22/Wednesday-Briefings/EU-22-Yair-Aikido-Turning-EDRs-to-Malicious-Wipers.pdf

bei Netzwerk-APIs ist um ein Vielfaches höher und bedarf daher besonderer Absicherungsmaßnahmen.

Eine der wichtigsten Absicherungsmaßnahmen von APIs ist die Zugriffskontrolle. Zunächst muss definiert sein, wer sich mit der API verbinden darf (Authentifizierung). Die Authentifizierung kann beispielsweise anhand von IP-Adressen, Benutzername/Kennwort oder Zertifikaten erfolgen. Wenn die aufrufende Komponente sich authentifiziert hat, muss die API wissen, welche Rechte der Benutzer hat (Autorisierung). Das sogenannte Accounting rundet die Absicherungsmaßnahmen ab. Hierbei geht es um das Nutzungsverhalten, das Accounting beantwortet die Frage, welche Daten während der Sitzung verarbeitet wurden, welche Ressourcen wie stark beansprucht wurden, etc.

Gerade in Cloud-Applikationen, die naturgemäß von sehr vielen unterschiedlichen Benutzern genutzt werden und häufig in Tenants unterteilt sind, ist die Gefahr groß, dass bei den gerade beschriebenen Maßnahmen Fehler entstehen. So kann es dann dazu kommen, dass Daten fälschlicherweise an nicht autorisierte Benutzer ausgeliefert werden.

Eine weitere häufig vorkommende Form der Kompromittierung von APIs sind DDos Attacken. Dabei versucht der Angreifer die API durch eine schiere Menge von Anfragen auszubremsen bzw. vollständig lahm zu legen. Die API ist bei einer erfolgreichen DDos Attacke für reguläre Benutzer nicht mehr zu verwenden.

Ein anderer Angriff sind sogenannte Buffer Overflows, die zwei Dinge zum Ziel haben: Entweder stürzt die API ab oder aber es erfolgt ein unkontrollierter Datenaustausch. Bei einem Buffer Overflow schickt der Angreifer bewusst zu große Datenpakete an die API. Wenn diese damit nicht adäquat umgehen kann, kommt es unter anderem zu den beschriebenen Fehlerzuständen.

Auch Subservices können das Ziel von Angriffen sein. Bei einem SaaS-Angebot wird von einem Subservice gesprochen, wenn von dem Angebot weitere Dienste, die außerhalb des Cloud-Angebotes gehostet werden, in Anspruch genommen werden.

Ein Beispiel für einen Angriff über einen solchen Subservice ist der Angriff, der im Dezember 2021 durch die amerikanische Presse ging. Ein vom Personalmanagement-Unternehmen Kronos beauftragtes Rechenzentrum, das zur Erfüllung des Dienstes "Kronos Private Cloud" benötigt wird, wurde hierbei von einer Ransomware Gruppe angegriffen. Es wurden bei dem Angriff eine größere Menge an Kundendaten entwendet und verschlüsselt.

Bei einem IaaS-Angebot bauen oft Cloud-Anwender eigene Dienste für ihre eigenen Kunden auf. Wenn dieser Dienst wieder Schnittstellen zu weiteren externen Ressourcen oder Diensten hat, können diese auch wieder als Subservice bezeichnet werden. Wenn hierbei über die Schnittstelle oder das Angebot Gefahren entstehen, die nicht nur für den Kunden selbst, sondern auch für andere Kunden relevant sind, dann kann auch das als Supply-Chain-Angriff definiert werden.

3.6 Cloud Anwendungssoftware (SaaS)

Aus der Cloud bezogene Anwendungssoftware (Software as a Service, SaaS) beschreibt Software, die von einem Betreiber auf dessen Systemen und in dessen Rechenzentren für Kunden betrieben wird (Abweichend kann die Bereitstellung durch den Betreiber auch mittels gemieteter Systeme, möglicherweise betrieben in Rechenzentren Dritter oder seinerseits auf einer Cloud-Plattform (IaaS) erfolgen). Die Nutzung erfolgt über das Internet, meist mit auf dem Client betriebenen Web-Browsern oder speziellen, vom Anbieter bereitgestellten Apps.

In der Software verarbeitete Daten geraten damit in den Zugriff des Betreibers und aller Dritten, die möglicherweise berechtigt oder unberechtigt Zugriff auf die zum Betrieb genutzten Systeme haben. Daraus entstehende Risiken umfassen unberechtigten Zugriff auf Daten sowie unberechtigte Veränderung und unberechtigte Löschung von Daten. Auch ist der Nutzer bei der Verfügbarkeit von Anwendung und darin gespeicherten Daten vom Betreiber abhängig, d.h. Risiken des Betreibers (z.B. zeitweiser Ausfall oder gar Verlust der Systeme, Insolvenzrisiko, etc.) schlagen auf den Nutzer durch.

Ein weiteres Risiko entsteht auf Client-Seite durch ggf. vom Betreiber gelieferte, auf dem Client betriebene Software-Komponenten (z.B. Java-Script Code, Apps), die Schadcode enthalten können.

3.7 Cloud Security Services

Bei Cloud Security Services (Security as a Service, SECaaS) werden Teile der IT-Sicherheit oder die IT-Sicherheit als Ganzes an einen Betreiber ausgelagert, der seine Dienste mit eigenen Systemen über das Internet bereitstellt. Beispiele für solche Dienste sind E-Mail-Gateways in der Cloud, Cloud VPN, Cloud Firewall oder Security Operation Center (SOC) as a Service.

Auch immer mehr Sicherheitssoftware wie Endpunktschutz werden als reiner Cloud Service oder als vollständig gemanagter Service angeboten. Diese Lösungen arbeiten mit Audit-Berechtigungen auf Cloud API-Ebene, mit Agenten zur Gewinnung von sicherheitsrelevanter Telemetrie und können gerade im Bereich EDR weitreichenden Zugriff auf die Systeme der Kunden erfordern.

Diese Dienste haben beim Kunden naturgemäß eine hohe Vertrauensstellung und verfügen entsprechend regelmäßig über erweiterte Rechte. Angriffe, die über solche Services ausgeführt werden oder Schadcode, der darüber ausgeliefert wird, haben daher schnell breite Auswirkungen auf Kundensysteme. Wie bei anderen Cloud-Diensten ist der Nutzer bei der Verfügbarkeit vom Betreiber abhängig, d.h. Risiken des Betreibers (z.B. Ausfall der Systeme, Insolvenzrisiko, etc.) schlagen auf den Nutzer durch.

3.8 Client Platform / Browser

SaaS-Anwendungen nutzen häufig den auf dem Client-System installierten Webbrowser als Interface zum Endnutzer. Auch in vielen Mobile Apps ist ein Webbrowser integriert, der zur Interaktion mit der serverseitigen Anwendung genutzt wird.

Da der Webbrowser auf dem lokalen Client läuft und dort dynamisch Daten der serverseitigen Anwendung anzeigt oder auch lokal Programmelemente ausführt, wird der Webbrowser zum neuralgischen Punkt der Cloud-Lieferkette. Sicherheitslücken im Webbrowser, insbesondere solche, die das Ausbrechen einer Cloudanwendung aus der Browserumgebung ermöglichen, können von Schadcode in der Cloudanwendung genutzt werden, um Zugriff auf das lokale System des Nutzers zu erhalten - mit allen Rechten des lokalen Benutzers.

4 Schutzmaßnahmen

4.1 Provider Assessment

In einem sich ständig weiter entwickelnden organisatorischen und technischen Umfeld wird es zunehmend wichtiger, vor und auch während einer Zusammenarbeit mit einem Cloud-Anbieter eine Einschätzung dazu zu erhalten, inwieweit der Anbieter bestimmte Standards oder auch Kundenanforderungen in der IT- und Informationssicherheit einhält.

Die Notwendigkeit der Steuerung und damit der (regelmäßigen) Überprüfung von Cloud-Anbietern kann sich aus regulatorischen Anforderungen ergeben - hier insbesondere DORA für den Finanzbereich von der BaFin, Cyber Resilience Act (ENISA) als auch NIS 2.0 - z.B. im Banken- und Versicherungsbereich oder im Bereich Kritischer Infrastrukturen, muss aber auch im Übrigen heutzutage als wesentlicher Bestandteil eines ordnungsgemäßen Risikomanagements im Rahmen der IT-Compliance angesehen werden. Dies zumindest dann, wenn die Risikoabschätzung ergibt, dass der Anbieter personenbezogene oder geschäftskritische Daten des Kunden speichert oder in sonstiger Form verarbeitet.

Dieser Abschnitt soll beschreiben, inwieweit im Rahmen des eigenen Risikomanagements auch eine Überprüfung der Informationssicherheit eines externen Anbieters erforderlich ist.

Eine solche Überprüfung geschieht z.B. durch Self-Assessments des Anbieters, aber vor allem auch über Zertifikate oder auch Testate, vgl. hierzu die Ausführungen in Abschnitt 5 des "Leitfaden Cloud Security".[3] Diese Überprüfung kann dem Kunden einen ersten Eindruck davon vermitteln, in welchem Umfang der Anbieter Kontrollen zur Sicherstellung eines angemessenen Sicherheitsniveaus eingerichtet und auch umgesetzt hat.

Für die meisten Nutzer von Cloud-Diensten ist eine solche Überprüfung ausreichend. Allerdings kann es möglich oder aus regulatorischen Anforderungen heraus sogar erforderlich sein, dass der Kunde sich bei dem Anbieter vor Ort zusätzlich ein eigenes Bild zum Stand der Informationssicherheit verschafft. Für eine solche Lagefeststellung kann je nach Schutzbedarf der Daten des Kunden ein Self Assessment des Anbieters ausreichen, bei kritischen Daten können jedoch tiefergehende Maßnahmen wie eine Dokumenten- oder sogar eine Vor-Ort-Prüfung beim Anbieter angezeigt sein.

Hierzu ist es unbedingt erforderlich, dass der Kunde sich vertragliche Prüfungsrechte ("Audit-Recht") einräumen lässt, die ihn in die Lage versetzen, entsprechende Überprüfungen vornehmen zu können. Große Aufmerksamkeit sollte dabei der Vertragsgestaltung mit dem Anbieter geschenkt werden. Beispielsweise existiert ein zielführendes Modell zur Verteilung der Verantwortlichkeiten zwischen Kunde und Cloud-Anbieter ("Shared Responsibility Model"), das nun diskutiert wird.

4.2 Shared Responsibility Model

Wird die IT-Infrastruktur samt Anwendungen eigenständig (on-premises) betrieben, liegt die Verantwortung und somit alle damit verbundenen Aufgaben ganz eindeutig bei der eigenen IT-Abteilung.

Sobald einzelne Services an Dritte ausgelagert werden (z.B. durch Überführung der Services in die Cloud), verändert sich die Zuordnung der Verantwortung. Je nach Sourcing-Modell können Teile der Verantwortung und der Aufgaben auf den Dienstleister übertragen werden.

Im Cloud-Umfeld wird in dem Zusammenhang von der "geteilten Verantwortung" (Engl.: "shared responsibility") gesprochen. Dieses weit propagierte Modell wurde umfassend im TeleTrusT Leitfaden zu Cloud Security behandelt.[4] Daher wird an dieser Stelle nicht weiter darauf eingegangen.

Auch wenn gemäß dem Modell der geteilten Verantwortung der Dienstleister für die einzelnen Sicherheitsmaßnahmen zuständig ist, kann der Cloud-Anwender dennoch dazu verpflichtet sein (z.B. aus Sicht des Gesetzgebers oder Regulierers), die Einhaltung geforderter Sicherheitsmaßnahmen durch den Dienstleister zu überprüfen.

---

[3] TeleTrusT, Cloud Security (https://www.teletrust.de/publikationen/broschueren/cloud-security/)
[4] TeleTrusT, Cloud Security (https://www.teletrust.de/publikationen/broschueren/cloud-security/)

Um den Überblick über die einzelnen Services und die jeweilige Zuständigkeit zu behalten, ist der Einsatz eines IT Asset Managements sinnvoll.

4.3 IT Asset Management und Software Bill of Materials (SBOM)

Das Absichern gegen Cybersicherheitsrisiken im Zusammenhang mit Lieferketten setzt Transparenz voraus: ein Unternehmen braucht den Überblick über seine eingesetzten IT-Assets, denn man kann nur schützen, was man kennt. Zur Transparenz über eingesetzte IT-Assets dient ein Inventarverzeichnis bzw. ein IT-Asset-Management-System (ITAM-System).

Im ISO-Standard ISO 19770-1 werden Anforderungen und Prozesse für Aufbau und Betrieb eines solchen ITAM-Systems definiert. Es soll sichergestellt werden, dass alle Informationen zu den eingesetzten IT-Assets (z.B. Eigentumsverhältnisse, Risikobewertungen und Verantwortlichkeiten) dokumentiert und überwacht werden. Die Norm kann dabei auf alle Arten von IT-Assets angewendet werden, egal ob physisch, virtuell, on-premises oder in der Cloud. Der Geltungsbereich und die Managementziele des ITAM-Systems sind dabei vom Unternehmen so zu definieren, dass sie mit den Unternehmenszielen übereinstimmen. Essenziell für den Erfolg des ITAM-Systems ist das entsprechende Engagement der Managementebene, welche neben der Bereitstellung der benötigten Ressourcen auch die Zuweisung der Rollen und Verantwortlichkeiten im eigenen Unternehmen übernehmen muss.

Gerade extern bereitgestellte Dienste wie Software as a Service (SaaS), Platform as a Service (PaaS) oder Infrastructure as a Service (IaaS) stellen u.a. aufgrund von gemischten Verantwortlichkeiten und den damit einhergehenden Risiken besondere Anforderungen an das IT-Asset-Management. Nach ISO 19770-1 müssen alle ausgelagerten Prozesse und Aktivitäten sowie alle dazugehörigen Informationen in das ITAM-System integriert werden. Neben dem Umfang der ausgelagerten Prozesse müssen auch alle Schnittstellen mit den unternehmenseigenen Prozessen bestimmt und dafür Sorge getragen werden, dass alle Fragen in Bezug auf Verantwortlichkeiten und Befugnisse geklärt und dokumentiert werden. Gleichzeitig ist sicherzustellen, dass die nötigen Prozesse zum Wissens- und Informationsaustausch mit den jeweiligen externen Dienstleistern definiert sind.

Das IT-Asset-Management und die dazugehörigen Geschäftsprozesse können insbesondere für kleinere Unternehmen eine kaum zu überwindende Hürde darstellen. Es empfiehlt sich also ein mehrstufiges Vorgehen, wie es im Annex B der ISO 19770-1 beschrieben wird.

So beschränkt sich die erste Stufe (Tier 1) darauf, einen Überblick über die im eigenen Unternehmen eingesetzten IT-Assets zu erhalten, um diese verwalten zu können. In der zweiten Stufe (Tier 2) folgen dann Prozesse, die in Zusammenhang mit dem Lebenszyklus der IT-Assets stehen. In Stufe 3 (Tier 3) folgen dann weitere Optimierungen wie die Integration des Relationship Managements.

"Software Bill of Materials" (kurz "SBOM") sind eine sinnvolle und zunehmend erforderliche, Ergänzung des IT-Asset Managements. Einfach ausgedrückt handelt es sich um eine Stückliste, aus der hervorgeht, welche Komponenten in einer Software eingebaut wurden. Das betrifft nicht nur die Komponenten, die vom Anbieter selbst entwickelt wurden, sondern insbesondere auch solche Bestandteile, die er von Drittlieferanten in seiner Software einsetzt.

Minimumanforderung ist die konkrete Bezeichnung der eingebauten Komponente sowie die jeweilige Version. Im Sinne der Transparenz und der Risikobewertung sollten SBOM für jede in einem Unternehmen eingesetzte Software durch den Software-Lieferanten bereitgestellt werden. Mindestens jedoch muss der Software-Lieferant auf Anfrage Auskunft zu einer SBOM und somit den in seiner Software enthaltenen wesentlichen Komponenten geben. Entsprechend des Entwicklungszyklus der Software muss diese SBOM zudem mit jedem Release und Update aktualisiert werden.

Die Inhalte der SBOM für eingesetzte Software müssen in den Schwachstellenmanagement-Prozess einfließen und als Vergleichsgrundlage in den regelmäßigen Scans gegen bekannte Schwachstellen verwendet werden.

Um SBOMs für jede Softwareversion zu generieren, zu speichern und abzurufen, ist ein SBOM-Plugin idealerweise in die CI/CD-Pipeline integriert. Das hilft Lieferanten bei der Verwaltung von Software-Abhängigkeiten und bietet Kunden Funktionen zum Verständnis der einzelnen Komponenten ihrer Software. Darüber hinaus kann es für die dynamische Überwachung von Bedrohungen in Echtzeit eingesetzt werden.

In SBOMs werden VEX-Berichte (VEX: Vulnerability Exploitability eXchange) integrierbar sein, um die Ausnutzbarkeit von Schwachstellen zu identifizieren und zu bewerten. Damit lassen sich Bedrohungsanalysen für Software-Abhängigkeiten in zwei Stufen durchführen. Zunächst werden alle in einer SBOM genannten Software-Abhängigkeiten auf bekannte, in CVE- und NVD-Datenbanken erfasste Schwachstellen gescannt und es wird eine Schwachstellenliste

erstellt. Danach wird jede Schwachstelle in Bezug auf ihre Exposition in der Software genau untersucht und ein VEX-Bericht erstellt. Ein VEX-Bericht bestimmt, welche der entdeckten Schwachstellen für eine bestimmte Software ausnutzbar sind.

Für SBOM wurden verschiedene Datenformate entwickelt. ISO-Standards gibt es für die Formate SPDX[5] und SWID[6], von OWASP wurde der Standard Cyclone DX verabschiedet[7]. SWID und SPDX dienen primär der eindeutigen Identifikation von Software zu verschiedenen Zwecken (nicht nur Sicherheit). Cyclone DX dagegen fokussiert auf der Sicherheit von Anwendungen und der Analyse der Komponenten der Supply-Chain, auch über Software hinaus, unter Einbeziehung z.B. von Hardware-Komponenten und Cloud Services. Die Formate sind zueinander nicht kompatibel.

Perspektivisch wird das Konzept der Stücklisten auf allgemeinere BOMs (Bill of Materials) weiterentwickelt. Dadurch lässt sich Transparenz nicht nur hinsichtlich verwendeter Software (SBOM) herstellen, sondern auch hinsichtlich aller anderen eingesetzten Komponenten: Software as a Service Bill of Materials (SaaSBOM), Hardware Bill of Materials (HBOM), Operations Bill of Materials (OBOM)[8].

Die US-Administration hat durch eine Executive Order im Mai 2021[9], konkretisiert durch das US Department of Commerce (Juli 2021)[10] und NIST (Februar 2022)[11], die Bereitstellung und Verwendung von SBOM durch Lieferanten der US-Administration vorgeschrieben. Die EU-Kommission arbeitet im Rahmen des Cyber Resilience Act an einer ähnlichen Vorschrift[12]. Es wird erwartet, dass sich die Bereitstellung von SBOM durch Lieferanten und Betreiber von Software und Services zum Marktstandard entwickelt. Allerdings lassen die bisher beschriebenen Konzepte für SBOM die erweiterten Anforderungen durch die Nutzung von Cloud Services - sei es als SaaS, über Cloud APIs oder auch nur durch dynamische Einbindung gehosteter Softwarebibliotheken - weitgehend unberücksichtigt.

Die neuesten Entwicklungen zeigen Versuche, mittels KI (Künstlicher Intelligenz) die SBOM kontinuierlich zu überprüfen und selber Tests zu unternehmen. Die sog. "Test-Bibliotheken" dazu sind gerade im Entstehen. Somit wäre eine Aktualisierung von SBOM aus zwei (2) Seiten möglich, zum einen über globale Plattformen, die von Anbietern gepflegt werden, als auch von Anwender-Seite. Dies kann dazu beitragen die Zero-Exploits Zeiten zu verkürzen.

4.4 Monitoring

Da Supply-Chain-Angriffe nicht direkt die eigene IT-Infrastruktur von Unternehmen attackieren, sondern über als vertrauenswürdig eingestufte IT-Services Dritter eingeschleust werden, sind übliche Schutzmaßnahmen von Anwenderunternehmen gegen diese Attacken häufig wirkungslos - insbesondere solche, die am Unternehmensperimeter ansetzen. Wenn über eine Supply Chain Attacke Schadcode in die IT-Infrastruktur eingebracht wird, dann können bei einer groben Betrachtung drei Szenarien unterschieden werden:

1. Der Schadcode hat die Aufgabe, Daten aus der IT-Infrastruktur zu exfiltrieren.
2. Der Schadcode soll die IT-Infrastruktur sabotieren.
3. Der Schadcode soll eine Kombination aus den zuvor aufgeführten Varianten durchführen.

Solange der Schadcode inaktiv ist, besteht ohne konkreten Verdacht und daraufhin durchgeführte gezielte Untersuchungen nur eine sehr geringe Chance, den Schadcode zu entdecken. Sobald der Schadcode aktiv wird, kommt es allerdings zu ungewöhnlichen Aktivitäten in der IT-Infrastruktur. Dies können unterschiedliche Verhaltensänderungen sein:

- Entstehen neuer Kommunikationsbeziehungen.
- Verwendung unerwarteter öffentlicher IP-Adressen.
- Auftreten typischer Ereignisse zu ungewöhnlichen Zeiten.
- Verringerung von TCP-Fenstergrößen, modifizierte Payload in Standard-Netzwerktechnik-Protokollen, etc.

---

[5] ISO/IEC 5962:2021 - SPDX Specification V2.2.1
[6] ISO/IEC 19770-2:2015 - Software identification tag (SWID)
[7] OWASP CycloneDX Software Bill of Materials (SBOM) Standard (https://cyclonedx.org/)
[8] Siehe z.B https://cyclonedx.org/capabilities/
[9] US White House Executive Order 14028 on Improving the Nation's Cybersecurity (12. Mai 2021)
[10] US Department of Commerce: "The Minimum Elements for an SBOM" (12. Juli 2021)
[11] NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1 (Februar 2022)
[12] European Commission: Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act (15.9.2022)

Derartige Verhaltensänderungen in einer IT-Infrastruktur können mit Monitoring-Systemen, die eine sogenannte Anomalie-Erkennung bieten, grundsätzlich erkannt werden. Das Bundesamt für Sicherheit in der Informationstechnik listet zur besseren Orientierung von Unternehmen und Behörden in seiner Empfehlung BSI-CS-134 Anomalien auf, die von entsprechenden Monitoring-Systemen erkannt werden sollten[13]. Auch sollten ggf. genutzte Accounts (auch programmatische Service Accounts und die API-Nutzung) von Hyperscalern[14] in ein solches Monitoring aufgenommen werden, da sich Angriffe aus einer Supply-Chain-Schwachstelle auf andere Bereiche ausweiten können. Dies kann durch die Auswertung der Cloud-Audit Logs erreicht werden (UEBA - User & Entity Behaviour Analytics).

Je nach technologischer Ausprägung und Funktionsumfang können derartige Monitoring-Systeme Anomalien nicht nur erkennen, sondern auch wichtige Informationen über Eintrittswege und Ausbreitung in der IT-Infrastruktur liefern. Dies sind relevante Informationen zur Eliminierung des Schadcodes oder betroffener Ressourcen und zur Begrenzung von Kosten für die Bereinigung und die Wiederherstellung von IT-Systemen.

4.5 Notfallplanung

Wurde inventarisiert, welche Services und Komponenten in der Supply Chain für die eigenen Anwendungen und Dienste erforderlich sind, sollte man sich auch damit befassen, was bei Ausfall oder Manipulation eines der zugelieferten Bestandteile gemacht werden soll. Generell ist für jegliche Störungen und Angriffe sinnvoll, ein Incident-Handling und Notfall-Management zu etablieren, in das man dann auch Supply-Chain spezifische Vorfälle einklinkt.

Dazu wird eine zweistufige Vorgehensweise empfohlen: Zunächst sollten Verantwortlichkeiten und Kommunikationswege für Notfälle generell festgelegt sein. Für besonders wichtige Services sollten dann konkrete technische und organisatorische Maßnahmen für relevante Szenarien vorgeplant werden. Die Festlegungen werden in einem Notfallhandbuch festgehalten.

Hilfreich ist dafür eine Orientierung an Standards wie beispielsweise BSI 200-4[15]. Bezüglich der Gefährdungen durch die Supply Chain ist empfehlenswert, Schutzziele wie Verfügbarkeit und Vertraulichkeit sowie Integrität zu unterscheiden. Für wesentliche Geschäftsprozesse sollte dokumentiert sein, von welchen IT-Systemen, IT-Anwendungen und Diensten diese abhängig sind und wie der Schutzbedarf der zu verarbeiteten Daten ist. Dies dient als Grundlage, um festzulegen, wie man bei Ausfall, Störung oder Manipulation von zugelieferten Bestandteilen umgeht.

Im Wesentlichen unterscheidet sich die Notfallplanung bezüglich Angriffe oder Störungen der Supply Chain nicht von der Notfallplanung, die man für jegliche Informationstechnik benötigt, die man einsetzt oder nutzt. Es ist hilfreich entsprechend vorbereitet zu sein, um dann im konkreten Fall von Ausfällen, Störungen oder Manipulationen einzelner zugelieferter Komponenten entscheiden zu können, wie vorzugehen ist. Man ist nicht gänzlich der Zulieferung ausgeliefert, jede Institution kann zumindest über die temporäre Nicht-Nutzung von Systemen und Diensten entscheiden. Das sollte nur vorab festgelegt sein und nicht erst dann geklärt werden, wenn der Notfall eintritt.

[13] BSI.CS-134 gilt zwar eigentlich für Netzwerke in Produktionsumgebungen, gibt aber wertvolle Hinweise auch für das Monitoring von Netzwerken generell.

[14] Hyperscaler sind Systeme, die durch Cloud-Computing entstehen. In diesen Systemen sind Tausende oder gegebenenfalls Millionen von Servern in einem Netzwerk verbunden. Zu den großen Hyperscalern gehören u.a. Amazon (Amazon Web Services), Microsoft (Azure) und Google (Google Cloud Platform).

[15] BSI-Standard 200-4 Business Continuity Management: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD_2_0.pdf?__blob=publicationFile&v=6

5 Schlussfolgerungen und Forderungen

5.1 Forderung: Technische und Organisatorische Realisierung Inventarverzeichnis

Wie bereits in den vorstehenden Kapiteln ausgeführt können einzelne Unternehmen in der heutigen, vernetzten und zunehmend arbeitsteiliger aufgestellten digitalen Umgebung für sich alleine keinen angemessenen Grad an IT-/Cybersicherheit nur "aus eigener Kraft" sicherstellen. Neben der Verwendung von Hard- und Software, deren "Ingredienzien" in der Regel nicht bzw. nicht vollständig bekannt sind, ist die Inanspruchnahme von IT- und Kommunikationsdienstleistungen ein weiterer "blinder Fleck" für die IT-Sicherheit des diese Dienstleistungen in Anspruch nehmenden Unternehmens.

Die in 5.2 beschriebenen bzw. geforderten rechtlichen Rahmenbedingungen wirken zwar auf das in Deutschland beheimatete Unternehmen, welches Cloud-Dienstleistungen nutzt, finden jedoch nicht zwingend Anwendung auf einen diese Dienstleistungen bereitstellenden im Ausland sitzenden Anbieter. Aus diesem Grund wäre es wünschenswert, möglichst einheitliche, internationale Regelungen/Vereinbarungen zu implementieren. Folgende Aspekte sollten geregelt werden:

a) Konvention zur eindeutigen Identifikation von Softwarecode-Versionen,
b) Plattform oder Konvention der Schnittstellen für den Informationsaustausch.
c) Pflicht des "Code-Einbringers" zur vollständigen und aktuellen Liste verwendeter Codeversionen und
d) Pflicht des "Code-Verwenders" (auch bei indirekter Verwendung durch Cloud-Dienstleistungen) zur Ermittlung und Pflege einer Übersicht (in)direkt verwendeter Softwarecodeversionen.

Zu a)
Unter Verwendung der bekannten Nomenklatur im Internet könnte die Kombination eines einheitlichen Produkt- und Versionscodes sowie der IP-Adresse (und ggf. CVE) die eindeutige Identifikation in Cloud-Dienstleistungen (oder direkt) verwendeter Softwarecodes sichergestellt werden.

Die Zusammenstellung der in einer Anwendung, einer Clouddienstleistung oder letztendlich in einem Unternehmen verwendeten Software-Codeversionen könnte über "Inhaltslisten" erfolgen. Hier bietet es sich an, die aus den USA initiierte SBOM-Initiative als "Beipackzettel" für Software oder Cloudienstleistungen zu verwenden.

Zu b)
In Anlehnung an das der US-amerikanischen National Cybersecurity unterstellte CVE-Referenzierungssystem, welches durch die Mitre Corporation gepflegt wird, sollte eine internationale Organisation ähnlich der ICANN oder einem Escrow-System als Betreiber einer Plattform (Datenbank) sicherstellen, dass die Bereitsteller und die Nutzer von Softwarecodes basierend auf der unter a) beschriebenen Nomenklatur Informationen in Echtzeit austauschen können.

Um auch mehrstufige Betrachtungen vornehmen zu können, muss sichergestellt sein, dass die Plattform einen "Drill Down" bis zur letzten Ebene ermöglicht.

Zu c)
Inwiefern sich eine weltweite gesetzliche Pflicht zur Dokumentation und Pflege verwendeter Softwarecodes durchsetzen lässt ist mehr als fraglich. Aus diesem Grund wird der Umsetzungsdruck allenfalls über die Verwender-Seite (Schneeball-System) realisierbar sein, die im Idealfall zu entsprechenden vertraglichen Anforderungen führt.

Zu d)
Mittels einer mindestens EU-weiten (besser in Abstimmung mit den USA) Regelung z.B. auf Basis der derzeitigen US-amerikanischen SBOM-Initiative werden alle Unternehmen im Geltungsbereich verpflichtet, aktuelle Verzeichnisse der von ihnen direkt oder indirekt (Cloud-Services) verwendeten Softwarecodeversionen bereit zu halten, sei es "on premises" oder über ein Konto bei einer MITRE-ähnlichen anerkannten Plattform/Datenbank.

Zur Umsetzung des vorstehenden Ansatzes bedarf es neben umfangreichen Vorarbeiten insbesondere des politischen Willens teilnehmender Staaten (Gemeinschaften) um ein nachhaltig funktionierendes, integriertes System der Cloud Supply Chain Security zu erschaffen.

5.2 Forderung: Rechtliche Rahmenbedingungen

a) Identifikation der anwendbaren Regulatorik

Die rechtlichen Rahmenbedingungen für Sicherheit in der (Cloud-)Supply Chain sind vielschichtig und unterliegen kontinuierlichen Erweiterungen. Eine ausführliche Darstellung würden den Rahmen dieses Leitfadens sprengen. Es sollen hierzu daher in diesem Leitfaden nur grundlegende Überlegungen und Schlussfolgerungen getroffen werden.

Die rechtlichen Rahmenbedingungen und die entsprechende Ratio für "Sicherheit in der Cloud" basieren durchweg auf der Überlegung, dass ein Unternehmen, das zur Erbringung seiner Services einen Dritten ("Cloud-Anbieter") einsetzen möchte, im Rahmen seines eigenen internen Kontrollsystems eine Bewertung durchführen muss, ob und inwieweit der Einsatz des Dritten eine Gefährdung bzw. Risiko für die eigenen Unternehmensziele und Sicherheit darstellt.

Für einige Bereiche wie z.B. Banken (§ 25b KWG) und Versicherungen (§§ 32 VAG) ist die Notwendigkeit derartiger Risikoabwägungen in Verbindung mit dezidierten Verordnungen und Verwaltungsvorschriften ausdrücklich geregelt, ergibt sich aber auch im Übrigen aus entweder allgemein anwendbaren Gesetzen wie §§ 28, 32 DSGVO für Auftragsverarbeitungen und einer allgemeinen Pflicht der Geschäftsleitung zur Einhaltung der IT-Compliance (§§ 76, 91 II, 93 I AktG). Diese Pflicht ist ausdrücklich nur für Aktiengesellschaften geregelt, strahlt jedoch nach wohl herrschender Meinung auch auf andere Gesellschaftsformen aus.

Ob und in welcher Tiefe ein solches Risikomanagement auch die Überprüfung des externen Cloud-Anbieters gebietet, kann sich entweder ausdrücklich aus dem Gesetz (s.o.) oder auch aus dem Schutzbedarf für die eigenen Informationen ergeben.

Wer z.B. einem SaaS-Provider, der wiederum die Rechenzentrumsleistungen eines US-amerikanischen Hyperscalers nutzt, seine hoch unternehmenskritischen Daten anvertraut, wird den SaaS-Provider einer kritischeren und tieferen Prüfung unterziehen müssen als den Anbieter einer lokal gehosteten Software, mit der die Getränkelieferungen für einzelne Standorte koordiniert werden.

b) Stand der Technik

Diverse Vorschriften wie Artikel 32 DSGVO fordern die Ergreifung (geeigneter) technischer UND organisatorischer Maßnahmen.

Während organisatorische Maßnahmen vor allem auf die Einrichtung und den Ablauf bestimmter Prozesse und die durchführenden Personen abzielt, z.B. Mitarbeiterschulungen im Datenschutz, betreffen die technischen Maßnahmen den relevanten "Tech Stack", also Hardware-, Software- und Netzwerkkomponenten, die für die Datenverarbeitung genutzt und herangezogen werden.

Maßstab für die technische Angemessenheit für Sicherheitsmaßnahmen ist der "Stand der Technik" (s. z.B. §§ 25, 32 DSGVO). Hier besteht jedoch ein gewisses Maß an Unsicherheit, welche Maßnahmen umgesetzt sein müssen, um dem sog. "Stand der Technik" zu genügen, da diesbezüglich keine einheitlichen Bewertungskriterien vorhanden sind.

Der Stand der Technik muss fortlaufend evaluiert werden. Orientierungshilfe für den Bereich Cloud-Sicherheit ist hier z.B. der BSI Cloud Computing Compliance Criteria Catalogue ("BSI C5 2020"), der neben organisatorischen Maßnahmen auch relevante technische Themenbereiche abdeckt, aber auch die "Handreichung Stand der Technik in der IT-Sicherheit" des TeleTrusT.[16]

Eine Zertifizierung nach "BSI C5" ist für Cloud-Anbieter der beste verfügbare Zertifizierungsmechanismus, um die Angemessenheit des internen Kontrollsystems und die Einhaltung des Standes der Technik zum Schutz von Informationen nachzuweisen.

Da Standards des BSI wie der "BSI C5: 2020" regelmäßig den jeweiligen Stand der Technik widerspiegeln, sollte nach hiesiger Auffassung für einen entsprechend zertifizierten Cloud-Anbieter die Vermutung gelten, dass er diesen eingehalten hat.

[16] Siehe TeleTrusT, https://www.stand-der-technik-security.de/startseite/

Es wäre im Sinne einer umfassenden Rechtssicherheit zusätzlich wünschenswert, wenn einheitliche Kriterien für die Bewertung des "Standes der Technik" bereitstünden, um so unterschiedlichen Auffassungen hierzu vorzubeugen.

c) Vertrag zwischen Cloud-Kunde und Cloud-Anbieter

Wie die Ausführungen in diesem Leitfaden gezeigt haben, ist "Sicherheit in der Cloud" von einer Vielzahl von Faktoren abhängig, u.a., dass geschäftskritische Assets und die für die Assets bestehenden Sicherheitsrisiken bekannt sind.

Da Informationssicherheit technisch nie vollständig gewährleistet werden kann, kommt der rechtlichen Absicherung eine umso höhere Bedeutung zu.

Verantwortlichkeiten ("Responsibility") können zwischen Cloud-Kunde und Cloud-Anbieter z.B. nach dem Shared Responsibility Model vereinbart werden. Gleichzeitig sollte jedoch auch die Frage der "Accountability" und damit auch die Frage der Haftung der jeweils anderen Parteien ausdrücklich im Vertrag geklärt werden.

Es ist beispielsweise sicherlich zielführend, wenn ein IaaS-Provider verantwortlich für die Funktionalität und technische Sicherheit der von ihm in seinem Rechenzentrum vorgehaltenen Systeme zeichnet und er entsprechend z.B. bei einer Nicht-Verfügbarkeit innerhalb definierter Zeiten diese wieder in Betrieb nehmen muss.

Nicht selten kann dem Cloud-Kunden jedoch durch die Nicht-Verfügbarkeit seiner Daten ein eigener Schaden und/oder Schäden bei Dritten entstehen, die der Cloud-Kunde dann regulieren muss. Daher sollte der Vertrag mit dem Cloud-Anbieter auch eine entsprechende Haftung für solche Schäden vorsehen bzw. eine entsprechende Freistellung gegenüber dem Cloud-Kunden.

Gerade an diesem Punkt wird oftmals eine ernsthafte Verhandlung mit dem Cloud-Anbieter versäumt. Dies kann zu entsprechenden Haftungsrisiken für die hierzu berufenen Vertreter des Unternehmens auf Seiten des Kunden, z.B. CIO, führen.

Ein weiterer wesentlicher Aspekt ist zudem die Vereinbarung eines umfassenden Audit-Rechts gegenüber dem Cloud-Anbieter, um eine eigenständige Überprüfung der technischen und organisatorischen Maßnahmen des Cloud-Anbieters vornehmen zu können.

d) Forderungen

Der Gesetzgeber ist auf europäischer und nationaler Ebene bestrebt, das Cyber-Sicherheitsrecht durch verschiedene Gesetze weiter zu vereinheitlichen. Zu nennen sind hier vor allem der Cyber Resilience Act, der sich unmittelbar an Hersteller von **Produkten** mit digitalen Elementen richtet, sowie "The Network and Information Security Directive ("NIS-2")" und der "Digital Operational Resilience Act ("DORA")" mit Anforderungen an das Niveau der Cybersicherheit von **Organisationen**, was ausdrücklich die Sicherstellung der Sicherheit in der Supply Chain miteinschließt (siehe z.B. NIS-2 Rz. 85 ff. bzw. DORA Art. 28 Abs. 6).

Hinsichtlich der NIS-2-Richtlinie ist eine zeitnahe Konkretisierung durch die nationalen Gesetzgeber wünschenswert, um den betroffenen Unternehmen Sicherheit darüber zu verschaffen, ob sie in den Anwendungsbereich des Gesetzes fallen und welche Maßnahmen, insbesondere mit dem Blick auf die Absicherung der Supply Chain, zu ergreifen sind.

6 Fazit

Angriffe auf die IT-Infrastruktur von Unternehmen erfolgen vermehrt über die Supply Chain. Die Sicherheit von Lieferketten ist deshalb von zunehmender Bedeutung. Ein wesentliches Problem ist dabei mangelnde Transparenz der genutzten Elemente der Supply Chain. Besonders Software as a Service wird meist "as is" eingekauft (so, wie sie ist), ohne detaillierte Informationen darüber, welche Hardware, Betriebssysteme, Softwarebibliotheken etc. beim Anbieter zum Einsatz kommen oder gar welche Versionen jeweils aktuell eingesetzt werden und welche bekannten Schwachstellen (Vulnerabilities) es darin gibt. Soweit z.B. auf Grund datenschutzrechtlicher Anforderungen Elemente der IT und Schutzmaßnahmen auf Anbieterseite beschrieben werden, bleibt diese Information in der Regel oberflächlich.

Eine Einschätzung von Risiken in der Supply Chain durch Anwender ist dadurch bestenfalls schwierig, für kleine und mittlere Unternehmen in der Regel unmöglich. Anwender verlassen sich deshalb auf Risikoeinschätzung und Schutzmaßnahmen der Anbieter, ohne diese im Detail beurteilen und nachvollziehen zu können oder gar zu einer eigenen aktuellen Bewertung zu kommen. Entsprechend sind sie auch bei Attacken praktisch vollständig vom Anbieter abhängig.

Die Situation wird dadurch verschärft, dass die Supply Chain über viele Stufen geht. Anbieter aggregieren ihrerseits als Anwender Elemente und Services anderer Anbieter und sind von diesen abhängig. Diese Problematik wurde bei den o.g. Attacken auf SolarWinds, Kaseya und 3CX sehr deutlich.

Auf den ersten Blick sind Anbieter von Cloud-Diensten und IT-Komponenten für die Sicherheit der von ihnen gelieferten Komponenten und Dienstleistungen verantwortlich. Doch aus Sicht der Anwender, die am Ende von Angriffen auf die Sicherheit betroffen sind, ist dies oft unbefriedigend. Die Anwender müssen auch eigene Maßnahmen zum Schutz ihrer Infrastruktur und Daten ergreifen, um sich gegen solche Angriffe zu verteidigen.

Maßnahmen zur sicheren Nutzung von Cloud Services dienen auch der Verbesserung der Supply Chain Security: ein sorgfältiges Provider Assessment, klare Absprachen von Zuständigkeiten, Monitoring auch externer Dienste und eine Notfallplanung.

Um das Problem der mangelnden Transparenz zu lösen, führt der Weg über eine Software Bill of Materials (SBOM). Eine SBOM ist eine Aufstellung aller Komponenten, die in einer Software-Anwendung enthalten sind. Sie stellt damit Transparenz bezüglich der eingesetzten Software-Bestandteile einer Anwendung her. Auf weitere Elemente der Supply Chain angewendet (d.h. erweitert auf Hardware, Cloud Services etc.), erlaubt das Konzept eine vollständige Transparenz über alle eingesetzten Komponenten. Wenn neue Erkenntnisse zu Fehlern und Lücken in diesen Komponenten auftauchen, können Anwender schnell ermitteln, ob sie möglicherweise betroffen sind und ob die von ihnen genutzten Anwendungen gefährdet sind. Ggf. können dann eigene Maßnahmen getroffen oder über eine temporäre Nicht-Nutzung entschieden werden.

Die statische Bereitstellung von SBOMs, etwa zum Zeitpunkt des Vertragsschlusses, reicht jedoch nicht aus. Es ist vielmehr eine dynamische Bereitstellung dieser Informationen durch die Anbieter nötig. Das bedeutet, dass diese Informationen zu jedem Zeitpunkt, auch nach Updates, aktuell sein müssen. Anbieter müssen auch wiederum aktuelle Informationen zu den von ihnen genutzten Komponenten erhalten und an ihre Anwender weitergeben. Diese Art der Bereitstellung von SBOMs gibt es bislang noch nicht. Ansätze sind vorhanden, jedoch in Teilen zueinander inkompatibel.

Anwender können einen erheblichen Beitrag zur Verbesserung der Sicherheit in der Supply Chain leisten, wenn sie die Bereitstellung von SBOMs durch Provider in ihren Anforderungskatalog aufnehmen. Provider sollten ihrerseits ihren Anwendern diese Informationen zur Verfügung stellen. Die gewonnene Transparenz versetzt Anbieter und Anwender in die Lage, Cybersicherheit aktiv zu managen, statt nur auf Vorfälle zu reagieren.

7 Glossar

AG	Arbeitsgruppe
API	Application Programming Interface
AV	Antivirus
BSI	Bundesamt für Sicherheit in der Informationstechnik
CI/CD	Continuous Integration / Continuous Deployment
CVE	Common Vulnerabilities and Exposures
DDoS (Attacken)	Distributed Denial of Service (Attacken)
DORA	Digital Operational Resilience Act
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
IaaS	Infrastructure as a Service
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
ITAM	IT-Asset-Management-System
NVD	National Vulnerability Database
on-premises	in den eigenen Räumlichkeiten, lokal
OWASP	Open Worldwide Application Security Project
PaaS	Platform as a Service
SaaS	Software as a Service
SBOM	Software Bill of Materials
SECaaS	Security as a Service
SPDX	Software Package Data Exchange
SWID	Software Identification Tag
TLS	Transport Layer Security
UI	User Interface
VPN	Virtual Private Network
VEX	Vulnerability Exploitability eXchange