EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA-BERICHT ZUR BEDROHUNGSLAGE – LIEFERKETTENANGRIFFE

JULI 2021

ÜBER ENISA

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einem hohen gemeinsamen Maß an Cybersicherheit in ganz Europa beizutragen. Sie wurde im Jahr 2004 gegründet und durch den Rechtsakt zur Cybersicherheit in ihrem Mandat weiter gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen und Einrichtungen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Kapazitätsaufbau und Sensibilisierung arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und nicht zuletzt ein sicheres digitales Umfeld für die Gesellschaft und die Bürgerinnen und Bürger Europas zu gewährleisten. Weitere Informationen über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

KONTAKT

Wenn Sie mit den Autoren Kontakt aufnehmen möchten, wenden Sie sich bitte an etl@enisa.europa.eu.
Medienanfragen zu dieser Veröffentlichung richten Sie bitte an press@enisa.europa.eu.

HERAUSGEBER

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou und Apostolos Malatras – Agentur der Europäischen Union für Cybersicherheit
Sebastian Garcia und Veronica Valeros – Tschechische Technische Universität Prag

DANKSAGUNGEN

Wir danken den Mitgliedern und Beobachtern der von der ENISA eingerichteten Ad-hoc-Arbeitsgruppe für Cyber-Bedrohungslagen für ihre wertvollen Rückmeldungen und ihre Kommentare zur Validierung dieses Berichts. Ebenso bedanken wir uns bei Volker Distelrath (Siemens) und Konstantinos Moulinos (ENISA) für ihre Rückmeldungen.

RECHTLICHER HINWEIS

Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 2019/881 angenommen wurde. Die ENISA kann diese Veröffentlichung von Zeit zu Zeit aktualisieren.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung dient ausschließlich Informationszwecken. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

HINWEIS ZUM COPYRIGHT

ISBN: 978-92-9204-509-8 – DOI: 10.2824/168593

INHALT

ZUSAMMENFASSUNG

Lieferkettenangriffe sind schon seit vielen Jahren ein Sicherheitsproblem. Seit Anfang 2020 scheint die Community der Sicherheitsexperten jedoch verstärkt mit Lieferkettenangriffen konfrontiert zu sein. Möglicherweise im Zuge der Einführung robusterer Sicherheitsmaßnahmen bei den Organisationen haben Angreifer ihre Angriffe zunehmend und mit Erfolg auf Lieferanten verlagert. Durch die Herbeiführung von Systemausfällen, finanziellen Verlusten und Reputationsschäden − um nur einige zu nennen − ist ihnen gelungen, erhebliche Schäden zu verursachen. Lieferketten haben deshalb so große Bedeutung, weil von erfolgreichen Angriffen zahlreiche Kunden eines Lieferanten betroffen sein können. Die Kaskadeneffekte eines einzelnen Angriffs können also weitreichende Auswirkungen haben.

In diesem Bericht werden Lieferkettenangriffe beschrieben und untersucht, die im Zeitraum von Januar 2020 bis Anfang Juli 2021 entdeckt wurden. Den beobachteten Trends und Mustern zufolge haben Lieferkettenangriffe im Jahr 2020 zugenommen und wurden immer ausgefeilter. Dieser Trend setzt sich 2021 fort und stellt ein wachsendes Risiko für Organisationen dar. Schätzungen zufolge wird es im Jahr 2021 viermal mehr Lieferkettenangriffe geben als im Jahr 2020. Die Angriffe werden zur Hälfte APT-Akteuren (Advanced Persistence Threat = fortgeschrittene, andauernde Bedrohung) zugeschrieben und sind hinsichtlich ihrer Komplexität und Ressourcen den üblichen unspezifischen Angriffen weit überlegen. Damit auch weiterhin die Sicherheit von Organisationen gewährleistet ist, werden zunehmend neue Ansätze zur Erhöhung des Schutzes benötigt, die auch die Lieferanten einbeziehen.

Dieser Bericht mit einer Darstellung der Bedrohungslage in Bezug auf Lieferkettenangriffe aus Sicht der Agentur wurde mit Unterstützung der Ad-hoc-Arbeitsgruppe für Cyber-Bedrohungslagen erstellt.[1]

Die wesentlichen Ergebnisse des Berichts im Überblick:

- Im Bericht wird eine **Taxonomie** zur Klassifizierung von Lieferkettenangriffen beschrieben, um die Angriffe systematisch und besser analysieren zu können und zu verstehen, wie sie durchgeführt werden.
- Von Januar 2020 bis Anfang Juli 2021 wurden **24 Lieferkettenangriffe** gemeldet, die in diesem Bericht behandelt werden.
- Etwa **50 % der Angriffe** wurden von der Community der Sicherheitsexperten **bekannten APT-Gruppen** zugeschrieben.
- Rund **42 % der analysierten Angriffe** konnten **noch keiner bestimmten Gruppe zugeordnet** werden.
- Ca. **62 % der Angriffe auf Kunden** machten sich **deren Vertrauen in ihre Lieferanten** zunutze.
- In **62 % der Fälle bestand die Angriffstechnik** im Einsatz von **Schadprogrammen**.
- Bei **66 % der Vorfälle konzentrierten** sich die Angreifer auf den **Code der Lieferanten**, um so die eigentlich im Fokus stehenden Kunden zu kompromittieren.
- Etwa **58 % der Lieferkettenangriffe zielten darauf ab**, sich Zugang zu **Daten** (vor allem Kundendaten, einschließlich personenbezogener Daten und geistigen Eigentums) zu verschaffen. Bei rund **16 %** der Angriffe ging es um den Zugang zu **Personen**.
- **Nicht alle Angriffe sollten als Lieferkettenangriffe bezeichnet werden**, aber aufgrund ihrer Art sind sie oft potenzielle Vektoren für neue künftige Lieferkettenangriffe.

[1] Siehe https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes.

- **Organisationen müssen ihre Methodik zur Gewährleistung der Cybersicherheit in Bezug auf Lieferkettenangriffe aktualisieren** und alle ihre Lieferanten in den Schutz und die Sicherheitsüberprüfung einbeziehen.

1. EINFÜHRUNG

Lieferkettenangriffe sind schon seit vielen Jahren ein Sicherheitsproblem. Seit 2020 scheint die Community jedoch zunehmend mit organisierten Angriffen konfrontiert zu sein. Möglicherweise im Zuge der Einführung robusterer Sicherheitsmaßnahmen bei den Organisationen haben Angreifer ihre Angriffe zunehmend und mit Erfolg auf Lieferanten verlagert, und durch die Herbeiführung von Systemausfällen, finanziellen Verlusten und Reputationsschäden − um nur einige zu nennen − ist ihnen gelungen, erhebliche Schäden zu verursachen. In diesem Bericht werden Lieferkettenangriffe beschrieben und untersucht, die im Zeitraum zwischen Januar 2020 und Anfang Juli 2021 entdeckt wurden.

Die verheerenden Auswirkungen von Lieferkettenangriffen zeigten sich in vollem Umfang beim Angriff auf SolarWinds.[2] Der Angriff auf SolarWinds gilt als einer der größten Lieferkettenangriffe in den letzten Jahren, vor allem hinsichtlich der betroffenen Entitäten (u. a. Regierungsorganisationen und große Unternehmen). Er löste ein großes Medienecho aus und führte weltweit zu politischen Initiativen.[3] Der erst im Juli 2021 bekannt gewordene Angriff auf Kaseya[4] hat gezeigt, dass Lieferkettenangriffe auf Managed Service Providers stärker berücksichtigt werden müssen. Leider sind diese beiden Beispiele keine Einzelfälle, und die Zahl der Lieferkettenangriffe hat im letzten Jahr stetig zugenommen. Dieser Trend unterstreicht erneut, dass die politischen Entscheidungsträger und die Sicherheitsbehörden neue Schutzmaßnahmen entwickeln und einführen müssen, um potenziellen Lieferkettenangriffen in Zukunft zu begegnen und ihre Auswirkungen zu mindern.

Auf der Grundlage einer sorgfältigen Erhebung und Analyse werden in diesem Bericht Lieferkettenangriffe anhand der von Januar 2020 bis Anfang Juli 2021 festgestellten Vorfälle beschrieben. Für jeden Vorfall wurden die konstituierenden Schlüsselelemente ermittelt, z. B. die Angriffstechniken sowie die von den Angriffen betroffenen Lieferanten- und Kunden-Assets. Die Einführung einer Taxonomie für Lieferkettenangriffe wird deren Klassifizierung erleichtern und kann der Ausgangspunkt für einen strukturierteren Ansatz bei der Analyse solcher Angriffe und der Entwicklung spezieller Sicherheitskontrollen zu deren Abschwächung sein. Die vorgeschlagene Taxonomie hilft zudem, diese Angriffe auf einer gemeinsamen Grundlage zu klassifizieren, zu vergleichen und zu diskutieren. Die Ähnlichkeiten zwischen der vorgeschlagenen Taxonomie und bereits etablierten weiteren Rahmenmodellen werden erörtert.

Außerdem werden in diesem Bericht Parallelen zwischen dem Lebenszyklus von Lieferkettenangriffen und den bekannteren Angriffen durch fortgeschrittene, andauernde Bedrohungen (Advanced Persistent Threats, APTs) analysiert. Der Anhang enthält eine Zusammenfassung der wichtigsten Lieferkettenvorfälle seit 2020, die jeweils gemäß der oben genannten Taxonomie eingeordnet wurden.

Im Zentrum des Berichts steht eine Analyse aller gemeldeten Lieferkettenvorfälle mit dem Ziel, deren wichtigsten Merkmale und Techniken zu ermitteln. Die Analyse gibt Antworten auf folgende Fragen: Welche Angriffstechniken werden bei Lieferkettenangriffen am häufigsten eingesetzt, auf welche Kunden-Assets haben es die Angreifer hauptsächlich abgesehen, und welche Beziehung besteht zwischen den Angriffen und den Assets, auf die die Angriffe abzielen?

Infolge der zunehmenden aufmerksameren Beachtung von Lieferkettenangriffen wurden auch viele andere sicherheitsrelevante Vorfälle mit Lieferketten in Verbindung gebracht, d. h. es wurde vermutet, dass es sich dabei um Lieferkettenangriffe handelte. Daher wird hier anhand einiger Beispiele erörtert, was einen Lieferkettenangriff kennzeichnet und warum viele Angriffe eigentlich keine Lieferkettenangriffe sind. Das Verständnis der

[2] Russian SolarWinds hackers launch email attack on government agencies, The Guardian, https://www.theguardian.com/technology/2021/may/28/russian-solarwinds-hackers-launch-assault-government-agencies. Accessed on 08/07/2021.
[3] Siehe https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.
[4] Ransomware Attack Affecting Likely Thousands of Targets Drags On, WSJ, https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071. Zugriff am 9.7.2021.

Bedrohungslage in Bezug auf Lieferkettenangriffe ist wichtig, da eine falsche Klassifizierung von Vorfällen zu Fehlern bei der Analyse von Trends und zu falschen Schlussfolgerungen führen kann.

Der Bericht enthält zudem eine Reihe von Empfehlungen an politische Entscheidungsträger und Organisationen, insbesondere an Lieferanten, deren Befolgung die allgemeine Sicherheit gegen Lieferkettenangriffe erhöhen kann.

Dieser Bericht ist wie folgt gegliedert:

- **Kapitel 1** bietet eine kurze Einführung zum Begriff der Lieferkette und zur speziellen Bedrohungslage aus Sicht der ENISA.
- In **Kapitel 2** wird erörtert, was unter einem Lieferkettenangriff zu verstehen ist, und es wird eine strukturierte Taxonomie zur Klassifizierung relevanter Vorfälle eingeführt, die sich auch auf etablierte Rahmenmodelle zur Klassifizierung von Informationen über Cyberbedrohungen stützt.
- **Kapitel 3** vermittelt einen Überblick über den Lebenszyklus eines typischen Lieferkettenangriffs.
- In **Kapitel 4** werden die wichtigsten Lieferkettenangriffe im Zeitraum Ende 2020 bis Anfang 2021 beschrieben.
- **Kapitel 5** enthält eine Zeitleiste der relevanten Vorfälle und eine gründliche Analyse der Vorfälle.
- In **Kapitel 6** wird das Problem einer fälschlichen Einstufung von Vorfällen als Lieferkettenangriffe behandelt.
- **Kapitel 7** enthält sowohl allgemeine als auch technische Empfehlungen zur Verbesserung der Sicherheit der Lieferkette und zur Abschwächung der Auswirkungen von Lieferkettenangriffen.
- In **Anhang A** werden 24 in diesem Bericht genannte und analysierte Lieferkettenvorfälle zusammenfassend beschrieben.

2. WAS IST EIN LIEFERKETTENANGRIFF?

Der Begriff Lieferkette bezieht sich auf das Ökosystem von Prozessen, Menschen, Organisationen und Händlern bzw. Distributoren, die an der Erstellung und Lieferung einer endgültigen Lösung oder eines Produkts beteiligt sind.[5] Im Bereich der Cybersicherheit umfasst die Lieferkette ein breites Spektrum an Ressourcen (Hardware und Software), Speichern (Cloud oder lokal), Vertriebsmechanismen (Webanwendungen, Online-Shops) und Verwaltungssoftware.

In einer Lieferkette gibt es die folgenden vier wesentlichen Elemente:

- *Lieferant*: Eine Entität, die einer anderen Entität ein Produkt liefert oder eine Dienstleistung für sie erbringt.
- *Lieferanten-Assets*: Werte, die ein Lieferant zur Herstellung eines Produkts oder zur Erbringung einer Dienstleistung einsetzt.
- *Kunde*: Entität, die das vom Lieferanten erzeugte Produkt oder die von ihm erbrachte Dienstleistung bezieht.
- *Kunden-Assets*: Werte im Eigentum derjenigen, die das eigentliche Ziel eines Angriffs sind.

Eine Entität kann eine Einzelperson, eine Gruppe von Personen oder eine Organisation sein. Assets können u. a. Menschen, Software, Dokumente, Finanzmittel oder Hardware sein.

Bei einem Lieferkettenangriff werden mindestens zwei Angriffe kombiniert. Der erste Angriff richtet sich gegen einen Lieferanten, der dann dazu benutzt wird, das eigentliche Ziel anzugreifen, um schließlich Zugang zu dessen Assets zu erhalten. Das Ziel kann der Endkunde, aber auch ein anderer Lieferant sein. Damit ein Angriff als Lieferkettenangriff eingestuft werden kann, müssen daher sowohl der Lieferant als auch der Kunde Ziele sein.

2.1. EINE TAXONOMIE FÜR LIEFERKETTENANGRIFFE

In diesem Bericht wird eine Taxonomie zur Beschreibung von Lieferkettenangriffen und zur Strukturierung ihrer anschließenden Analyse vorgeschlagen. Bei dieser Taxonomie werden alle vier Schlüsselelemente einer Lieferkette sowie die von Angreifern verwendeten Techniken berücksichtigt. Die Taxonomie kann Organisationen dabei helfen, die verschiedenen Bestandteile eines Lieferkettenangriffs zu verstehen, sie mit anderen ähnlichen Cyberangriffen zu vergleichen und vor allem die Vorfälle als Lieferkettenangriffe zu identifizieren.

Die Taxonomie sollte als Leitfaden dienen, mit dem die Community bei einem neuen potenziellen Lieferkettenangriff versuchen kann, diesen zu analysieren, indem sie jedes der vier verschiedenen Taxonomie-Elemente identifiziert und darstellt. Wenn nicht sowohl ein Kunde als auch ein Lieferant angegriffen wurde, handelt es sich wahrscheinlich nicht um einen Lieferkettenangriff.[6]

Die in Tabelle 1 dargestellte Taxonomie enthält jeweils einen Abschnitt für den Lieferanten und für den Kunden. Im Abschnitt über die Lieferanten wird im ersten Teil („Angriffstechnik zur Kompromittierung der Lieferkette“) beschrieben, **wie** der jeweilige Lieferant angegriffen wurde. Der zweite Teil des Abschnitts über Lieferanten ist mit „Lieferanten-Assets als Gegenstand von Lieferkettenangriffen“ überschrieben und gibt Aufschluss darüber, **was** das Ziel des Angriffs auf den Lieferanten war.

Im Abschnitt über die Kunden wird im ersten Teil („Angriffstechniken zur Kompromittierung der Kunden“) beschrieben, **wie** der jeweilige Kunde angegriffen wurde. Der zweite Teil des Abschnitts über Kunden ist mit

[5] Beamon, B. M. (1998). Supply chain design and analysis: Models and methods. International journal of production economics, 55(3), 281-294.
[6] Weitere Beispiele siehe Abschnitt „Nicht alles ist ein Lieferkettenangriff“.

„Kunden-Assets als Gegenstand von Lieferkettenangriffen“ überschrieben und gibt Aufschluss darüber, **was** das Ziel des Angriffs auf den Kunden war.

Für jedes dieser vier Kriterien der Taxonomie haben wir die Elemente definiert, mit denen ein Lieferkettenangriff besser beschrieben werden kann. Die entsprechenden Elemente können besser deutlich machen, was über einen Angriff bekannt ist oder nicht. Die Taxonomie unterscheidet sich konzeptionell von der MITRE ATT&CK®-Wissensbasis und soll Letztere nicht ersetzen, sondern ergänzen. Die in der vorgeschlagenen Taxonomie definierten und in Tabelle 1 dargestellten Angriffstechniken sind in einigen Fällen mit relevanten Angriffstechniken verwandt, die im Rahmenmodell MITRE ATT&CK® beschrieben werden, und wurden dementsprechend mit dem jeweiligen MITRE ATT&CK®-Identifikator in eckigen Klammern gekennzeichnet (z. B. [T1189]). In den folgenden Unterabschnitten werden die vier Teile der Taxonomie und die Identifizierung ihrer Elemente erläutert.

Tabelle 1: Vorgeschlagene Taxonomie für Lieferkettenangriffe mit vier Teilbereichen: (i) Angriffstechniken gegen den Lieferanten, (ii) angegriffene Lieferanten-Assets, (iii) Angriffstechniken gegen den Kunden, (iii) angegriffene Kunden-Assets.

LIEFERANT		**KUNDE**	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung der Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Infektion mit einem Schadprogramm	Bereits vorhandene Software	Ausnutzen einer Vertrauensbeziehung [T1199]	Daten
Social Engineering	Software-Bibliotheken	Drive-by Compromise [T1189]	Personenbezogene Daten
Brute-Force-Angriff	Code	Phishing [T1566]	Geistiges Eigentum
Ausnutzen einer Sicherheitslücke in einer Software	Konfigurationen	Infektion mit einem Schadprogramm	Software
Ausnutzen einer Sicherheitslücke in einer Konfiguration	Daten	Physischer Angriff oder Modifikation	Prozesse
Open-Source Intelligence (OSINT, Informationsgewinnung aus frei zugänglichen Quellen)	Prozesse	Fälschung	Bandbreite
	Hardware		Finanzieller Schaden
	Menschen		Menschen
	Lieferanten		

Die Koordinierung der Reaktion auf Vorfälle und der Informationsaustausch auf Unionsebene erfolgen anhand einer EU-Taxonomie für Cybersicherheitsvorfälle.[7] Da die Taxonomie konzeptionell unterschiedlich ist und keine detaillierte Analyse von Lieferkettenvorfällen zulässt, empfehlen wir die komplementäre Verwendung beider Taxonomien.

[7] Cybersecurity incident taxonomy, Publications of the NIS Cooperation Group, Juli 2018. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. Zugriff am 28.7.2021.

2.2. ANGRIFFSTECHNIKEN ZUR KOMPROMITTIERUNG EINER LIEFERKETTE

Die Bezeichnungen der Angriffstechniken nehmen Bezug darauf, „wie“ der Angriff erfolgt ist, nicht aber, „was“ für den Angriff genutzt wurde. In dieser Kategorie wird beispielsweise unterschieden, ob der Lieferant mit einem online gefundenen Kennwort (OSINT, Informationsgewinnung aus frei zugänglichen Quellen) angegriffen wurde oder ob das Kennwort unter einfachem Ausprobieren zahlloser Kombinationen (Brute-Force-Angriff) ausfindig gemacht wurde. Für die Taxonomie ist allerdings auch unerheblich, ob das online gefundene Kennwort infolge eines Leaks erlangt, auf dem Schwarzmarkt angeboten oder als Standardkennwort erraten wurde. Die nachstehenden Kategorien von Angriffstechniken umfassen die häufigsten Angriffstechniken der in diesem Bericht analysierten Lieferkettenangriffe. Bei einem bestimmten Angriff können natürlich mehrere Techniken zum Einsatz gekommen sein, und in mehreren Fällen wissen die Entitäten möglicherweise nicht, wie sich die Angreifer Zugang zu ihrer Infrastruktur verschafft haben, bzw. die Informationen wurden nicht offengelegt oder unberechtigt mitgeteilt.

Tabelle 2: Angriffstechniken zur Kompromittierung von Lieferanten in der Lieferkette; bei den einzelnen Techniken wird beschrieben, wie der Angriff erfolgte, nicht aber, was angegriffen wurde. Bei ein und demselben Angriff können mehrere Techniken zum Einsatz gekommen sein.

ANGRIFFSTECHNIKEN ZUR KOMPROMITTIERUNG EINER LIEFERKETTE	
Infektion mit einem Schadprogramm	Beispielsweise Spyware, die eingesetzt wird, um Anmeldedaten von Mitarbeitern abzugreifen.
Social Engineering	Beispielsweise Phishing, gefälschte Bewerbungen, Typo-Squatting, Wi-Fi Impersonation, Veranlassen eines Lieferanten zu bestimmten Handlungen.
Brute-Force-Angriff	Beispielsweise Ausprobieren eines SSH-Kennworts oder eines Web-Logins.
Ausnutzen einer Sicherheitslücke in einer Software	Beispielsweise SQL Injection oder Ausnutzung eines Buffer-Overflow in einer Anwendung.
Ausnutzen einer Sicherheitslücke in einer Konfiguration	Beispielsweise Ausnutzen eines Konfigurationsproblems.
Physischer Angriff oder Modifikation	Beispielsweise eine Hardware-Modifikation oder physisches Eindringen.
Open-Source Intelligence (OSINT, Informationsgewinnung aus frei zugänglichen Quellen)	Beispielsweise Online-Suche nach Anmeldeinformationen, API-Schlüsseln und Benutzernamen.
Fälschung	Beispielsweise böswillige Imitation von USB-Medien.

2.3. LIEFERANTEN-ASSETS ALS GEGENSTAND VON LIEFERKETTENANGRIFFEN

Die Lieferanten-Assets, auf die der Angriff gerichtet ist, sind der Gegenstand („was"), auf den der Angriff auf einen Lieferanten abzielte und der weitere Angriffe ermöglichte. Die angegriffenen Assets stehen in der Regel in direktem Zusammenhang mit dem eigentlichen Ziel, und eine Analyse der Liste der betroffenen Assets gibt gewöhnlich

Aufschluss über die eigentlichen Absichten des Angreifers. Manchmal ist es allerdings nicht möglich, Informationen über die angegriffenen Assets zu erhalten, weil der Lieferant keine Informationen offengelegt oder mitgeteilt hat. Dies kann auch der Fall sein, wenn Lieferanten das Wissen oder die Erfahrung fehlen, um zu ermitteln, welche Assets von den Angreifern kompromittiert wurden.

Tabelle 3: Von Angreifern angegriffene Lieferanten-Assets; die Elemente geben jeweils an, was bei dem Lieferanten angegriffen wurde. Bei ein und demselben Angriff können mehrere Techniken eingesetzt werden, die sich auf mehrere Assets auswirken können.

LIEFERANTEN-ASSETS ALS GEGENSTAND VON LIEFERKETTENANGRIFFEN	
Bereits vorhandene Software	Beispielsweise die vom Lieferanten eingesetzte Software, Webserver, Anwendungen, Datenbanken, Überwachungssysteme, Cloud-Anwendungen oder Firmware; Software-Bibliotheken werden nicht dazu gezählt.
Software-Bibliotheken	Beispielsweise Bibliotheken von Dritten oder installierte Fremd-Software (npm, ruby, usw.).
Code	Beispielsweise Quellcode oder vom Lieferanten hergestellte Software.
Konfigurationen	Beispielsweise Kennwörter, API-Schlüssel, Firewall-Regeln oder URLs.
Daten	Beispielsweise Informationen über den Lieferanten, Werte von Sensoren, Zertifikate, personenbezogene Daten von Kunden oder von den Lieferanten selbst oder personenbezogene Daten.
Prozesse	Beispielsweise Aktualisierungen, Backups oder Validierungsprozesse und Signierungszertifikat-Prozesse.
Hardware	Beispielsweise vom Lieferanten hergestellte Hardware, Chips, Ventile und USB-Medien.
Menschen	Beispielsweise gezielte Angriffe auf bestimmte Personen mit Zugang zu Daten, Infrastruktur oder anderen Personen.

2.4. ANGRIFFSTECHNIKEN ZUR KOMPROMITTIERUNG EINES KUNDEN

Dieses Element der Taxonomie bezieht sich auf die Angriffstechniken, die darauf abzielen, einen Kunden über einen Angriff auf seinen Lieferanten zu kompromittieren. Mit diesem Element der Taxonomie wird ermittelt, „wie“ der Kunde angegriffen wurde, nicht aber, „was“ für den Angriff genutzt wurde. Es handelt sich um eine Technik und nicht um eine bestimmte Art von Angriff. Wenn der Kunde beispielsweise beim Aktualisieren seiner von einem Lieferanten bezogenen Software ein Schadprogramm herunterlädt, ist sowohl ein auf dem „Ausnutzen einer Vertrauensbeziehung“ beruhender Angriff als auch eine „Infektion mit einem Schadprogramm“ gegeben. Natürlich besteht die Möglichkeit, dass von Fall zu Fall nicht nur eine einzige Technik zur Anwendung kommt. Die Kunden haben nicht immer Kenntnis von der Technik, mit der sich die Angreifer über ihre Lieferanten Zugang zu ihren Assets verschafft haben, können aber feststellen, dass die verwendete Technik nicht vom eigenen Unternehmen ausging.

Tabelle 4: Angriffstechniken zur Kompromittierung von Kunden; bei den einzelnen Techniken wird beschrieben, wie der Angriff erfolgte, nicht aber, was angegriffen wurde. Bei ein und demselben Angriff können mehrere Techniken zum Einsatz gekommen sein.

ANGRIFFSTECHNIKEN ZUR KOMPROMITTIERUNG EINES KUNDEN	
Ausnutzen einer Vertrauensbeziehung [T1199]	Beispielsweise Vertrauen in ein Zertifikat, Vertrauen in eine automatische Aktualisierung oder Vertrauen in eine automatische Sicherung.
Drive-by Compromise [T1189]	Beispielsweise bösartige Skripte auf einer Website, um Nutzer mit einem Schadprogramm zu infizieren.
Phishing [T1566]	Beispielsweise Nachrichten, die scheinbar von einem Lieferanten stammen, oder gefälschte Aktualisierungsmeldungen.
Infektion mit einem Schadprogramm	Beispielsweise Fernzugriffstrojaner (Remote Access Trojan, RAT), Backdoor-Programme oder Ransomware.
Physischer Angriff oder Modifikation	Beispielsweise eine Hardware-Modifikation oder ein physisches Eindringen.
Fälschung	Beispielsweise Herstellung eines gefälschten USB-Mediums, Modifizierung einer Hauptplatine oder Ausgeben als Mitarbeiter eines Lieferanten.

2.5. KUNDEN-ASSETS ALS GEGENSTAND VON LIEFERKETTENANGRIFFEN

Die Kunden-Assets sind das wichtigste und eigentliche Ziel der Angreifer und in der Regel der Grund für einen Lieferkettenangriff. Diese Assets können je nach Branche und Art der angebotenen Dienstleistung unterschiedlich sein. In der Taxonomie soll dieses besondere Element die Auswirkungen eines Angriffs verständlicher machen und Vergleiche hinsichtlich der Ziele der Angreifer ermöglichen. Bestimmte Assets könnten von Angreifern unmittelbar angegriffen worden sein, während andere möglicherweise eher beiläufig in Mitleidenschaft gezogen werden. Die Auswirkungen von Lieferkettenangriffe beschränken sich in der Regel nicht auf einen einzigen Kunden. Möglicherweise ist dem Kunden auch nicht bewusst, dass er Ziel eines Angriffs war (z. B. weil der Angriff entweder fehlgeschlagen ist oder rasch entdeckt wurde).

Tabelle 5: Angegriffene Kunden-Assets; die Elemente geben jeweils an, was bei dem Kunden angegriffen wurde. Bei ein und demselben Angriff können mehrere Techniken zum Einsatz gekommen sein. Diese Assets sind in der Regel das eigentliche Ziel des Angriffs.

KUNDEN-ASSETS ALS GEGENSTAND VON LIEFERKETTENANGRIFFEN	
Daten	Beispielsweise Zahlungsdaten, Videoübertragungen, Dokumente, E-Mails, Flugpläne, Verkaufsdaten, Finanzdaten und geistiges Eigentum.
Personenbezogene Daten	Beispielsweise Kundendaten, Mitarbeiterdaten und Berechtigungsnachweise.

Software	Beispielsweise Zugriff auf den Quellcode des Kundenprodukts oder Modifikationen an der Software des Kunden.
Prozesse	Beispielsweise Dokumentation interner Betriebsabläufe und Konfigurationen, Einschleusen neuer Schadprozesse oder Dokumentation von Plänen oder Diagrammen.
Bandbreite	Beispielsweise die Belegung von Bandbreite für DDoS-Angriffe (Distributed Denial of Service), der Versand von Spam oder Infizieren von Drittsystemen in großem Maßstab.
Finanzieller Schaden	Beispielsweise das Stehlen von Kryptowährung oder das Kapern von Bankkonten oder Überweisungsprozessen.
Menschen	Beispielsweise Personen, die aufgrund ihrer Position oder ihres Wissens zu Zielen werden.

2.6. VERWENDUNG DER TAXONOMIE

Im Folgenden wird anhand eines Beispiels gezeigt, wie die Anwendung der Taxonomie auf einen konkreten Fall dazu beitragen kann, dessen besondere Merkmale zu ermitteln und leichter Aufschluss über die Merkmale des Angriffs zu erhalten.

Codecov ist ein Unternehmen, das Software zur Ermittlung der Codeabdeckung sowie Prüfwerkzeuge entwickelt. Das Unternehmen liefert Werkzeuge an andere Unternehmen wie IBM und Hewlett Packard Enterprise. Im April 2021 berichtete Codecov, dass Angreifer aufgrund eines Fehlers bei der Erstellung eines Docker-Images[8] einige ihrer gültigen Anmeldedaten aus einem Docker-Image erlangt hatten. Die Angreifer nutzten die entwendeten Anmeldedaten, um ein von Codecov-Kunden verwendetes „Upload-Bash-Skript“ zu kompromittieren.[9] Nachdem die Kunden dieses Skript heruntergeladen und ausgeführt hatten, konnten die Angreifer Daten der Codecov-Kunden abfangen, einschließlich sensibler Informationen, die den Angreifern Zugriff auf Ressourcen der Kunden ermöglichten.[10] Mehrere Codecov-Kunden berichteten, dass die Angreifer mithilfe der infolge des erfolgreichen Angriffs auf Codecov entwendeten Informationen in der Lage waren, auf ihren Quellcode zuzugreifen.[11] Der Angriff konnte keinen bestimmten Angreifern zugeordnet werden. In der folgenden Abbildung 1 sind die einzelnen Schritte bei diesem Angriff dargestellt.

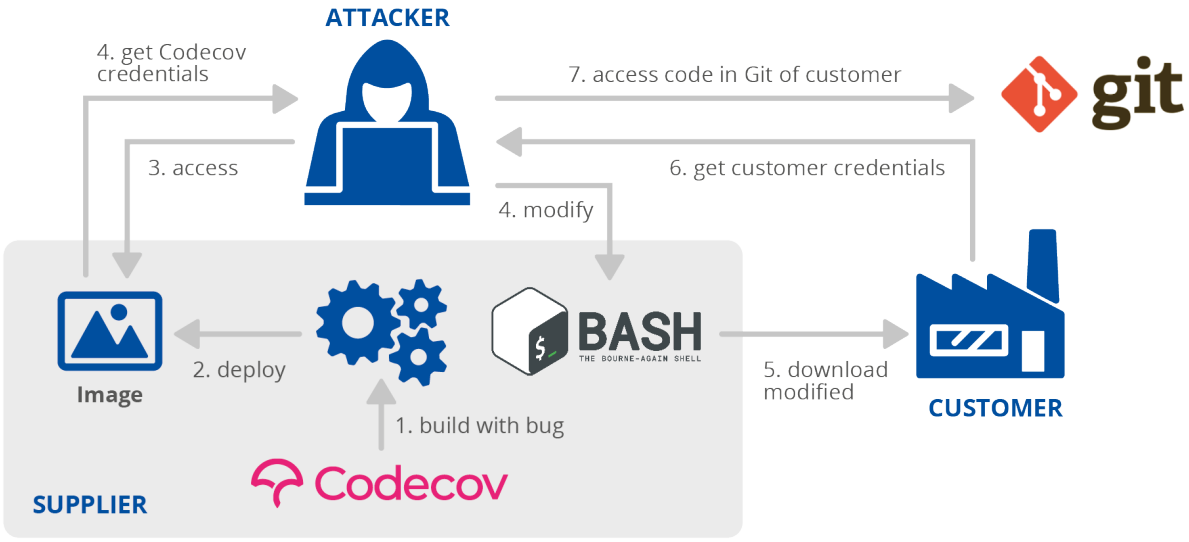
Anhand dieser Informationen können wir die vier Elemente der vorgeschlagenen Taxonomie ermitteln. Zunächst ist die Frage zu beantworten, „wie“ sich die Angreifer Zugang zu diesem Lieferanten verschafft haben − in diesem Fall durch „Ausnutzen einer Sicherheitslücke in einer Konfiguration“. Das Lieferanten-Asset, gegen das der Angriff gerichtet war, besteht in einem „Code“. Nachdem die in der Taxonomie definierten Elemente für den Lieferanten ermittelt wurden, können wir untersuchen, wie der Kunde angegriffen wurde. Bei Codecov erfolgte der Angriff durch „Ausnutzen einer Vertrauensbeziehung“ zum Lieferanten, die nicht abgesichert war und nicht überprüft wurde. Das eigentliche Kunden-Asset, auf das der Angriff abzielte, war den Angaben zufolge der Quellcode, also eine „Software“.

[8] Codecov supply chain attack breakdown, GitGuardian, https://blog.gitguardian.com/codecov-supply-chain-breach/. Zugriff am 27.6.2021.
[9] Bash Uploader Security Update, Codecov, https://about.codecov.io/security-update/. Zugriff am 27.6.2021.
[10] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Zugriff am 27.6.2021.
[11] Rapid7 Source Code Breached in Codecov Supply-Chain Attack, The Hacker News, https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html. Zugriff am 27.6.2021.

Tabelle 6: Taxonomie für Lieferkettenangriffe − Anwendung auf den Angriff auf das Unternehmen Codecov; die Angreifer nutzten eine Sicherheitslücke in einer Konfiguration bei Codecov aus, um den Code des Lieferanten zu verändern. Sie machten sich die Vertrauensbeziehung zwischen Codecov und seinen Kunden zunutze, um Daten abzufangen, die für den Zugriff auf den Software-Quellcode des Kunden erforderlich waren.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Konfiguration	Code	Ausnutzen einer Vertrauensbeziehung [T1199]	Software

Abbildung1: Grafische Darstellung des Lieferkettenangriffs auf Codecov; im Prozess der Container-Erstellung bei Codecov gab es einen Fehler, der auch in den online verfügbaren Containern vorhanden war (1). Die Angreifer verschafften sich Zugang zu dem Container und erlangten die Anmeldedaten für den Zugang zu Codecov (2). Anschließend änderten sie das Bash-Skript von Codecov (3), das bei den Kunden aktualisiert wurde (4). Über den Schadcode des Bash-Skripts wurden die Anmeldedaten des Kunden an den Angreifer weitergeleitet (5), der damit auf die Daten der Kunden zugriff (6).



2.7. LIEFERKETTENTAXONOMIE UND ANDERE RAHMENMODELLE

2.7.1. Die MITRE ATT&CK®-Wissensbasis

MITRE ATT&CK® ist eine kuratierte Wissensbasis und ein Modell für das Verhalten von Cyberangreifern. Die in diesem Bericht vorgeschlagene Taxonomie unterscheidet sich von der MITRE ATT&CK®-Taxonomie,[12] da mit beiden sehr unterschiedliche Zwecke verfolgt werden. Wir haben uns entschieden, vorrangig die vier Aspekte zu betrachten, die kennzeichnend für typische Lieferkettenangriffe und insbesondere für die Lieferanten-Kunden-Beziehung sind. Daher kann das MITRE ATT&CK®-Modell für die Lieferkettentaxonomie nicht herangezogen werden. MITRE

[12] MITRE ATT&CK®, MITRE, https://attack.mitre.org/. Zugriff am 8.7.2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

ATT&CK® bildet die Optionen und Schritte im Lebenszyklus aller Angriffe vollständig ab. Lieferketten werden mit diesem Modell jedoch noch nicht mit vergleichbarer Detailtiefe abgedeckt.

In der MITRE ATT&CK®-Kategorie „Initial Access“ beispielsweise gibt es die Technik „Supply Chain Compromise“.[13] Diese Kategorie ist sehr hilfreich, damit Unternehmen eine Lieferkette überhaupt als Risiko erkennen, aber zu allgemein, wenn es speziell um Lieferkettenangriffe geht. Die vorgeschlagene Taxonomie bildet alle Details des eigentlichen Lieferkettenangriffs ab und könnte daher die MITRE ATT&CK®-Wissensbasis ergänzen.

2.7.2. Das Cyber Kill Chain®-Modell von Lockheed Martin

Die vorgeschlagene Taxonomie hat auch einen anderen Zweck als das bekannte Cyber Kill Chain®-Modell von Lockheed Martin.[14] Die Cyber Kill Chain wurde als Rahmenmodell entwickelt, um zu ermitteln, mit welchen Schritten Angreifer ihre Ziele erreichen. Diese Schritte können zwar auch bei einem Lieferkettenangriff durchgeführt werden, sind aber zu allgemein, um Lieferkettenangriffe klassifizieren, verstehen und vergleichen zu können. Die hier vorgestellte Taxonomie ermöglicht eine detailliertere Analyse dieser Angriffe und bietet vor allem die Möglichkeit, beide Angriffe abzubilden, die jeweils bei einem Lieferkettenangriff erfolgen: den Angriff auf den Lieferanten und den Angriff auf den Kunden.

[13] Supply Chain Compromise, Technique T1195 – Enterprise, MITRE ATT&CK®, https://attack.mitre.org/techniques/T1195/. Zugriff am 8.7.2021.
[14] Cyber Kill Chain®, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Zugriff am 8.7.2021.

3. DER LEBENSZYKLUS VON LIEFERKETTENANGRIFFEN

Ein Lieferkettenangriff besteht in der Regel aus einem Angriff auf einen oder mehrere Lieferanten und einem anschließenden Angriff auf das eigentliche Ziel, nämlich den Kunden. Die Lebenszyklen dieser Angriffe können dem Lebenszyklus von APT-Angriffen sehr ähnlich sein.

Obwohl es schwierig ist, sich auf eine einheitliche Definition eines APT-Angriffs zu verständigen, wird in diesem Bericht davon ausgegangen, dass es sich bei einem APT-Angriff um einen gezielten Angriff handelt, mit dem unberechtigter Zugang zu einer Organisation erlangt wird (in der Regel durch die Ausführung von Code), der sich über einen langen Zeitraum erstreckt und dessen eigentliches Ziel in einem bestimmten Zusammenhang mit dem unmittelbaren Angriffsziel steht (anders als z. B. beim Kryptomining). Eine solche Definition ist natürlich nicht vollständig, und es kann noch viele weitere geben. Eine Definition ist jedoch wichtig, um zu verstehen, dass Lieferkettenangriffe in der Regel zielgerichtet, komplex und kostspielig sind und von den Angreifern wahrscheinlich von langer Hand geplant werden. Allein die Tatsache, dass bei typischen Lieferkettenvorfällen mindestens zwei Arten erfolgreicher Angriffe zum Tragen kommen, ist ein Indikator sowohl für die Ausgefeiltheit des Vorgehens der Angreifer als auch für ihre Hartnäckigkeit und ihre Erfolgsorientierung.

Viele APT-Angriffe wurden von der Community in Bezug auf die Qualität der Codes, der Exploits und der Schadprogramme als nicht „fortgeschritten“ eingestuft. Es kann jedoch davon ausgegangen werden, dass sich die Bewertung als „fortgeschritten“ auf das gesamte Vorgehen bezieht und nicht unbedingt auf den Code beschränkt. Letztendlich stellen die Planung, Ausgestaltung, Entwicklung und Durchführung von zwei Angriffen in zwei Organisationen eine komplexe Aufgabe dar.

Diese Unterscheidungen sind wichtig, um zu verstehen, **dass eine Organisation selbst dann für einen Lieferkettenangriff anfällig sein könnte, wenn sie selbst über recht gute Abwehrmechanismen verfügt**. Daher versuchen die Angreifer, neue mögliche Wege zu finden, um Organisationen zu infiltrieren, indem sich verstärkt auf deren Lieferanten konzentrieren und diese zum Ziel ihrer Angriffe machen. Außerdem werden mit Lieferkettenangriffen auf zahlreiche Kunden eines einzigen Lieferanten wahrscheinlich immense Auswirkungen erzielt. Dies ist ein weiterer Grund dafür, dass derartige Angriffe immer häufiger vorkommen: Angreifer können an Ansehen gewinnen und möglicherweise große finanzielle Gewinne erzielen.

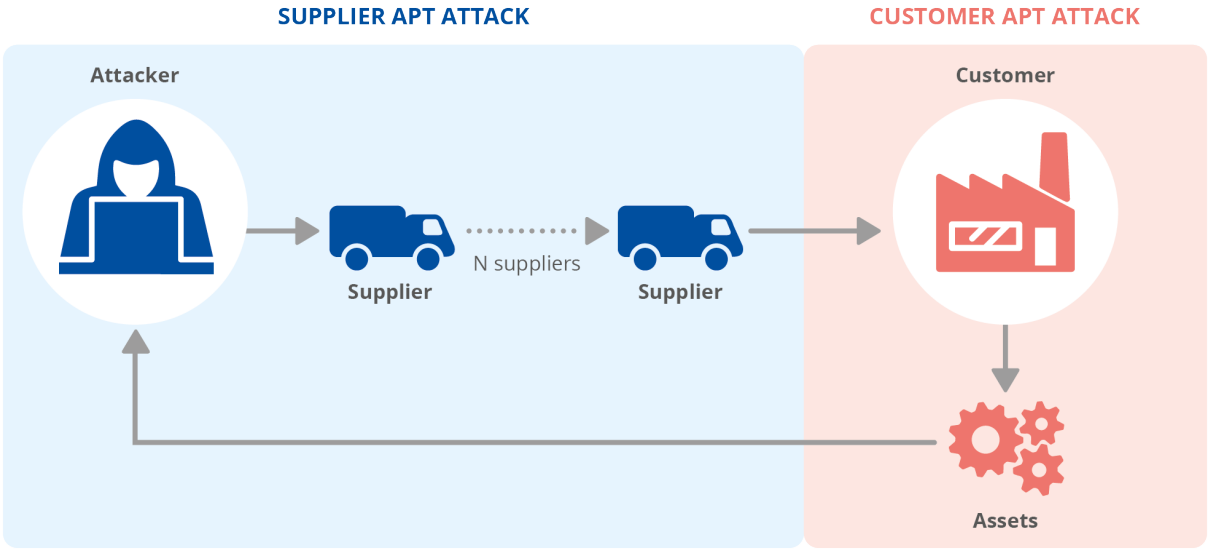
Weitere Merkmale von Lieferkettenangriffen sind die Komplexität ihrer Behandlung und die Anstrengungen, die zur Eindämmung und Bekämpfung solcher Angriffe erforderlich sind. Die bloße Tatsache, dass mindestens zwei Entitäten einer Organisation betroffen sind und höchstwahrscheinlich ausgefeilte Angriffsvektoren zum Einsatz kommen, erschwert die Behandlung eines Vorfalls sowie die forensische Analyse und die allgemeine Handhabung des Vorfalls. Da sich die Beziehungen zwischen Lieferanten und Kunden ständig weiterentwickeln und sowohl die Lieferanten als auch die Kunden ihre Systeme ständig aktualisieren, besteht die Notwendigkeit einer kontinuierlichen Aufrechterhaltung der Sicherheit der Lieferkette sowie einer aktiven Risikobewertung und eines aktiven Risikomanagements.

Der Lebenszyklus eines Lieferkettenangriffs besteht aus zwei Hauptteilen: dem Angriff auf den Lieferanten und dem Angriff auf den Kunden. Jeder dieser Angriffe ist in der Regel komplex und erfordert einen Angriffsvektor, einen Aktionsplan und eine sorgfältige Ausführung. Diese Angriffe können sich über Monate erstrecken, und in vielen Fällen können sie lange Zeit unentdeckt bleiben. Der Lebenszyklus eines Lieferkettenangriffs ist in Abbildung 2 dargestellt.

Der erste Angriff im Lebenszyklus wird als „APT-Lieferantenangriff“ bezeichnet und zielt auf die Kompromittierung eines oder mehrerer Lieferanten ab. Der zweite Angriff im Lebenszyklus wird als „APT-Kundenangriff“ bezeichnet und richtet sich auf die Kompromittierung eines oder mehrerer Kunden. Diese beiden Elemente stehen über den Zugang

zum Lieferanten miteinander in Verbindung, können sich ansonsten hinsichtlich der verwendeten Techniken, der genutzten Angriffsvektoren und des Zeitaufwands aber stark unterscheiden.

Abbildung 2: Der Lebenszyklus eines Lieferkettenangriffs kann als aus zwei miteinander verbundenen APT-Angriffen bestehend betrachtet werden. Der erste Angriff richtet sich auf einen oder mehrere Lieferanten, der zweite auf die Kunden. Diese Angriffe erfordern eine sorgfältige Planung und Ausführung.



In mindestens elf der in diesem Bericht untersuchten Fälle bestätigten die Untersuchungen, dass die Lieferkettenangriffe von bekannten APT-Gruppen durchgeführt wurden. Diese Zuschreibungen wurden von den Sicherheitsunternehmen vorgenommen, von denen die in Anhang A genannten Berichte stammen. In den anderen 13 Fällen wurden die Vorfälle nicht vollständig untersucht oder eine Zuordnung war nicht möglich. Die Zuschreibungen sprechen für die Vermutung, dass beide Teile des Lebenszyklus eines Lieferkettenangriffs in ihrer Wirkungsweise APT-Angriffen ähneln können. Es ist darauf hinzuweisen, dass die Zuordnung von Angreifern sehr schwierig, fehlerträchtig, ungenau und politisch schwierig, aber nicht unmöglich ist.

Da die Bestandteile eines Lieferkettenangriffs jeweils als APT-Angriff betrachtet werden können, ist davon auszugehen, dass deren individueller Lebenszyklus im Allgemeinen die gleichen Phasen durchläuft wie auch andere APT-Angriffe. Diese Phasen werden zum Beispiel in den MITRE ATT&CK® Tactics for Enterprises detailliert beschrieben.[15]

[15] MITRE ATT&CK® Tactics − Enterprise Version 9, MITRE, https://attack.mitre.org/tactics/enterprise/. Zugriff am 29.6.2021.

4. AUFSEHENERREGENDE LIEFERKETTENANGRIFFE

Dieser Abschnitt enthält eine Zusammenfassung der wichtigsten Lieferkettenangriffe von Januar 2020 bis Anfang Juli 2021 sowie eine Klassifizierung gemäß der vorgeschlagenen Taxonomie. Diese Fälle wurden ausgewählt, weil sie in der Community erhebliche Auswirkungen hatten oder weil daran bestimmte (in den Elementen der Taxonomie beschriebene) wichtige Merkmale deutlich werden. Anhang A enthält eine vollständige Aufstellung aller Lieferkettenangriffe von Januar 2020 bis Anfang Juli 2021 einschließlich der jeweiligen Beschreibungen.

4.1. SOLARWINDS ORION: IT-MANAGEMENT UND ELEKTRONISCHE ÜBERWACHUNG

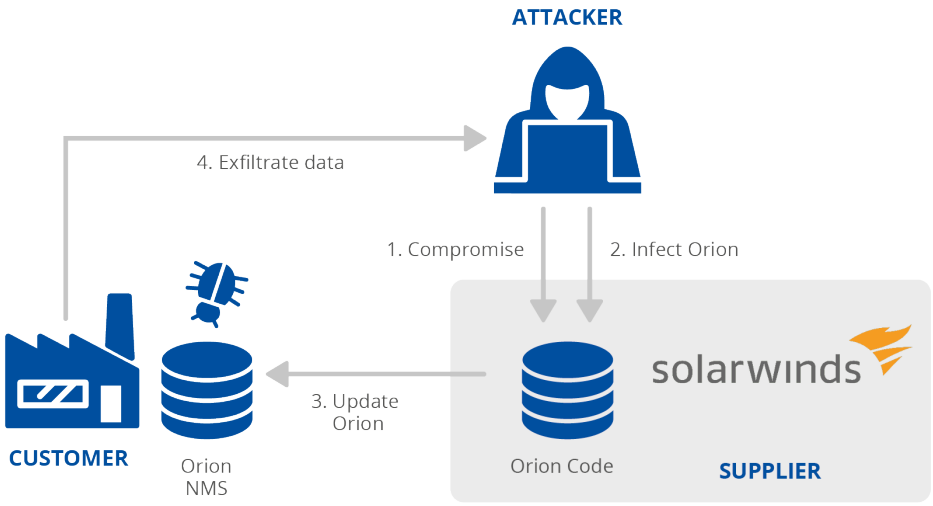
SolarWinds ist ein Anbieter von Management- und Überwachungssoftware.[16] Ein Produkt des Unternehmens ist das Netzverwaltungssystem (NMS, Network Management System) Orion.[17] Im Dezember 2020 wurde entdeckt, dass Orion kompromittiert worden war. In einer umfassenden Untersuchung wurde festgestellt, dass sich Angreifer Zugang zum SolarWinds-Netzwerk verschafft hatten, möglicherweise durch Ausnutzen einer Zero-Day-Sicherheitslücke in einer Anwendung oder einem Gerät eines Drittanbieters, durch einen Brute-Force-Angriff oder durch Social Engineering. Nach dem Eindringen in das Netz sammelten die Angreifer über einen längeren Zeitraum Informationen. Die Schadsoftware wurde über den Build-Prozess in Orion eingeschleust.[18, 19] Die kompromittierte Software wurde dann von den Kunden direkt heruntergeladen und kam zum Sammeln und Abgreifen von Informationen zum Einsatz.[20] Der Angriff wurde der Gruppe APT29 zugeschrieben.[21,22]

Tabelle 7: Taxonomie für Lieferkettenangriffe − Anwendung auf den Angriff auf SolarWinds; die Angreifer nutzten mehrere Angriffstechniken, um die Orion-Software von SolarWinds zu kompromittieren. Sie modifizierten den Code des Lieferanten und machten sich die Vertrauensbeziehung der Kunden zu SolarWinds zunutze, um Schadprogramme an die Kunden zu verteilen. Eigentliches Ziel der Angreifer waren die Daten der Kunden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Software Brute-Force-Angriff Social Engineering	Prozesse, Code	Ausnutzen einer Vertrauensbeziehung [T1199] Infektion mit einem Schadprogramm	Daten

[16] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Zugriff am 8.7.2021.
[17] Orion Platform − Scalable IT Monitoring, SolarWinds, https://www.solarwinds.com/solutions/orion. Zugriff am 8.7.2021.
[18] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Zugriff am 8.7.2021.
[19] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Zugriff am 8.7.2021.
[20] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Zugriff am 8.7.2021.
[21] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Zugriff am 8.7.2021.
[22] Russian hacker group 'Cozy Bear' behind Treasury and Commerce breaches, The Washington Post, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html. Zugriff am 8.7.2021.

Abbildung 3: Grafische Darstellung des Lieferkettenangriffs auf SolarWinds; die Angreifer kompromittierten SolarWinds und modifizierten den Code der Orion-Software. Die Orion-Instanzen bei den Kunden wurden mit Schadsoftware aktualisiert, die den Angreifern ermöglichte, auf die Daten der Kunden zuzugreifen.



4.2. MIMECAST: CYBERSICHERHEITSDIENSTE IN DER CLOUD

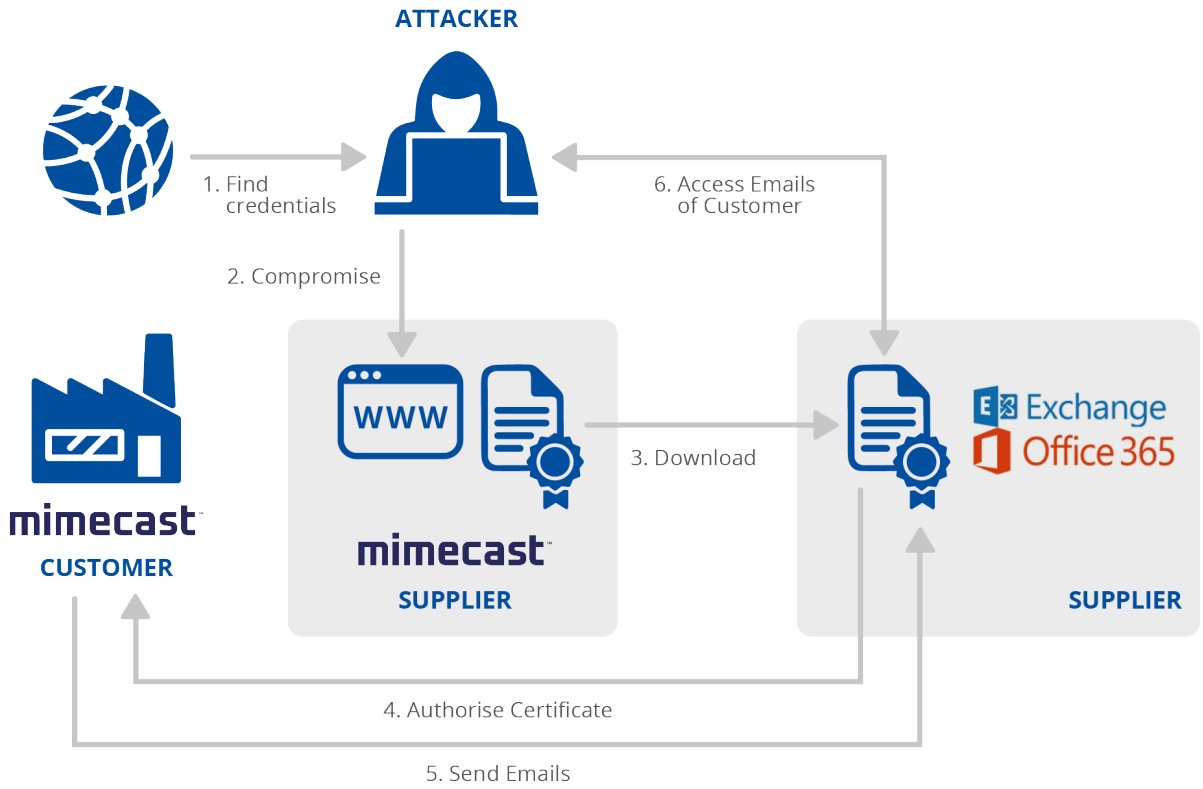
Mimecast ist ein Anbieter von Cloud-basierten Cybersicherheitsdiensten. Das Unternehmen vertreibt unter anderem E-Mail-Sicherheitsdienste an, bei denen die Kunden eine sichere Verbindung zu den Mimecast-Servern herstellen müssen, damit sie ihre Microsoft-365-Konten nutzen können. Im Januar 2021 wurde entdeckt, dass Angreifer Mimecast (über den Lieferanten SolarWinds) kompromittiert hatten. Nach der Kompromittierung hatten die Angreifer Zugriff auf ein von Mimecast ausgestelltes und von Kunden für den Zugriff auf Microsoft-365-Dienste verwendetes Zertifikat. Anschließend konnten sie die Netzwerkverbindungen abfangen und sich mit den Microsoft-365-Konten verbinden, um Informationen abzugreifen.[23, 24] Der Angriff wurde der Gruppe APT29 zugeschrieben.[25] Die Kompromittierung des Lieferanten wurde Berichten zufolge mit SolarWinds in Verbindung gebracht, es liegen jedoch keine konkreten Informationen vor, die zu einer Überprüfung herangezogen werden könnten.

Tabelle 8: Taxonomie für Lieferkettenangriffe − Anwendung auf den Angriff auf Mimecast; es ist nicht bekannt, wie die Angreifer ihren Angriff auf die Lieferanten ausgeführt haben. Insbesondere ist unklar, wie der Angriff auf ein von Mimecast ausgestelltes Zertifikat erfolgte. Die Angreifer machten sich die Vertrauensbeziehung der Kunden zunutze, die ihre Daten zu Mimecast hochladen. Sie verschafften sich Zugang zu den Daten der Kunden von Mimecast.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Daten	Ausnutzen einer Vertrauensbeziehung [T1199]	Daten

[23] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/ Zugriff am 8.7.2021..
[24] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Zugriff am 8.7.2021.
[25] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Zugriff am 8.7.2021.

Abbildung 4: Grafische Darstellung des Lieferkettenangriffs auf Mimecast; die Angreifer erlangten Zugriff auf Anmeldeinformationen, die ihnen ermöglichten, den Lieferanten zu kompromittieren und auf seine Zertifikate zuzugreifen. Anschließend verwenden sie die Zertifikate, um auf Kundendaten zuzugreifen, nachdem der Kunde das Zertifikat validiert und als vertrauenswürdig eingestuft hatte.



4.3. LEDGER: HARDWARE-WALLETS

Ledger ist ein Unternehmen, das Hardware-Wallet-Technologie für Kryptowährungen liefert. Im Juli 2020 verschafften sich Angreifer gültige Anmeldedaten, um auf die E-Commerce-Datenbank von Ledger zuzugreifen.[26] Die gestohlenen Daten wurden in einem Online-Forum veröffentlicht.[27] Die Angreifer nutzten die gestohlenen Daten für Online-Phishing und für die Erpressung von Nutzern[28, 29] sowie für den Diebstahl von Geldern der Nutzer durch einen physischen Angriff. Dazu übermittelten sie den Nutzern gefälschte Ledger-Wallets, die nach dem Aufbau einer Verbindung zu einem System die Nutzer nach ihren Sicherheitsschlüsseln fragten, das System mit einem Schadprogramm infizierten und die gestohlenen Informationen an die Angreifer zurückschickten[30]. Der Angriff konnte nicht zugeordnet werden.

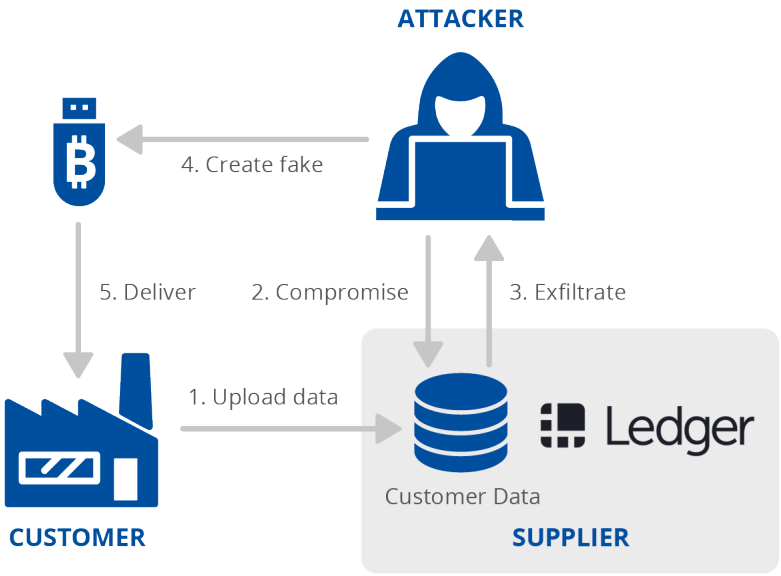
Tabelle 9: Taxonomie für Lieferkettenangriffe − Anwendung auf den Angriff auf Ledger; die Angreifer nutzten OSINT-Techniken (Open Source Intelligence = Informationsgewinnung aus frei zugänglichen Quellen), um gültige Anmeldeinformationen für den Zugriff auf Ledger-Datensätze zu finden und Kundendaten abzugreifen. Mit diesen

[26] Addressing the July 2020 e-commerce and marketing data breach − A Message From Ledger's Leadership, Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Zugriff am 8.7.2021.
[27] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577 Zugriff am 8.7.2021.
[28] Message by LEDGER's CEO − Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Zugriff am 8.7.2021.
[29] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, Bitdefender HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html, Zugriff am 8.7.2021.
[30] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Zugriff am 8.7.2021.

Daten machten sich die Angreifer das Vertrauensverhältnis der Kunden zu Ledger zunutze, indem sie Phishing-Mails und gefälschte USB-Medien mit Crypto-Wallets verschickten, um Kryptowährungen von den Kunden zu stehlen.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
OSINT	Daten	Ausnutzen einer Vertrauensbeziehung [T1199] Phishing [T1566], Fälschung	Finanzieller Schaden

Abbildung 5: Grafische Darstellung des Lieferkettenangriffs auf Ledger; die Angreifer gelangten über das Netz an die Anmeldedaten bei Ledger, griffen auf die Kundendatenbank zu und nutzten die Informationen, um die Kunden anzugreifen.



4.4. KASEYA: KOMPROMITTIERUNG VON IT-MANAGEMENT-DIENSTEN DURCH RANSOMWARE

Kaseya ist ein Software-Dienstleister, der sich auf Tools für die elektronische Überwachung und Verwaltung spezialisiert hat. Das Unternehmen bietet seinen Kunden VSA-Software (Virtual System/Server Administrator) zum Herunterladen an und eröffnet die Möglichkeit, auch über seine eigenen Cloud-Server zu arbeiten. MSPs (Managed Service Providers) können die VSA-Software vor Ort nutzen oder Lizenzen für die VSA-Cloud-Server von Kaseya erwerben. MSPs bieten ihrerseits anderen Kunden verschiedene IT-Dienste an.[31] Im Juli 2021 nutzten Angreifer eine Zero-Day-Sicherheitslücke in Kaseyas eigenen Systemen (CVE-2021-30116)[32] aus, über die die Angreifer aus der Ferne Befehle auf den VSA-Appliances von Kaseya-Kunden ausführen lassen konnten. Kaseya kann Remote-Updates an alle VSA-Server senden. Am Freitag, dem 2. Juli 2021, wurde ein Update an die VSAs der Kaseya-

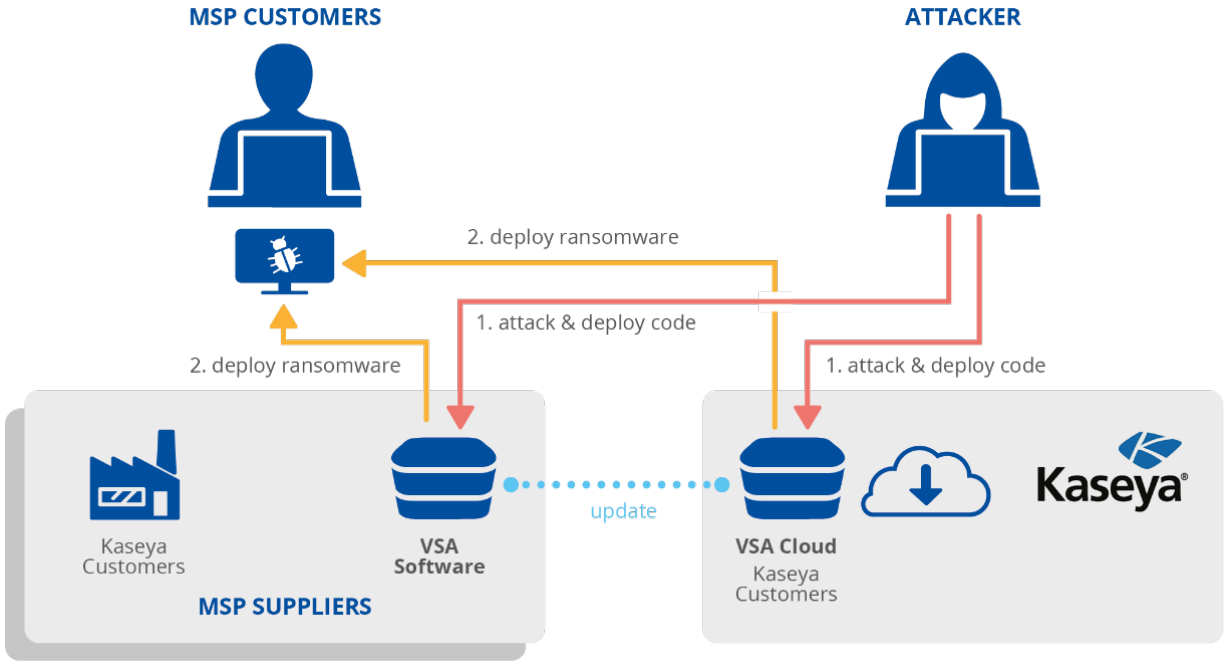
[31] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Zugriff am 8.7.2021.
[32] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116. Zugriff am 8.7.2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Kunden verteilt, mit dem von den Angreifern eingeschleuster Programmcode ausgeführt wurde. Dieses Schadprogramm bewirkte die Installation von Ransomware[33, 34] bei von dieser VSA verwalteten Kunden.

Tabelle 10: Taxonomie für Lieferkettenangriffe − Anwendung auf den Angriff auf Kaseya; durch Ausnutzen einer Software-Sicherheitslücke verschafften sich Angreifer Zugang zu Software von Kaseya. Über diesen Zugang installierten die Angreifer Ransomware auf der Infrastruktur von Kaseya-Kunden. Der Angriff zielte auf die Daten sowie (durch Lösegeldforderungen) auf die finanziellen Ressourcen der Kunden von Kaseya ab.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Software	Bereits vorhandene Software	Ausnutzen einer Vertrauensbeziehung [T1199] Infektion mit einem Schadprogramm	Daten, finanzieller Schaden

Abbildung 6: Grafische Darstellung des Lieferkettenangriffs auf Kaseya; die Angreifer schleusten Code in VSA-Instanzen von MSP-Anbietern ein (ob in der Cloud oder vor Ort, wird noch geprüft). Über einige dieser MSPs wurden Schadprogramme und Ransomware bei deren Kunden installiert.



4.5. EIN BEISPIEL MIT VIELEN UNBEKANNTEN: DAS FLUGGASTABFERTIGUNGSSYSTEM SITA

Der Fall SITA ist aufgrund der vielen noch **nicht bekannten** Bestandteile von Lieferkettenangriffen und der möglichen Folgen dieser Angriffe von besonderer Bedeutung. Er zeigt, dass es häufig Umstände geben kann, unter denen die Einzelheiten von Angriffen nie veröffentlicht werden, weil dies technisch nicht möglich ist oder weil einer

[33] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/. Zugriff am 8.7.2021.
[34] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Zugriff am 8.7.2021.

Veröffentlichung politische oder marketingbezogene Erwägungen der Unternehmen entgegenstehen Dabei ist zwischen dem Nutzen für die Community mit Blick auf die Möglichkeit einer Verbesserung des Sicherheitsniveaus durch Erkenntnisgewinne aus detaillierten Informationen über die Kompromittierung anderer und dem Nutzen für die jeweiligen Unternehmen (z. B. finanzieller Art, in Bezug auf die Wahrung ihres Ansehens oder im Hinblick auf den Markt) abzuwägen.[35]

SITA ist ein Unternehmen, das sich auf IT-Anwendungen für den Luftverkehr und auf Verkehrsinformationen spezialisiert hat. Das Fluggastabfertigungssystem von SITA dient dazu, den Fluggesellschaften beim Boarding Informationen über die Fluggäste zu liefern, u. a. zum Risiko, das die Fluggäste für ein Land darstellen könnten.[36]

Im März 2021 wurde bekannt, dass Angreifer in die SITA-Server eingedrungen waren, um sich Zugang zu den Passagierdaten der Kunden von SITA zu verschaffen. Zudem meldeten einige Kunden von SITA Datenschutzverletzungen, u. a. Air India, Singapore Airlines und Malaysia Airlines.[36]

Nach Berichten über Datenverluste im Internet meldete auch Air India, dass seine Netzwerke kompromittiert und Daten gestohlen wurden.[37] Bei der Kompromittierung der internen Netzwerke von Air India wurde ein Zusammenhang mit dem Vorfall bei SITA vermutet, da ein Sicherheitsunternehmen feststellte, dass ein System von Air India die Bezeichnung „SITASERVER4“ trug. Bislang ist weder bekannt, wie die Angreifer auf die SITA-Server zugreifen konnten, noch, wie sich die Angreifer Zugang zu Air India verschafft haben könnten oder ob ihnen dies tatsächlich gelungen ist. Der interne Angriff auf die Netzwerke von Air India wurde der Gruppe APT41 zugeschrieben.[37]

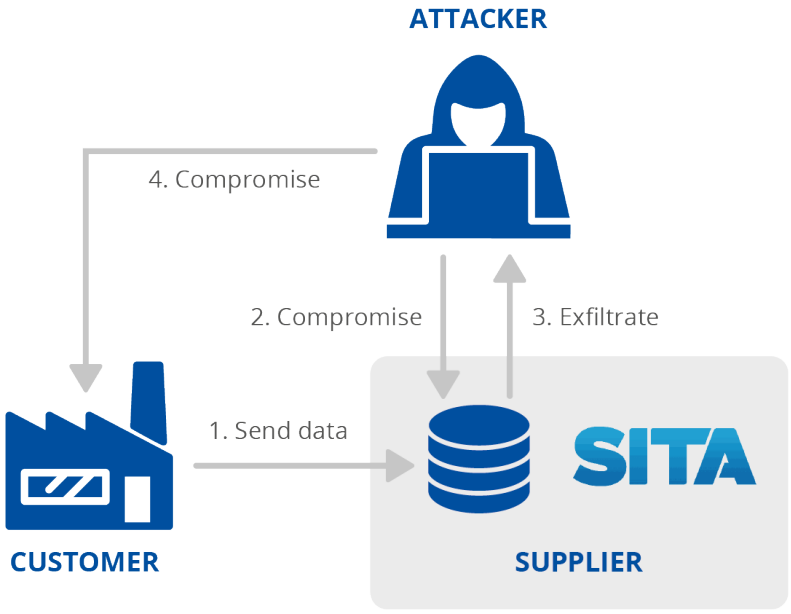
Die Anzahl der unbekannten Variablen bei diesem Vorfall ist typisch für die Bedrohungslage bei Lieferkettenangriffen. Bei vielen Organisationen sollten sich die Untersuchung von Cyberbedrohungen und die entsprechenden Vorbereitungen angesichts der komplexen wechselweisen Beziehungen mit den Lieferanten auch auf diese erstrecken.

Tabelle 11: Taxonomie für Lieferkettenangriffe − Anwendung auf den Angriff auf SITA; es ist nicht bekannt, wie sich die Angreifer Zugang zu dem Lieferanten verschafft haben. Die Angreifer verschafften sich Zugang zu den Kundendaten des Lieferanten. Es ist nicht bekannt, wie es den Angreifern gelang, bei Air India einzudringen. Die vorliegenden Informationen deuten darauf hin, dass das eigentliche Ziel der Angreifer die Kundendaten waren.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Daten	Unbekannt	Personenbezogene Daten

[35] Investors in SolarWinds sold millions in stock before Russia breach revealed, The Washington Post, https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/. Zugriff am 9.7.2021.
[36] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Zugriff am 8.7.2021.
[37] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Zugriff am 8.7.2021.

Abbildung 7: Grafische Darstellung des Lieferkettenangriffs auf SITA; die Angreifer entwendeten Passagierdaten von den Unternehmenskunden von SITA. Bislang ist weder bekannt, wie die Angreifer auf die SITA-Server zugreifen konnten, noch, wie sich die Angreifer Zugang zu Air India verschafft haben könnten oder ob ihnen dies tatsächlich gelungen ist.



5. ANALYSE DER LAGE IM HINBLICK AUF LIEFERKETTENVORFÄLLE

Dieser Abschnitt enthält eine Analyse der Lage im Hinblick auf Lieferkettenangriffe anhand von Angriffen, die von Anfang 2020 bis Anfang Juli 2021 gemeldet wurden. Die Analyse konzentriert sich auf öffentlich bekannte Lieferkettenangriffe. Eine detaillierte Übersicht ist Anhang A zu entnehmen. Wie später noch erörtert wird, wurden einige Angriffe fälschlicherweise als Lieferkettenangriffe eingestuft und daher nicht in die Analyse einbezogen. Tabelle 12 enthält eine Zusammenfassung aller im Bericht analysierten Vorfälle.

Tabelle 12: Die von Januar 2020 bis Anfang Juli 2021 ermittelten, analysierten und validierten Lieferkettenangriffe im Überblick

LIEFERANT	LIEFERANTENKATEGORIE	JAHR	WIRKUNG	ZUSCHREIBUNG ZU GRUPPE
Mimecast	Sicherheitssoftware	2021	Global	APT29
SITA	Luftfahrt	2021	Global	APT41
Ledger	Blockchain	2021	Global	-
Verkada	Physische Sicherheit	2021	Global	Hacktivisten-Gruppe
BigNox NoxPlayer	Software	2021	Regional	-
Stock Investment Messenger	Finanzsoftware	2021	Regional	Thallium APT
ClickStudios	Sicherheitssoftware	2021	Regional	-
Apple Xcode	Entwicklungssoftware	2021	Global	-
Website der Regierung von Myanmar	Öffentliche Verwaltung	2021	Regional	Mustang Panda APT
Ukraine SEI EB	Öffentliche Verwaltung	2021	Regional	-
Codecov	Unternehmenssoftware	2021	Global	-
Fujitsu ProjectWEB	Zusammenarbeit in der Cloud	2021	Regional	-
Kaseya	IT-Management	2021	Global	REvil Group
MonPass	Zertifizierungsbehörde	2021	Regional	Winnti APT Group
SYNNEX	Anbieter von Technologieprodukten	2021	Regional	APT 29
Microsoft Windows HCP	Software	2021	Global	-
SolarWinds	Cloud-Management	2020	Global	APT29
Accellion	Sicherheitssoftware	2020	Global	UNC2546
Wizvera VeraPort	Identitätsmanagement	2020	Regional	Lazarus APT
Able Desktop	Unternehmenssoftware	2020	Regional	TA428
Aisino	Finanzsoftware	2020	Regional	-
Vietnam VGCA	Zertifizierungsbehörde	2020	Regional	TA413, TA428
NetBeans	Entwicklungssoftware	2020	Global	-

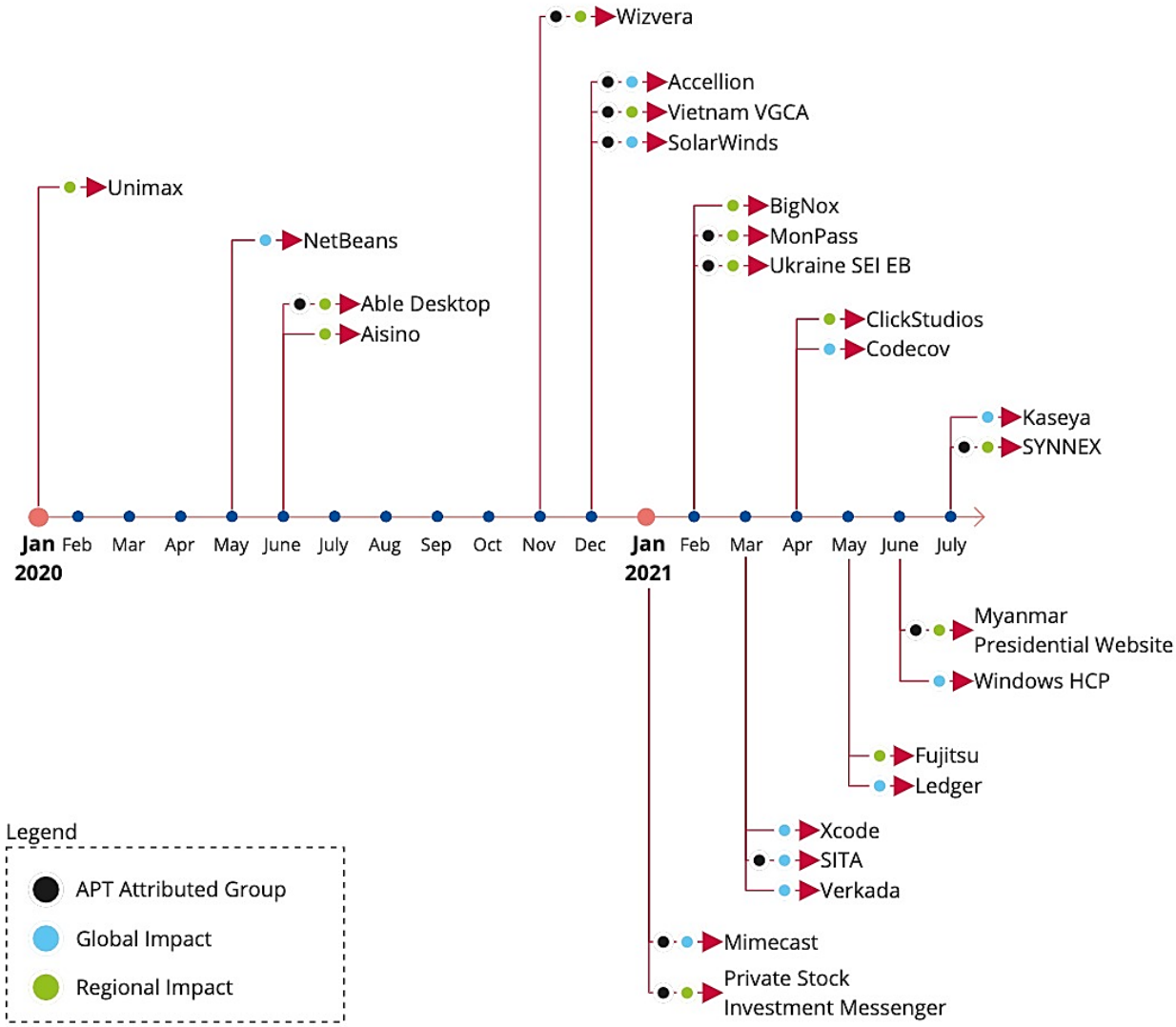
Unimax	Telekommunikation	2020	Regional	-

5.1. LIEFERKETTENANGRIFFE IN DER ZEITLEISTE

Die Analyse zeigt, dass von den 24 bestätigten Angriffen auf die Lieferkette acht (33 %) im Jahr 2020 und 16 (66 %) von Januar 2021 bis Anfang Juli 2021 gemeldet wurden. **Auf der Grundlage dieser Daten wird erwartet, dass es 2021 viermal mehr Lieferkettenangriffe geben könnte als 2020.**

Auf der Zeitleiste in Abbildung 8 sind die in diesem Bericht analysierten Angriffe dargestellt. Dabei wird angegeben, welche Vorfälle APT-Gruppen zugeschrieben wurden, und ob sie globale oder regionale Auswirkungen hatten. Die Auswirkungen werden bei jedem Angriff als global oder regional eingestuft. Globale Auswirkungen werden bei Angriffen dann als gegeben betrachtet, wenn das Unternehmen weltweit Kunden hat oder wenn die Zahl der möglicherweise betroffenen Endnutzer im Millionenbereich liegt. Für Angriffe, die sich auf Nutzer in einer bestimmten Region oder einem bestimmten Land auswirken oder nur einige Nutzer betreffen, werden hingegen Auswirkungen auf regionaler Ebene angenommen.

Abbildung 8: Zeitleiste der von Januar 2020 bis Anfang Juli 2021 gemeldeten Lieferkettenangriffe; in der Abbildung bezeichnen die Monate jeweils den Zeitpunkt der Meldung eines Vorfalls (und nicht der Zeitpunkt, zu dem der Angriff stattfand). APT-Gruppen zugeschriebene Vorfälle sind mit schwarzen Punkten, Vorfälle mit globalen Auswirkungen mit violetten Punkten und Vorfälle mit regionalen Auswirkungen mit grünen Punkten gekennzeichnet. Anhang A enthält detaillierte Zusammenfassungen der einzelnen Vorfälle.



5.2. ERLÄUTERUNG DES ABLAUFS DER ANGRIFFE

Die in Abbildung 7 dargestellten Vorfälle wurden jeweils analysiert, zusammenfassend beschrieben und nach der vorgeschlagenen Taxonomie klassifiziert. Die Taxonomie unterstützt und erleichtert eine strukturierte und umfassende Untersuchung von Lieferkettenangriffen.

Abbildung 8 besteht in einem Sankey-Diagramm[38], in dem die Flüsse der Angriffstechniken und -mittel dargestellt werden, die bei den in diesem Bericht untersuchten Lieferkettenangriffen am häufigsten beobachtet wurden. **Gegen Lieferanten gerichtete Angriffstechniken [Techniques used to attack Suppliers, ST] zielen auf Lieferanten-Assets [Supplier Assets, SA] ab, die dann wiederum für auf Kunden abzielende Angriffstechniken [Techniques used to attack Customers, CT] zur Kompromittierung von Kunden-Assets [Customer Assets, CA] genutzt werden.**

[38] Sankey-Diagramme sind eine besondere Form von Flussdiagrammen, bei denen die Flussmengen proportional durch die Breite der Pfeile dargestellt werden.

Aus Abbildung 8 ist ersichtlich, dass die meisten Angriffstechniken zur Kompromittierung von Lieferanten (Spalte 1 [ST]) verwendet werden:

- **Unbekannt (66 %)**; an zweiter Stelle stehen
- **Angriffe zur Ausnutzung von Software-Sicherheitslücken (16 %)**.

Durch die Angriffe auf Lieferanten-Assets (Spalte 2 [SA]) sollte meist Folgendes kompromittiert werden:

- **Code (66 %)**,
- **Daten (20 %) und**
- **Prozesse (12 %)**.

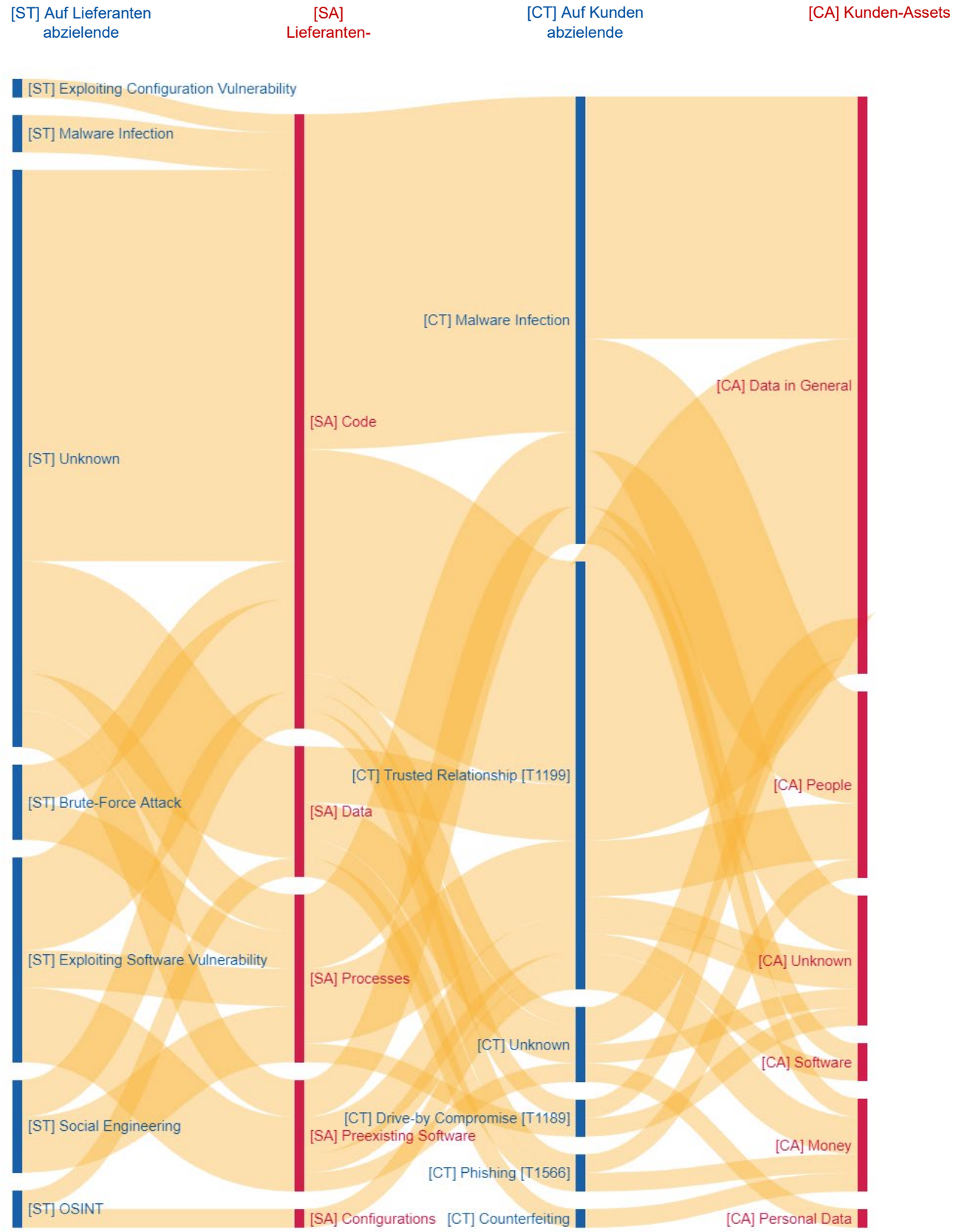
Die kompromittierten Lieferanten-Assets werden als Angriffsvektoren genutzt, um die Kunden zu kompromittieren. Diese Angriffe werden größtenteils mit folgenden Mitteln ausgeführt (Spalte 3 [CT]):

- durch **Ausnutzen des Vertrauens der Kunden (62 %)** in den Lieferanten oder
- durch den Einsatz von **Schadprogrammen (62 %)**.

Unabhängig von der verwendeten Technik zielen die meisten Lieferkettenangriffe darauf ab, Zugang zu Folgendem zu erlangen (Spalte 4 [CA]):

- **Daten** der Kunden **(58 %)**,
- wichtigen **Personen (16 %)** und
- **Finanzmitteln (8 %)**.

Abbildung 9: Analyse von Lieferkettenvorfällen auf der Grundlage der vorgeschlagenen Taxonomie; im Sankey-Diagramm werden die Flüsse von gegen Lieferanten gerichteten Angriffstechniken [Techniques used to attack Suppliers, ST] dargestellt, die auf Lieferanten-Assets [Supplier Assets, SA] abzielen, die wiederum für auf Kunden abzielende Angriffstechniken [Techniques used to attack Customers, CT] zur Kompromittierung von Kunden-Assets [Customer Assets, CA] genutzt werden. Die Verbindungen zwischen den verschiedenen Elementen werden umso breiter dargestellt, je häufiger sie bei Lieferkettenangriffen festzustellen waren.



5.3. ZIELORIENTIERTE ANGREIFER

Hinsichtlich der angegriffenen Assets ist festzustellen, dass sich die Angreifer bei **66 %** der Vorfälle auf **Code** der Lieferanten konzentrierten, um so die eigentlich im Fokus stehenden Kunden zu kompromittieren. Bei **20 %** der

analysierten Vorfälle ging es den Angreifern um **Daten**, und bei **12 %** waren **interne Prozesse** Ziel des Angriffs auf die Lieferanten. Dies ist entscheidend, um nachvollziehen zu können, worauf sich die Bemühungen um den Schutz der Cybersicherheit konzentrieren sollten. Organisationen sollten ihre Kräfte vor allem darauf verwenden, durch eine geeignete Validierung sicherzustellen, dass Code und Software von Dritten nicht manipuliert werden.

Die Kunden-Assets, auf die sich die Angriffe richteten, scheinen bei diesen Lieferkettenangriffen in erster Linie Kundendaten, einschließlich personenbezogener Daten und geistigen Eigentums, gewesen zu sein. Dies gilt für 58 % der untersuchten Lieferkettenvorfälle. In geringerem Maße ging es bei den Angriffen um sonstige Assets (u. a. Menschen, Software und finanzielle Ressourcen).

5.4. DIE MEISTEN ANGRIFFSVEKTOREN ZUR KOMPROMITTIERUNG VON LIEFERANTEN SIND NICHT BEKANNT

Unsere Ergebnisse zeigen, dass bei **66 %** der untersuchten Lieferkettenangriffe die **Lieferanten nicht wussten**, wie sie kompromittiert wurden, bzw. diesbezügliche Informationen nicht offenlegten. Bei den Kunden, die durch Angriffe auf die Lieferkette kompromittiert wurden, wussten hingegen weniger als **9 %** nicht, wie die Angriffe erfolgt waren. **Entsprechend besteht hinsichtlich der Qualität der Berichterstattung über Cybersicherheitsvorfälle bei Lieferanten und bei mit den Endnutzern konfrontierten Unternehmens ein erheblicher Unterschied.**

Da **83 %** der Lieferanten im **Technologie**sektor tätig sind, könnte das fehlende Wissen darüber, wie die Angriffe durchgeführt wurden, entweder darauf zurückzuführen sein, dass die Cyberabwehr in der Infrastruktur der Lieferanten **nicht hinreichend ausgereift** war oder keine Bereitschaft zur Weitergabe der entsprechenden Informationen bestand. Darüber hinaus könnten noch weitere Faktoren dazu beitragen, dass nicht verstanden wird, wie Lieferanten kompromittiert werden (beispielsweise im Hinblick auf die Komplexität und Ausgefeiltheit sowie die späte Entdeckung der Angriffe). Dieses mangelnde Verständnis kann Untersuchungen erschweren.

5.5. APT-GRUPPEN ZUGESCHRIEBENE AUSGEFEILTE ANGRIFFE

Mehr als **50 % der Lieferkettenangriffe wurden** bekannten Cybercrime-Gruppen **zugeschrieben**, u. a. APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413 und TA428. Die Analyse zeigt, dass APT-Gruppen offenbar eine gewisse Vorliebe für Ziele mit regionalen Auswirkungen haben und dass eine beträchtliche Anzahl dieser Angriffe darauf abzielte, Zugang zu Kundendaten zu erhalten.

Von den 24 analysierten Vorfällen konnten zehn keiner bestimmten Gruppe zugeordnet werden. Dies könnte vor allem darauf zurückzuführen sein, dass sieben dieser Angriffe in den letzten sieben Monaten stattfanden. Die Untersuchung solcher Vorfälle kann längere Zeit in Anspruch nehmen, und selbst dann ist es eine Zuschreibung manchmal nicht möglich. In Anbetracht der Ausgefeiltheit dieser Angriffe sollten Lieferanten jedoch damit rechnen, von organisierten Cyberkriminellen ins Visier genommen zu werden, und sich entsprechend vorbereiten.

6. NICHT ALLES IST EIN LIEFERKETTENANGRIFF

Von Januar 2020 bis Anfang Juli 2021 gab es viele Vorfälle, die zunächst als Lieferkettenangriffe erschienen oder als Teil eines wahrscheinlichen künftigen Lieferkettenangriffs betrachtet wurden. Viele ermittelte traditionelle Software-Sicherheitslücken wurden als „Risiko" für künftige Lieferkettenangriffe gemeldet. In einigen Fällen handelte es sich um Sicherheitslücken, von denen man annahm, dass sie absichtlich in die Soft- bzw. Hardware eingebaut worden waren. Später stellte sich aber heraus, dass es sich um Bugs oder unbeabsichtigte Fehler handelte. Bei vielen dieser Fälle handelte es sich insoweit nicht um Lieferkettenangriffe, als kein Lieferant kompromittiert wurde.

In mindestens drei Fällen ging es den Angreifern um Software-Bibliotheken oder Dependencies (Abhängigkeiten). In einem dieser Fälle, der im Dezember 2020 gemeldet wurde, luden die Angreifer Schadprogramm-Pakete in das RubyGems-Repository hoch.[39] Über einen sehr ähnlichen Fall wurde im März 2021 berichtet, als es einem Sicherheitsexperten gelang, NPM-Pakete mit Schadprogrammen unter den Namen von Komponenten oder Infrastrukturen bekannter Unternehmen hochzuladen.[40] Ein dritter Fall wurde im April 2021 gemeldet, als Angreifer ein NPM-Paket mit Schadcode hochluden, das sich als bekanntes Paket ausgab (sogenanntes Brandjacking).[41] In all diesen Fällen haben die Angreifer weder vorhandene Pakete noch die Software-Repositories selbst kompromittiert. Da ein eindeutiger Angriff auf Lieferanten-Assets nicht gegeben war, haben wir sie nicht als Lieferkettenangriffe betrachtet.

In vielen Fällen wurden Sicherheitslücken in Software entdeckt, aber nicht für Angriffe genutzt, oder es wurde festgestellt, dass die betreffenden Fehler nicht vorsätzlich eingebaut worden waren. Das erste Beispiel für einen solchen Fall wurde im Februar 2020 gemeldet, als ein Sicherheitsexperte eine Zero-Day-Sicherheitslücke in der von der Firma Xiaongmai entwickelten Firmware für DVRs, NVRs und IP-Kameras aufdeckte.[42] Weitere Beispiele sind die Sicherheitslücken, die im Mai 2021 in Code-Erweiterungen von Visual Studio[43] und im Juni 2021 auf Pling-basierten Marktplätzen für freie und quelloffene Software (FOSS)[44] gemeldet wurden. In all diesen Fällen wurden Sicherheitslücken entdeckt. Bis zum Zeitpunkt der Erstellung dieses Berichts waren keine aktiven Angriffe auf diese Sicherheitslücken gemeldet worden. Wie in den vorangegangenen Abschnitten erwähnt, umfasst ein Lieferkettenangriff mindestens zwei Angriffe: einen auf einen Lieferanten und einen weiteren auf einen Kunden. Wenn nicht sowohl ein Kunde als auch ein Lieferant angegriffen wurden, wird ein Angriff nicht als Lieferkettenangriff angesehen.

Darüber hinaus gab es weitere Angriffe auf die Cybersicherheit und auf Sicherheitslücken, bei denen es sich nicht um Lieferkettenangriffe handelte. Ein solcher Fall war der Angriff auf Systeme von Centreon. Centreon ist ein Unternehmen, das IT-Überwachungsdienste sowie eine Open-Source-Überwachungssoftware für IT-Infrastrukturen anbietet. Im Januar 2021 wurde entdeckt, dass Angreifer veraltete, öffentlich zugängliche Centreon-Instanzen

[39] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Zugriff am 8.7.2021.
[40] Malicious NPM packages target Amazon, Slack with new dependency attacks, Bleeping Computer, https://www.bleepingcomputer.com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/. Zugriff am 8.7.2021.
[41] Damaging Linux \& Mac Malware Bundled within Browserify npm Brandjack Attempt, Sonatype, https://blog.sonatype.com/damaging-linux-mac-malware-bundled-within-browserify-npm-brandjack-attempt. Zugriff am 8.7.2021.
[42] Vollständige Offenlegung 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras, Habr, https://habr.com/en/post/486856/. Zugriff am 8.7.2021.
[43] Newly Discovered Bugs in VSCode Extensions Could Lead to Supply Chain Attacks, The Hacker News, https://thehackernews.com/2021/05/newly-discovered-bugs-in-vscode.html. Zugriff am 8.7.2021.
[44] Unpatched Flaw in Linux Pling Store Apps Could Lead to Supply-Chain Attacks, The Hacker News, https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.html. Zugriff am 8.7.2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

ausgenutzt hatten, um die Infrastruktur von Kunden zu kompromittieren.[45, 46, 47] Die Angreifer, mutmaßlich die APT-Gruppe Sandworm, betrieben ihre Kampagne über drei Jahre, bis sie schließlich entdeckt wurden. Ziel des Angriffs war es, an Daten der betroffenen Kunden zu gelangen. Der Angriff richtete sich gegen französische IT-Anbieter. In diesem Fall wurde eine bestimmte Software-Sicherheitslücke bei einer von Kunden installierten Software ausgenutzt. Der Lieferant selbst wurde jedoch nicht kompromittiert, und die Gefährdung erfolgte nicht vorsätzlich.

[45] Sandworm Intrusion Set Campaign Targeting Centreon Systems, CERT-FR, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf. Zugriff am 8.7.2021.
[46] France Reveals 3-Year Long Supply Chain Attack, Secure World Expo, https://www.secureworldexpo.com/industry-news/france-supply-chain-attack-centreon-software. Zugriff am 8.7.2021.
[47] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Zugriff am 8.7.2021.

7. EMPFEHLUNGEN

Lieferkettenangriffe **machen sich die Vernetzung der globalen Märkte zunutze**. Wenn mehrere Kunden auf denselben Lieferanten angewiesen sind, wird mit einem Cyberangriff auf diesen Lieferanten eine verstärkte Wirkung erzielt. Dadurch können weitreichende Auswirkungen auf nationaler oder sogar grenzüberschreitender Ebene ausgelöst werden. Bei einigen Produkten (z. B. bei Software und bei ausführbarem Code) ist die Existenz einer Lieferkette für Endnutzer nicht ohne Weiteres ersichtlich oder bleibt sogar völlig verborgen. Endnutzer-Anwendungen beruhen direkt oder indirekt auf Software, die vom jeweiligen Lieferanten bereitgestellt wird. Abhängigkeiten bestehen über Pakete, Bibliotheken und Module, die allgemein genutzt werden, um Entwicklungskosten zu senken und Lieferzeiten zu verkürzen.

Je besser Unternehmen vor Cyberangriffen geschützt sind, desto stärker rücken Lieferanten ins Blickfeld. Die Konsequenz liegt auf der Hand: Die Lieferanten werden zum schwächsten Glied der Lieferkette. Gleichzeitig verlangen die Kunden Produkte, die einerseits mehr Cybersicherheit bieten, gleichzeitig aber auch kostengünstig sind. Diese beiden Anforderungen lassen sich nicht immer miteinander vereinbaren.

Wie wir bei zahlreichen Lieferkettenangriffen beobachten konnten, erkennen Organisationen zunehmend die Notwendigkeit, **das Niveau der Cybersicherheit ihrer Lieferanten** und das **Ausmaß des Risikos aufgrund der Kunden-Lieferanten-Beziehung zu bewerten**. Die Kunden müssen die Gesamtqualität der Produkte und der Verhaltensweisen ihrer Lieferanten im Hinblick auf die Cybersicherheit bewerten und berücksichtigen und u. a. klären, ob diese sichere Entwicklungsverfahren anwenden. Zudem sollten die Kunden bei der Auswahl und Überprüfung ihrer Lieferanten und beim Management des Risikos, das sich aus den entsprechenden Beziehungen ergibt, erhöhte Sorgfalt walten lassen.

Zur **Beherrschung des Cybersicherheitsrisikos in der Lieferkette** sollten die Kunden[48]

- Lieferanten- und Dienstleistertypen ermitteln und dokumentieren,
- Risikokriterien für verschiedene Lieferanten- und Dienstleistungstypen definieren (z. B. wichtige Abhängigkeiten von Lieferanten und Kunden, kritische Software-Abhängigkeiten und einzelne Fehlerpunkte),
- Risiken in der Lieferkette gemäß ihren eigenen Bewertungen der Auswirkungen auf die Kontinuität des Geschäftsbetriebs und nach ihren Anforderungen bewerten,
- Maßnahmen zur Risikobehandlung auf der Grundlage bewährter Verfahren festlegen,
- Risiken und Bedrohungen in der Lieferkette anhand interner und externer Informationsquellen sowie aufgrund der Ergebnisse der Leistungsüberwachung und -überprüfung der Lieferanten überwachen und
- ihr Personal auf die Risiken aufmerksam machen.

Zur **Handhabung ihrer Beziehungen zu den Lieferanten** sollten die Kunden

- die Handhabung von Lieferantenbeziehungen auf den gesamten Lebenszyklus eines Produkts oder einer Dienstleistung ausdehnen, einschließlich der Verfahren für den Umgang mit Altprodukten oder -komponenten,
- Assets und Informationen klassifizieren, die mit Lieferanten geteilt werden oder für diese zugänglich sind, und Verfahren für den Zugang zu diesen Assets und Informationen und für deren Handhabung festlegen,
- die Verpflichtungen der Lieferanten zum Schutz der Assets der Organisation, zur gemeinsamen Nutzung von Informationen, zu Auditrechten, zur Kontinuität des Geschäftsbetriebs, zur Überprüfung des Personals und zum Umgang mit Vorfällen in Bezug auf Verantwortlichkeiten, Meldepflichten und Verfahren festlegen,
- die Sicherheitsanforderungen für die bezogenen Produkte und Dienstleistungen festlegen,

[48] In Anlehnung an die Cybersicherheitskontrollen der Normen ISO/IEC 27002, ISO 9001 und ISO 31000.

- all diese Verpflichtungen und Anforderungen in Verträge aufnehmen und Regeln für die Vergabe von Unteraufträgen sowie mögliche kaskadierende Anforderungen vereinbaren,
- die Qualität der erbrachten Dienstleistungen überwachen und routinemäßige Sicherheitsprüfungen durchführen, um die Einhaltung der in den Vereinbarungen festgelegten Cybersicherheitsanforderungen sicherzustellen; dazu zählt auch der Umgang mit Vorfällen, Sicherheitslücken, Patches, Sicherheitsanforderungen usw.,
- von Lieferanten und Dienstleistern die Zusicherung erhalten, dass diesen versteckte Funktionen oder Backdoor-Programme nicht bekannt sind,
- sicherstellen, dass regulatorische und rechtliche Anforderungen berücksichtigt werden,
- Verfahren zur Verwaltung von Änderungen in den Lieferantenvereinbarungen festlegen, z. B. Modifikationen an Tools oder Technologien.

Die Lieferanten hingegen sollten die **sichere Entwicklung von Produkten und Dienstleistungen** nach allgemein anerkannten Sicherheitsverfahren gewährleisten.[49] Sie sollten

- sicherstellen, dass beim Entwurf sowie bei der Entwicklung, Herstellung und Lieferung von Produkten, Komponenten und Dienstleistungen der verwendeten Infrastruktur die Verfahren zur Gewährleistung der Cybersicherheit berücksichtigt werden,[50, 51]
- einen Prozess der Produktentwicklung, -wartung und -unterstützung nach allgemein anerkannten Produktentwicklungsprozessen einführen,
- einen sicheren Entwicklungsprozess unter Berücksichtigung allgemein anerkannter sicherheitstechnischer Verfahren einführen,[52, 53]
- die Anwendbarkeit der technischen Anforderungen für die jeweiligen Produktkategorien und Risiken prüfen,[54]
- ihren Kunden Konformitätserklärungen auf der Grundlage bekannter Normen anbieten (z. B. ISO/IEC 27001, IEC 62443-4-1, IEC 62443-4-2 (oder spezifische Normen wie die CSA Cloud Controls Matrix (CCM) für Cloud-Dienste) und möglichst die Integrität und Herkunft der in beliebigen Bestandteilen eines Produkts verwendeten Open-Source-Software gewährleisten und bescheinigen,
- Qualitätsziele wie die Anzahl der Mängel, extern festgestellter Sicherheitslücken oder extern gemeldeter Sicherheitsprobleme festlegen und als Instrument zur Verbesserung der Gesamtqualität einsetzen,
- genaue und aktuelle Daten über die Herkunft von Software-Code oder -Komponenten sowie über die Kontrollen von internen und externen Software-Komponenten, Tools und Diensten bei Software-Entwicklungsprozessen pflegen und
- regelmäßige Audits durchführen, um sicherzustellen, dass die oben genannten Maßnahmen eingehalten werden.

Da alle Produkte und Dienstleistungen aus Komponenten und Software mit potenziellen Sicherheitslücken bestehen bzw. darauf beruhen, **sollten** die Lieferanten außerdem **bewährte Verfahren zum Management von Sicherheitslücken einführen**,[55] z. B:

- die Überwachung sicherheitsrelevanter Sicherheitslücken, die von internen und externen Quellen gemeldet werden, einschließlich der verwendeten Komponenten von Dritten,

[49] Beispielsweise IEC 62443-4-1.
[50] Beispielsweise die Verfahren nach ISO/IEC 27001.
[51] Dazu können technische Maßnahmen zählen, z. B. a) die Trennung von Umgebungen, b) die Prüfung von Vertrauensbeziehungen, c) die Einführung einer mehrstufigen, risikobasierten Authentifizierung und bedingter Zugangskontrollen in der gesamten Organisation, d) die Minimierung von Abhängigkeiten von Produkten, die Teil der Umgebungen zur Entwicklung, Erstellung und Bearbeitung von Software sind, e) die Verschlüsselung von Daten und f) die Überwachung von Vorgängen und Warnungen sowie die Reaktion auf Angriffsversuche und tatsächliche Cybervorfälle.
[52] Beispielsweise IEC 62443-2-4
[53] Dazu können der Einsatz automatisierter Tools oder vergleichbarer Verfahren gehören, um vertrauenswürdige Quellcode-Lieferketten aufrechtzuerhalten und so die Integrität des Codes zu gewährleisten, oder der Einsatz automatisierter Werkzeuge oder vergleichbarer Verfahren, die bekannte und potenzielle Sicherheitslücken erkennen und beheben.
[54] Normen wie IEC 62443-4-2 bieten einen umfassenden Katalog an Sicherheitsanforderungen, klassifiziert nach Anforderungen an alle Produkte, an Softwareanwendungen (SAR), an eingebettete Geräte (EDR), an Hostgeräte (HDR) und an Netzwerkgeräte (NDR).
[55] Weitere Hinweise zum Sicherheitslücken- und Patch-Management sind den Normen IEC 62443-4-1, IEC 62443-2-4 und IEC TR 62443-2-3 zu entnehmen.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- die Risikoanalyse von Sicherheitslücken unter Verwendung eines Bewertungssystems (z. B. CVSS)[56],
- Wartungsrichtlinien für die Behandlung festgestellter Sicherheitslücken je nach Risiko,
- Prozesse zur Unterrichtung der Kunden,
- die Durchführung von Patch-Verifizierungen und -Tests, um sicherzustellen, dass die betrieblichen, sicherheitstechnischen und rechtlichen Anforderungen sowie die Anforderungen an die Cybersicherheit erfüllt werden und dass die Patches mit nicht eingebauten Fremdkomponenten kompatibel sind,
- Verfahren für die sichere Bereitstellung von Patches und Dokumentation der Patches für die Kunden und
- die Beteiligung an einem Programm zur Offenlegung von Sicherheitslücken mit einem Prozess zur Meldung und Offenlegung von Erkenntnissen.

Sicherheitslücken sollten die Lieferanten mit Patches begegnen. Ebenso sollten Kunden den Markt im Hinblick auf das Bekanntwerden von Sicherheitslücken beobachten bzw. entsprechende Mitteilungen von ihren Lieferanten erhalten. **Bewährte Verfahren zum Patch-Management** sind etwa[57]

- die Führung eines Verzeichnisses der Assets mit Informationen über Patches,
- die Nutzung von Informationsquellen zur Ermittlung maßgeblicher technischer Sicherheitslücken,
- die Bewertung der Risiken festgestellter Sicherheitslücken und Existenz einer dokumentierten und umgesetzten Wartungspolitik,
- der Bezug von Patches nur aus legitimen Quellen und das Testen der Patches vor dem Installieren,
- die Anwendung alternativer Maßnahmen, wenn ein Patch nicht verfügbar oder nicht anwendbar sein sollte, und
- die Anwendung von Rollback-Verfahren und effektiven Sicherungs- und Wiederherstellungsprozessen.

Über das hinaus, was Kunden und Lieferanten ihrerseits tun können, kommen Initiativen auch auf Branchenebene in Betracht. Google hat im Juni 2021 unter der Bezeichnung SLSA (Supply chain Levels for Software Artifacts)[58] ein End-to-End-Rahmenwerk zur Gewährleistung der Integrität von Software-Artefakten in der gesamten Software-Lieferkette eingeführt. Mit SLSA soll in der Branche die Situation insbesondere mit Blick auf Open Source-Software verbessert werden, um den größten Integritätsbedrohungen zu begegnen. Wenngleich sich SLSA auf Angriffe auf die Software-Lieferkette konzentriert, nicht aber auch alle anderen Arten von Angriffen berücksichtigt, ist dies ein guter Anfang, der Organisationen zugutekommen kann.

Eine allgemeinere, aber umfangreiche Gruppe von Empfehlungen zur Abwehr von Cyberbedrohungen wurde im Juni 2021 von MITRE mit dem Projekt MITRE D3FEND eingeführt.[59] MITRE D3FEND ist ein Rahmenwerk bzw. eine strukturierte Wissensdatenbank, in der Unternehmen spezifische Abhilfemaßnahmen zur Verhinderung bestimmter im MITRE ATT&CK®-Modell beschriebener Angriffe finden. Das Projekt ist weder spezifisch für die Lieferkette noch für APT-Angriffe. Die Empfehlungen können aber zur Verbesserung des allgemeinen Sicherheitsniveaus von Organisationen berücksichtigt werden.

Allerdings können nicht alle Risiken in der Lieferkette durch bewährte Verfahren von Kunden, Lieferanten oder Organisationen abgeschwächt werden. Insbesondere versteckte Funktionen und nicht dokumentierte Zugriffsmöglichkeiten (Backdoor-Programme) bei Hardwarekomponenten können bei den gängigsten Zertifizierungen oder Standard-Penetrationstests nicht vollständig ermittelt werden. Zudem stellen Zero-Day-Sicherheitslücken, d. h. Sicherheitslücken, die nur einer bestimmten Gruppe bekannt sind und von ihr genutzt werden, weiterhin eine Herausforderung dar. Daher können Maßnahmen auf nationaler oder sogar europäischer Ebene erforderlich sein. Die zuständigen nationalen Behörden könnten nationale Bewertungen von Sicherheitsrisiken für Lieferketten unter Berücksichtigung bekannter Akteure durchführen, um daraus Maßnahmen für die Beschaffung auf nationaler Ebene abzuleiten. Außerdem können Lieferkettenangriffe von staatlichen Akteuren mit fortgeschrittenen Fähigkeiten gesponsert werden. Bei solchen staatlich gesponserten Angriffen kann die Unterstützung der zuständigen Behörden erforderlich sein, um die bestehenden Risiken zu mindern.

[56] Siehe https://www.first.org/cvss/specification-document ;.
[57] In Anlehnung an ISO/IEC 27002.
[58] Google Online Security Blog: Introducing SLSA, an End-to-End Framework for Supply Chain Integrity, Google, https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html. Zugriff am 8.7.2021.
[59] MITRE D3FEND™, D3FEND Matrix, Version 0.9.2-BETA-3, https://d3fend.mitre.org/. Zugriff am 29.6.2021.

8. SCHLUSSFOLGERUNGEN

Da direkte Angriffe auf gut geschützte Organisationen inzwischen einen höheren Aufwand erfordern, ziehen es Angreifer vor, deren Lieferkette anzugreifen. Dabei bietet die Aussicht auf potenziell weitreichende und grenzüberschreitende Auswirkungen einen zusätzlichen Anreiz. Diese Verlagerung hat dazu geführt, dass die **Zahl der gemeldeten Lieferkettenangriffe ungewöhnlich zugenommen** hat. (**Für 2021 werden viermal mehr Lieferkettenangriffe erwartet als 2020**.) Infolge des inhärent globalen Charakters der modernen Lieferketten erhöht sich der Umfang ihrer potenziellen Auswirkungen. Gleichzeitig weitet sich für böswillige Akteure das Spektrum möglicher Angriffsziele. In diesem Bericht werden verschiedene bekannte Angriffe behandelt. Weitere Lieferkettenangriffe wurden möglicherweise nicht entdeckt oder nicht untersucht oder sind auf andere Ursachen zurückzuführen.

Insbesondere im Software-Bereich untergraben Lieferkettenangriffe das Vertrauen in das einschlägige Ökosystem. Die beschriebenen Vorfälle verdeutlichen, dass böswillige Akteure die **Software-Lieferkette bereits in den frühen Phasen** (d. h. in der Entwicklungsphase) **kompromittieren** können. Es müssen neue Ansätze entwickelt werden, um die Lieferkette von Grund auf zu sichern. Diesbezüglich scheinen neue Initiativen wie Google SLSA und MITRE D3FEND recht vielversprechend zu sein.

Die Analyse in diesem Bericht zeigt, dass es bei den untersuchten Vorfällen immer noch zahlreiche unbekannte Faktoren gibt. **66 % der bei Angriffen auf Lieferanten angewendeten Vektoren sind noch unbekannt.** Mangelnde Transparenz oder fehlende Ermittlungsmöglichkeiten stellen eine ernsthafte Gefahr für das Vertrauen in die Lieferkette dar. Die Verbesserung der Transparenz und der Rechenschaftspflicht ist ein erster Schritt zur Verbesserung der Sicherheit aller Elemente der Lieferkette und zum Schutz der Endkunden.

Lieferkettenangriffe können komplex sein und erfordern eine sorgfältige Planung, und oft erstreckt sich die Ausführung über Monate oder Jahre. **Diese Angriffe werden zu mehr als 50 % APT-Gruppen oder bekannten Angreifern zugeschrieben**. Angesichts der Wirksamkeit von Lieferkettenangriffen könnten Angriffe auf Lieferanten künftig auch für andere, allgemeinere Typen von Angreifern an Attraktivität gewinnen. Entscheidend ist daher, dass Organisationen sich im Hinblick auf ihre Sicherheit nicht nur auf sich selbst konzentrieren, sondern auch ihre Lieferanten berücksichtigen. Dies gilt insbesondere für Anbieter von Cloud-Diensten und für Managed Service Providers, bei denen die jüngsten Angriffe den erhöhten Bedarf an Cyber-Sicherheitskontrollen in diesen Sektoren deutlich machen.

Infolge der wachsenden wechselseitigen Abhängigkeit und Komplexität können die Auswirkungen von Angriffen auf Lieferanten **weitreichende Konsequenzen** haben. Dies liegt nicht nur an der großen Zahl der Betroffenen, sondern bietet vor allem in Fällen, in denen vertrauliche Informationen abgefangen werden, Grund zur Sorge um die nationale Sicherheit bzw. um geopolitische Auswirkungen.

In diesem komplexen Umfeld für Lieferketten sind **sowohl** die Einführung **bewährter Verfahren auf EU-Ebene als auch koordinierte Maßnahmen wichtig**, um im Interesse eines gemeinsamen Sicherheitsniveaus alle Mitgliedstaaten bei der Entwicklung vergleichbarer Fähigkeiten zu unterstützen.

ANHANG A: LIEFERKETTENANGRIFFE – ZUSAMMENFASSUNG

In diesem Abschnitt werden 24 für diesen Bericht ermittelte und analysierte Vorfälle in Lieferketten zusammenfassend beschrieben. Jeder Vorfall wird unter dem Namen des vom Angriff betroffenen Lieferanten behandelt. Auf jeden einzelnen Fall wird die in diesem Bericht vorgeschlagene Taxonomie angewendet. Ein Diagramm veranschaulicht jeweils den Ablauf des Angriffs. Die Zusammenfassungen enthalten die Informationen, die zum Zeitpunkt der Erstellung dieses Berichts verfügbar waren.

VERZEICHNIS DER LIEFERKETTENVORFÄLLE:

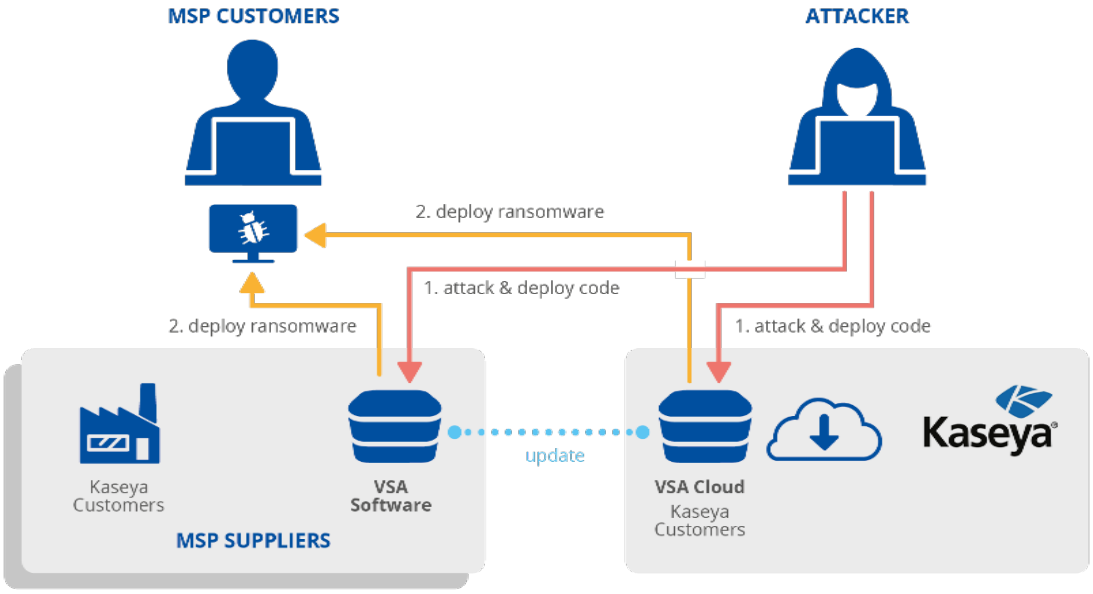
A.1 KASEYA: IT-SOFTWARE-MANAGEMENT

Kaseya[60] ist ein Software-Dienstleister, der sich auf Tools für die elektronische Überwachung und Verwaltung spezialisiert hat. Das Unternehmen vertreibt VSA-Software (Virtual System/Server Administrator) und stellt eigene Cloud-Server zur Verfügung. MSPs (Managed Service Providers) können die VSA-Software vor Ort nutzen oder Lizenzen für die VSA-Cloud-Server von Kaseya erwerben. MSPs bieten ihrerseits anderen Kunden verschiedene IT-Dienste an.[61]

Im Juli 2021 nutzten Angreifer eine Zero-Day-Sicherheitslücke in Kaseyas eigenen Systemen aus (CVE-2021-30116).[62] Angreifer konnten aus der Ferne Befehle auf den VSA-Appliances der Kunden von Kaseya ausführen. Kaseya kann Remote-Updates an alle VSA-Server senden. Am Freitag, dem 2. Juli 2021, wurde ein Update an die VSAs der Kaseya-Kunden verteilt, mit dem von den Angreifern eingeschleuster Programmcode ausgeführt wurde. Dieses Schadprogramm bewirkte die Installation von Ransomware[63, 64] bei von dieser VSA verwalteten Kunden.

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Software	Bereits vorhandene Software

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Daten, finanzieller Schaden

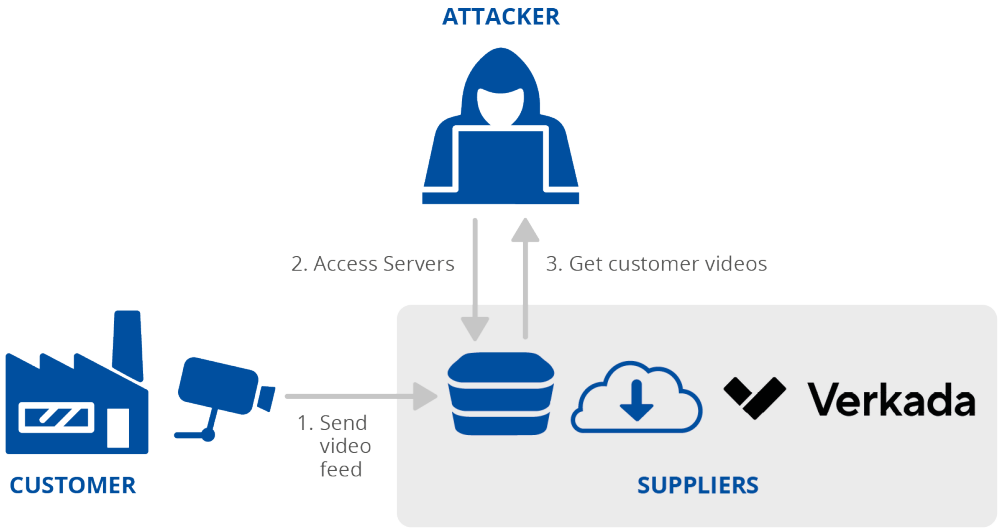


[60] IT Management Software − for MSPs and IT Teams, Kaseya, https://www.kaseya.com/. Zugriff am 9.7.2021.
[61] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Zugriff am 9.7.2021.
[62] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116, Zugriff am 9.7.2021.
[63] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/, Zugriff am 9.7.2021.
[64] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Zugriff am 9.7.2021.

A.2 VERKADA: CLOUD-BASIERTE LÖSUNGEN ZUR SICHERHEITSÜBERWACHUNG

Verkada bietet mehr als 5000 Kunden cloudbasierte Lösungen zur Sicherheitsüberwachung.[65] Im März 2021 wurde ein Produktionsserver kompromittiert. Infolge des Angriffs konnten die Angreifer, die sich die Anmeldedaten für einen privilegierten Zugang verschafft hatten, auf die in den Einrichtungen der Kunden installierten Sicherheitskameras zugreifen.[66] Die Anmeldedaten wurden angeblich „im Internet“ gefunden.[67] Die Angreifer erlangten Zugang zu den Videos und Bildern von mehr als 150 000 Kameras, die die Kunden in Schulen, Gefängnissen, Krankenhäusern, Polizeistationen und Tesla-Fabriken installiert hatten.[68] Eine Hacktivisten-Gruppe bekannte sich zu dem Anschlag.[69]

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
OSINT	Konfigurationen, Daten	Ausnutzen einer Vertrauensbeziehung [T1199]	Daten



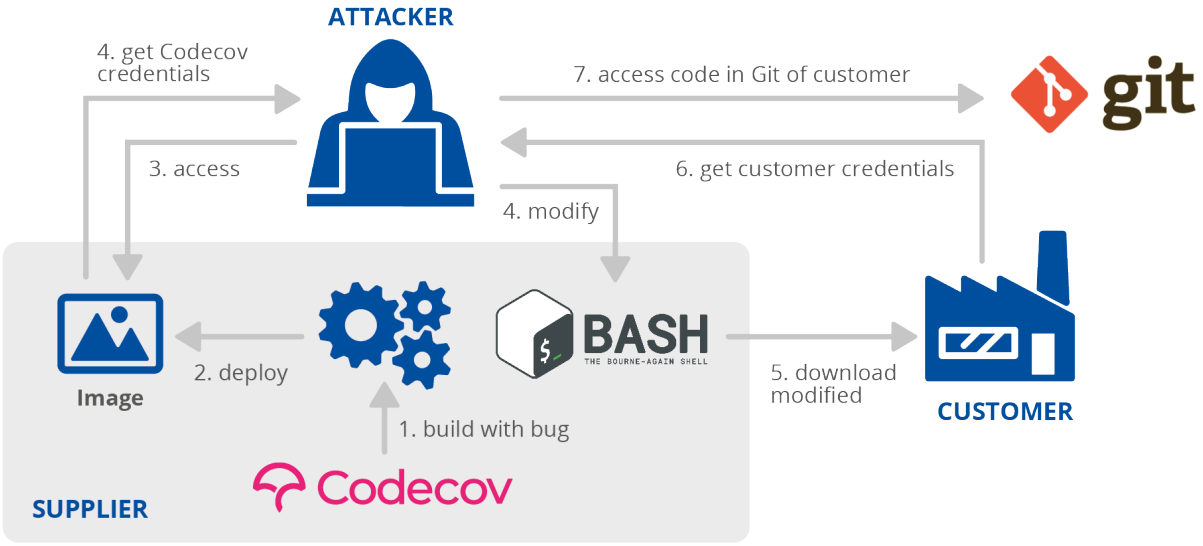
[65] The Future of Physical Security for the Enterprise: About Verkada, Verkada, https://www.verkada.com/about/. Zugriff am 9.7.2021.
[66] Verkada Security Update, Verkada, https://www.verkada.com/security-update/. Zugriff am 9.7.2021.
[67] Verkada Mass Hack, IPVM, https://ipvm.com/reports/verkada-hack. Zugriff am 9.7.2021.
[68] A hacker who exposed Verkada's surveillance camera snafu has been raided, The Verge, https://www.theverge.com/2021/3/12/22328344/tillie-kottmann-hacker-raid-switzerland-verkada-cameras. Zugriff am 9.7.2021.
[69] Tesla (TSLA), Cloudfare (NET) Breached in Verkada Security Camera Hack, Bloomberg, https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams. Zugriff am 9.7.2021.

A.3 CODECOV: CODE-MANAGEMENT UND AUDIT-LÖSUNGEN

Codecov ist ein Unternehmen, das Software zur Ermittlung der Codeabdeckung sowie Prüfwerkzeuge entwickelt. Das Unternehmen liefert Werkzeuge an andere Unternehmen (u. a. IBM und Hewlett Packard Enterprise). Im April 2021 berichtete Codecov, dass Angreifer aufgrund eines Fehlers bei der Erstellung eines Docker-Images einige ihrer gültigen Anmeldedaten aus einem Docker-Image erlangt hatten.

Über die erlangten Anmeldedaten kompromittierten sie ein „Upload-Bash-Skript“[70], das von Codecov-Kunden verwendet wird. Sobald die Kunden dieses Skript heruntergeladen und ausgeführt hatten, konnten die Angreifer Daten von Codecovs Kunden abfangen, einschließlich sensibler Informationen, die den Angreifern Zugriff auf Ressourcen der Kunden ermöglichten.[71] Mehrere Codecov-Kunden berichteten, dass die Angreifer mithilfe der infolge des Angriffs auf Codecov entwendeten Informationen in der Lage waren, auf ihren Quellcode zuzugreifen.[71] Der Angriff konnte nicht zugeordnet werden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Konfiguration	Code	Ausnutzen einer Vertrauensbeziehung [T1199]	Software



[70] Codecov supply chain attack breakdown, https://blog.gitguardian.com/codecov-supply-chain-breach/. Zugriff am 27.6.2021.

[71] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Zugriff am 27.6.2021.

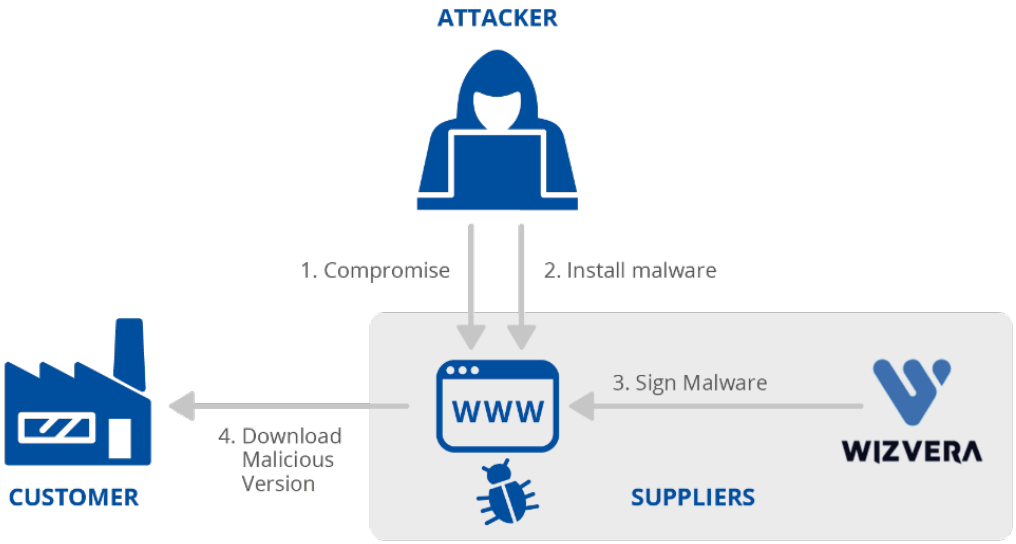
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.4 WIZVERA VERAPORT: SOFTWARE ZUR INTEGRATION VON INSTALLATIONSPROGRAMMEN

Wizvera ist ein Unternehmen, das Lösungen für Identitätsüberprüfungen, Kennwortmanagement und Cloud-Zertifikate anbietet.[72] VeraPort, eine Software von Wizvera zur Integration von Installationsprogrammen, ermöglicht Benutzern, die von ihren Arbeitgebern geforderte Sicherheitssoftware zu installieren.[73] Im November 2020 kompromittierten Angreifer eine legitime Website, die von VeraPort unterstützt wurde. Sie ersetzten die VeraPort-Konfiguration auf der kompromittierten Website derart, dass statt der erwarteten Sicherheitssoftware ein Schadprogramm verteilt wurde.

Die Konfiguration war von Wizvera digital signiert.[73] VeraPort vergewissert sich, dass die heruntergeladene Software eine gültige digitale Signatur hat, prüft aber nicht, wer das Zertifikat ausgestellt hat. Daher luden südkoreanische Nutzer, die auf die kompromittierte Website zugriffen, das Schadprogramm herunter. Der Angriff wurde der Gruppe Lazarus APT zugeschrieben.[73]

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Prozesse	Drive-by Compromise [T1189], Infektion mit einem Schadprogramm	Daten



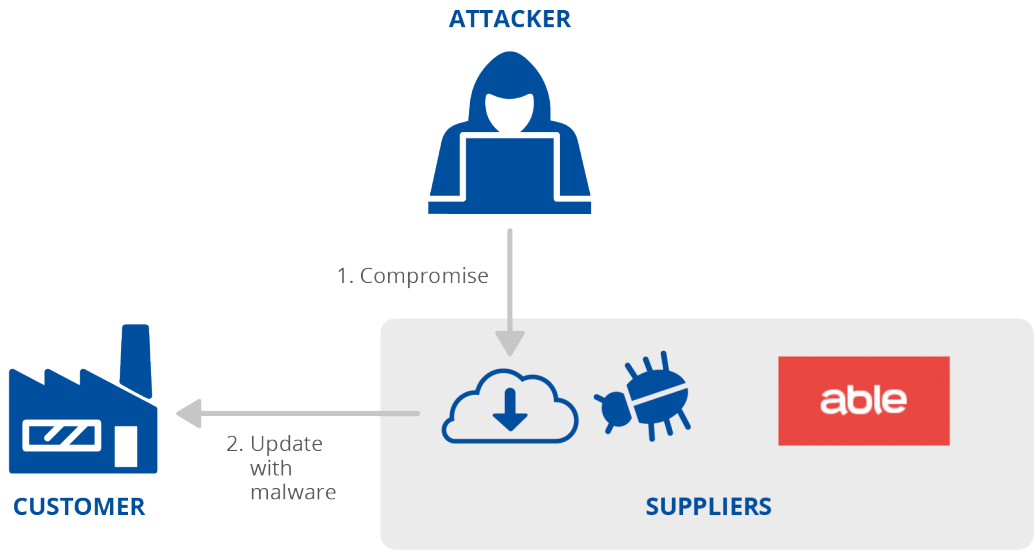
[72] Wizvera Company Profile & Funding, Crunchbase, https://www.crunchbase.com/organization/wizvera. Zugriff am 9.7.2021.
[73] Lazarus supply-chain attack in South Korea, WeLiveSecurity, https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/. Accessed Zugriff am 9.7.2021.

A.5 ABLE DESKTOP: CHAT-SOFTWARE

Able ist ein Unternehmen mit Sitz in der Mongolei, das Softwarelösungen für Regierungsbehörden und Unternehmen in der Region anbietet.[74] Im Juni 2020 haben Angreifer offenbar Zugang zum Backend von Able erlangt und das System kompromittiert, über das Software-Updates an alle Kunden verteilt werden. Die Angreifer fügten ein Schadprogramm in Anwendung „Able Desktop“ (ein Add-on, das für den Sofortnachrichtendienst des Hauptprodukts von Able benötigt wird) ein.[75] Es ist nicht bekannt, wie der Lieferant kompromittiert wurde, aber jedenfalls gelang es den Angreifern, die Benutzer zur Installation eines Schadprogramms zu zwingen.[75] Das Schadprogramm wurde dann genutzt, um Informationen von den infizierten Geräten der Kunden zu entwenden.[75] Der Angriff wurde der APT-Gruppe TA428 zugeschrieben.

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Daten

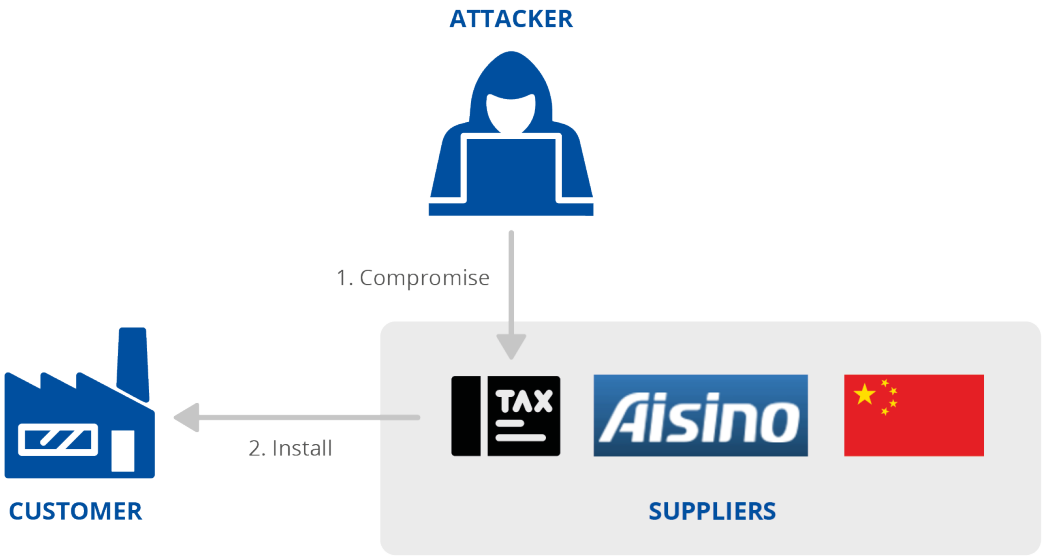


[74] Able − Working online, Able, https://web.able.mn/, Zugriff am 9.7.2021.
[75] Operation StealthyTrident: corporate software under attack, WeLiveSecurity, https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/. Zugriff am 9.7.2021.

A.6 AISINO INTELLIGENTES STEUERMANAGEMENT

Die Aisino Credit Information Company bietet internationalen Kunden über ihre Abteilung „Golden Tax“ Software zum Steuermanagement an, darunter die „Aisino Tax Software Suite“. Im Juni 2020 gaben Forscher bekannt, dass die „Aisino Tax Software Suite“ mit einem Schadprogramm kompromittiert wurde.[76] Es ist nicht bekannt, wie die Software kompromittiert wurde und was das Ziel des Angriffs war.[76] Da diese Software Teil eines nationalen chinesischen Programms ist, wird davon ausgegangen, dass der Angriff gegen Unternehmen in China gerichtet war.[77] Der Angriff konnte nicht zugeordnet werden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code	Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Unbekannt



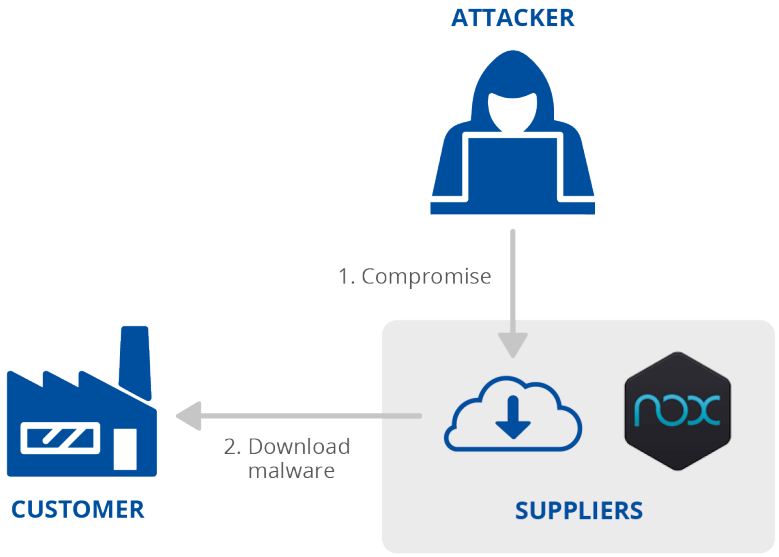
[76] The Golden Tax Department and Emergence of GoldenSpy Malware, Trustwave SpiderLabs, https://trustwave.azureedge.net/media/16929/the-golden-tax-department-and-emergence-of-goldenspy-malware.pdf. Zugriff am 9.7.2021.
[77] GoldenSpy Chapter 4: GoldenHelper Malware Embedded in Official Golden Tax Software, Trustwave, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/. Zugriff am 9.7.2021.

A.7 BIGNOX NOXPLAYER: ANDROID-EMULATOR FÜR PCS UND MACS

BigNox ist ein Anbieter von Emulationssoftware. Das wichtigste Produkt des Unternehmens, NoxPlayer, ist ein sehr beliebter Android-Emulator für Windows und Mac.[78] Im Februar 2021 berichteten Forscher, dass die NoxPlayer-Infrastruktur kompromittiert worden war. Sie konnte genutzt werden, um unter Missbrauch der Update-Funktion des Tools anstelle von Updates Schadprogramme zu installieren.[79]

Nach dem Einschleusen des ersten Codes konnten die Angreifer Informationen über ihre Opfer sammeln und weitere Schadprogramme an bestimmte Ziele verteilen.[79] Offenbar wollten die Angreifer sich die Möglichkeit verschaffen, bestimmte Ziele zu überwachen.[79] Der Angriff konnte nicht zugeordnet werden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code	Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Menschen, Daten



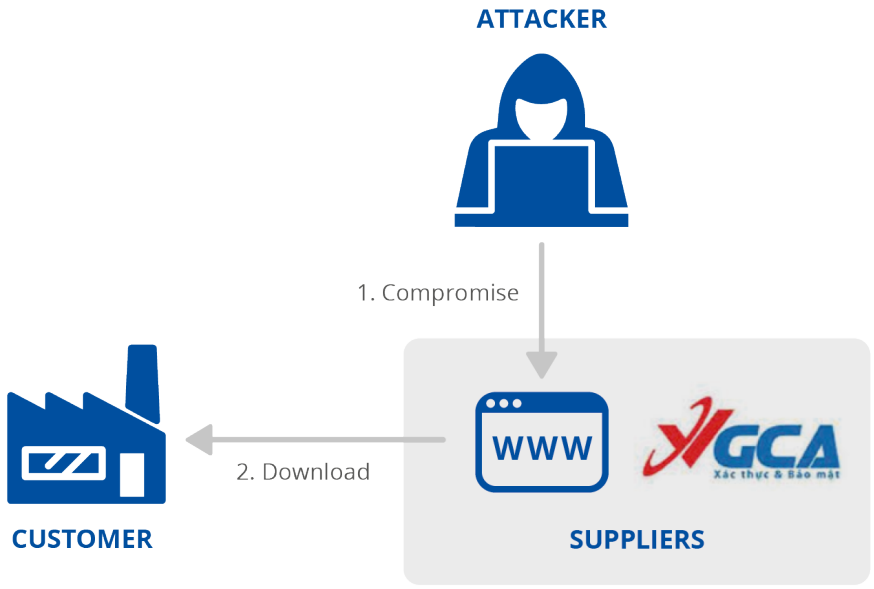
[78] NoxPlayer − Free Android Emulator on PC and Mac, BigNox, https://www.bignox.com/. Zugriff am 9.7.2021.
[79] Operation NightScout: Supply-chain attack targets online gaming in Asia, WeLiveSecurity, https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/. Zugriff am 9.7.2021.

A.8 ZERTIFIZIERUNGSBEHÖRDE DER VIETNAMESISCHEN REGIERUNG (VGCA)

Die vietnamesische staatliche Zertifizierungsstelle (VGCA) bietet digitale Zertifikate und eine Reihe von Anwendungen an, mit denen Bürgerinnen und Bürger sowie Unternehmen Dokumente digital signieren können.[80] Im Dezember 2020 berichteten Forscher, dass die Website der VGCA-Infrastruktur kompromittiert worden war, um legitime Binärdateien durch Trojaner-Programme zu ersetzen.[81] Das Ziel des Angriffs ist unklar, Forscher glauben jedoch, dass er Teil eines weiter reichenden Angriffs sein könnte.[81] Die verwendeten Tools deuten darauf hin, dass APT-Gruppen (TA413, TA428) hinter dem Angriff stehen könnten.[82]

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Menschen



[80] Vietnam targeted in complex supply chain attack, ZDNet, https://www.zdnet.com/article/vietnam-targeted-in-complex-supply-chain-attack/. Zugriff am 9.7.2021.
[81] Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia, WeLiveSecurity, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/. Zugriff am 9.7.2021.
[82] Panda's New Arsenal: Part 3 Smanager, Hiroki Hada, https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager. Zugriff am 9.7.2021.

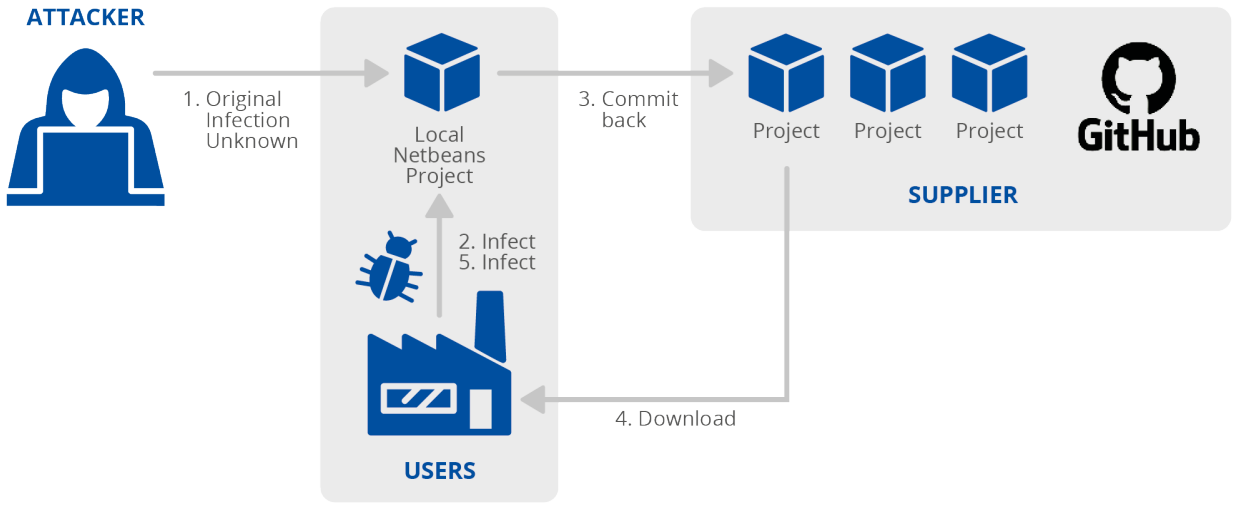
A.9 APACHE NETBEANS: ENTWICKLUNGSPLATTFORM

NetBeans ist eine integrierte Java-Entwicklungsplattform von Apache. Im Mai 2020 berichteten Forscher, dass einige NetBeans-Projekte auf GitHub Schadprogramme enthielten, von denen die Eigentümer nichts wussten. Die Systeme aller, die diese Projekte herunterluden und verwendeten, wurden infiziert. Dadurch gelangten Trojaner auf alle lokalen NetBeans-Projekte und wurden auf GitHub hochgeladen.

Außerdem wurden Nutzer mit einem RAT-Schadprogramm infiziert.[83, 84] Offenbar sollten mit dem Angriff geschützte Informationen gesammelt werden. Dieser Angriff scheint Teil eines umfangreicheren Lieferkettenangriffs zu sein. In diesem Fall waren sowohl der Lieferant als auch die Nutzer Opfer. GitHub ist das einzige gemeinsam zu nutzende Medium, das für den Angriff genutzt wurde. Der Angriff konnte nicht zugeordnet werden.

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Infektion mit einem Schadprogramm	Code

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Infektion mit einem Schadprogramm	Software, Daten

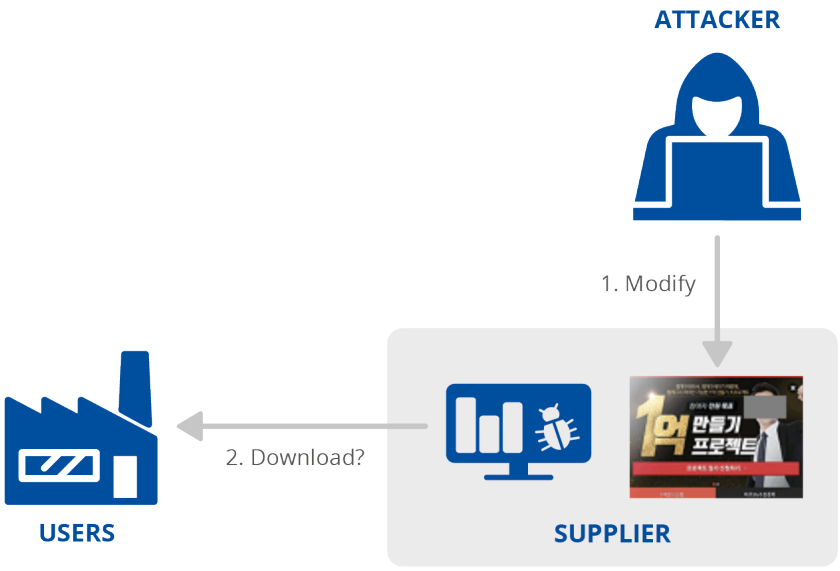


[83] The Octopus Scanner Malware: Attacking the open source supply chain, GitHub Security Lab, https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain/. Zugriff am 9.7.2021.
[84] Supply Chain Attack Event − Targeted Attacks on Java Projects in GitHub, NSFOCUS, https://nsfocusglobal.com/supply-chain-attack-event-targeted-attacks-on-java-projects-in-github/. Zugriff am 9.7.2021.

A.10 MESSENGER FÜR PRIVATE AKTIENANLAGEN

Im Januar 2021 berichteten Forscher über einen Angriff der Gruppe Thallium APT auf Aktienanleger, bei der eine weitverbreitete Messenger-Anwendung für private Aktienanlagen kompromittiert wurde.[85] Die Angreifer hatten einen Trojaner mit einem Schadprogramm in die Installationsprogramme der Messenger-Anwendung eingeschleust.[86] Mit dem Schadprogramm wurden die infizierten Nutzer ausgespäht.[87] Über den Angriff oder die verwendeten Methoden gibt es keine zuverlässigen Informationen.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code	Infektion mit einem Schadprogramm	Menschen

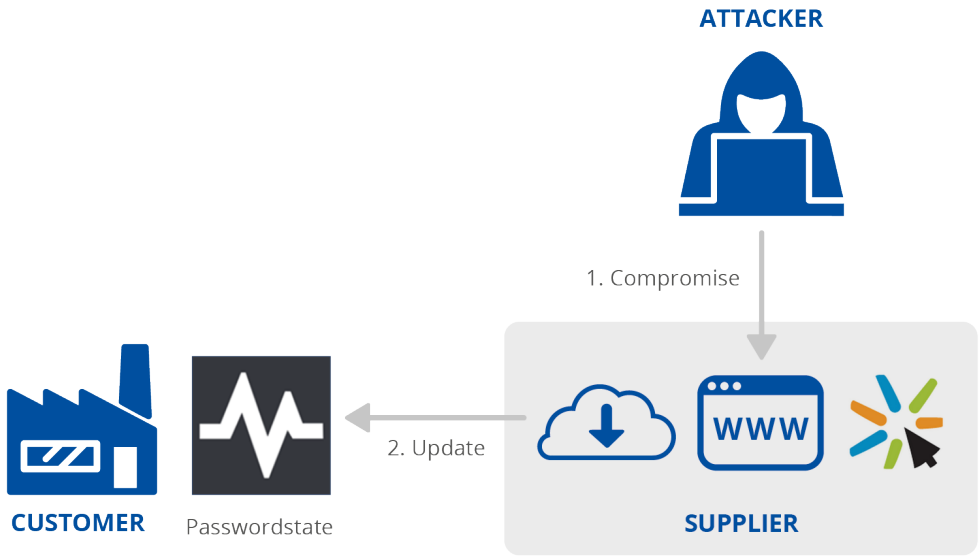


[85] Thallium Hacker Targeted Users of Private Stock Investment Messenger, Cyware Alerts − Hacker News, https://cyware.com/news/thallium-hacker-targeted-users-of-private-stock-investment-messenger-ac33d20d. Zugriff am 9.7.2021.
[86] Thallium Altered the Installer of a Stock Investment App, E Hacking News, https://www.ehackingnews.com/2021/01/thallium-altered-installer-of-stock.html. Zugriff am 9.7.2021.
[87] Thallium organization exploits private equity investment messenger to launch software supply chain attack, ESTsecurity, https://blog.alyac.co.kr/3489. Zugriff am 9.7.2021.

A.11 CLICKSTUDIOS PASSWORDSTATE: KENNWORTMANAGER

ClickStudios ist ein Anbieter von Lösungen für das Kennwortmanagement in Unternehmen.[88] Wichtigstes Produkt von ClickStudios ist das Tool Passwordstate. Im April 2021 wurde der zur Aktualisierung von Passwordstate verwendete Web-Mechanismus „Upgrade Director“ so kompromittiert,[89] dass die Nutzer statt der erwarteten Updates ein Schadprogramm herunterluden. Das installierte Schadprogramm wurde entwickelt, um Informationen von den kompromittierten Systemen zu entwenden.[89, 90] Der Angriff konnte nicht zugeordnet werden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code	Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Daten



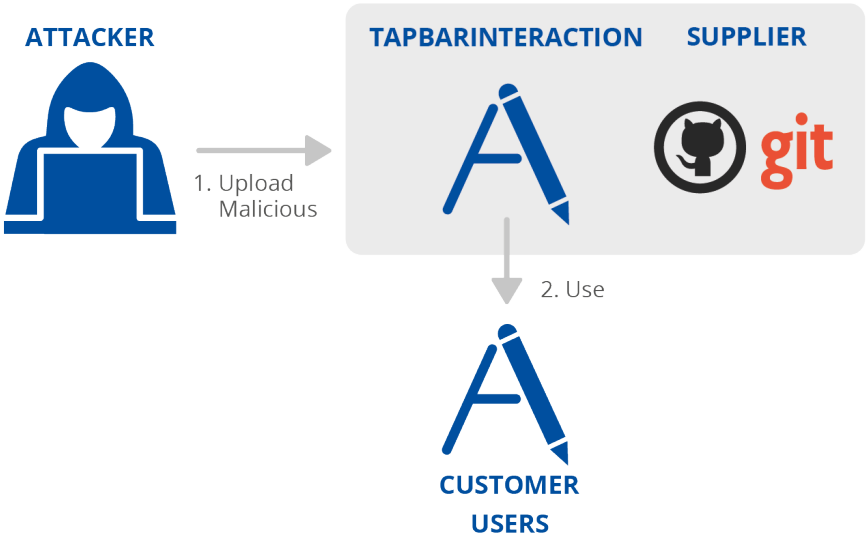
[88] Enterprise Password Management Software − Web based Server Password Manager, ClickStudios https://www.clickstudios.com.au/. Zugriff am 9.7.2021.
[89] ClickStudios PASSWORDSTATE Incident Management Advisory #01, ClickStudios, https://www.clickstudios.com.au/advisories/Incident_Management_Advisory-01-20210424.pdf. Zugriff am 9.7.2021.
[90] Moserpass supply chain, CSIS Security Group, https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/. Zugriff am 9.7.2021.

A.12 APPLE XCODE: INTEGRIERTE ENTWICKLUNGSUMGEBUNG

Apple Xcode ist eine Entwicklungsumgebung für die Entwicklung von OSX- und iOS-Anwendungen.[91] Im März 2021 berichteten Forscher, dass ein Xcode-Projekt mit Schadcode eingesetzt wurde, um die Systeme von Xcode-Entwicklern mit einem Backdoor-Programm zu infizieren.[92] Das Xcode-Projekt mit dem Schadcode war eine Kopie eines echten Xcode-Projekts. Über das Xcode-Projekt mit dem Schadcode wurden Nutzer aufgrund einer Sicherheitslücke in Xcode infiziert, die Angreifern ermöglichte, bei der Erstellung eines Projekts automatisch ein Skript ausführen zu lassen.[92]

Der Angriff konnte nicht zugeordnet werden, und es ist nicht klar, ob überhaupt Kunden angegriffen wurden.[93] Unklar ist zudem, wie das Xcode-Projekt mit dem Trojaner-Programm an die potenziellen Opfer übermittelt wurde, oder ob es überhaupt jemals dazu gekommen ist.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code	Infektion mit einem Schadprogramm	Unbekannt

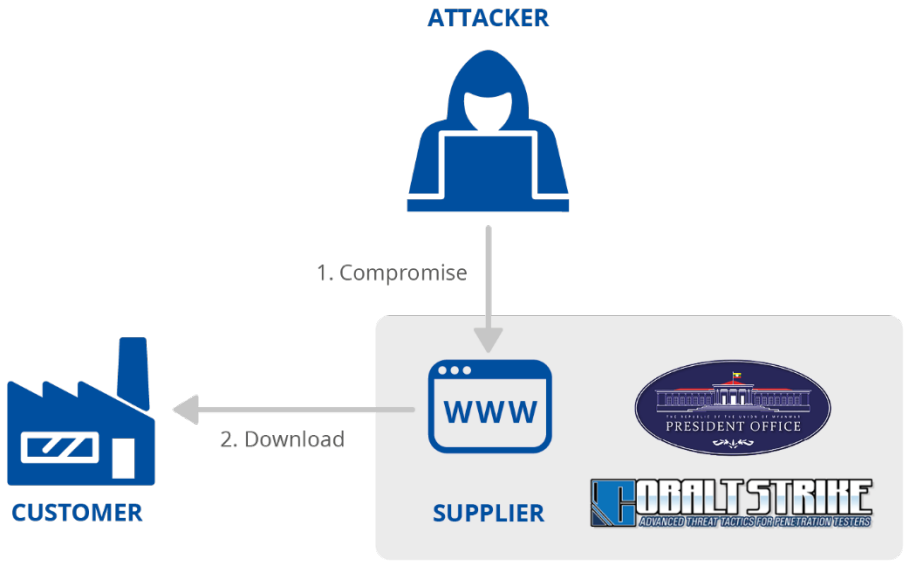


[91] Xcode 13 Overview, Apple Developer, https://developer.apple.com/xcode/. Zugriff am 9.7.2021.
[92] New macOS Malware XcodeSpy Targets Xcode Developers with EggShell Backdoor, SentinelLabs, https://labs.sentinelone.com/new-macos-malware-xcodespy-targets-xcode-developers-with-eggshell-backdoor/, Zugriff am 9.7.2021.
[93] XcodeSpy Mac Malware Targets Developers, SecureMac, https://www.securemac.com/news/xcodespy-mac-malware-targets-developers. Zugriff am 9.7.2021.

A.13 WEBSITE DER REGIERUNG VON MYANMAR

Im Juni 2021 berichteten Forscher, dass ein Trojaner zur Verbreitung von Schadprogrammen in Ressourcen eingeschleust worden war, die auf der Website des Präsidenten von Myanmar gehostet wurden.[94] Der Angriff wurde nicht offiziell einer bestimmten APT-Gruppe zugeschrieben.[95] Allerdings wurden Merkmale festgestellt, die auf die APT-Gruppe Mustang Panda hindeuten.[94,96]

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code	Phishing [T1566], Infektion mit einem Schadprogramm	Menschen



[94] "ESETresearch uncovered a supply chain attack on the Myanmar president office website", Twitter, https://twitter.com/ESETresearch/status/1400165767488970764. Zugriff am 9.7.2021.
[95] Backdoor malware found on the Myanmar president's website, again, The Record by Recorded Future, https://therecord.media/backdoor-malware-found-on-the-myanmar-presidents-website-again/. Zugriff am 9.7.2021.
[96] Cobalt Strike Beacons Being Hosted on Myanmar President's Website, Binary Defense, https://www.binarydefense.com/threat_watch/cobalt-strike-beacons-being-hosted-on-myanmar-presidents-website/. Zugriff am 9.7.2021.

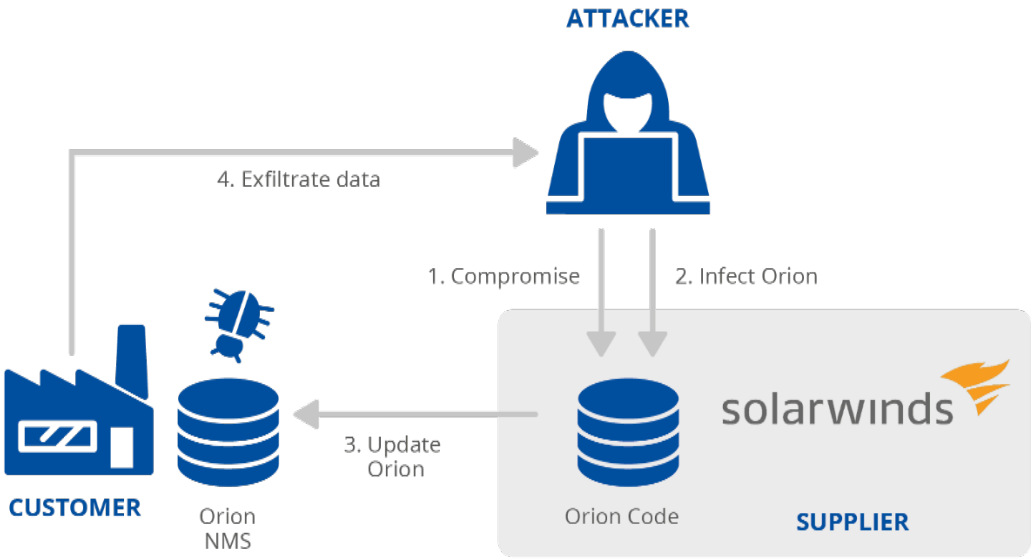
A.14 SOLARWINDS ORION: IT-MANAGEMENT UND ELEKTRONISCHE ÜBERWACHUNG

SolarWinds ist ein Anbieter von Management- und Überwachungssoftware.[97] Ein Produkt des Unternehmens ist das Netzverwaltungssystem (NMS, Network Management System) Orion.[98] Im Dezember 2020 wurde entdeckt, dass Orion kompromittiert worden war. In einer umfassenden Untersuchung wurde festgestellt, dass sich Angreifer Zugang zum SolarWinds-Netzwerk verschafft hatten, möglicherweise durch Ausnutzen einer Zero-Day-Sicherheitslücke in einer Anwendung oder einem Gerät eines Drittanbieters, durch einen Brute-Force-Angriff oder durch Social Engineering.[99] Nach dem Eindringen in das Netz sammelten die Angreifer über einen längeren Zeitraum Informationen.

Nach der Kompromittierung wurde ein Schadprogramm in den Erstellungsprozess von Orion eingeschleust.[99,100] Die kompromittierte Software wurde dann von den Kunden direkt heruntergeladen und ausgeführt und zum Sammeln und Abgreifen von Informationen genutzt.[101, 102] Der Angriff wurde der Gruppe APT29 zugeschrieben.[103]

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Software Brute-Force-Angriff, Social Engineering	Prozesse, Code	Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Daten

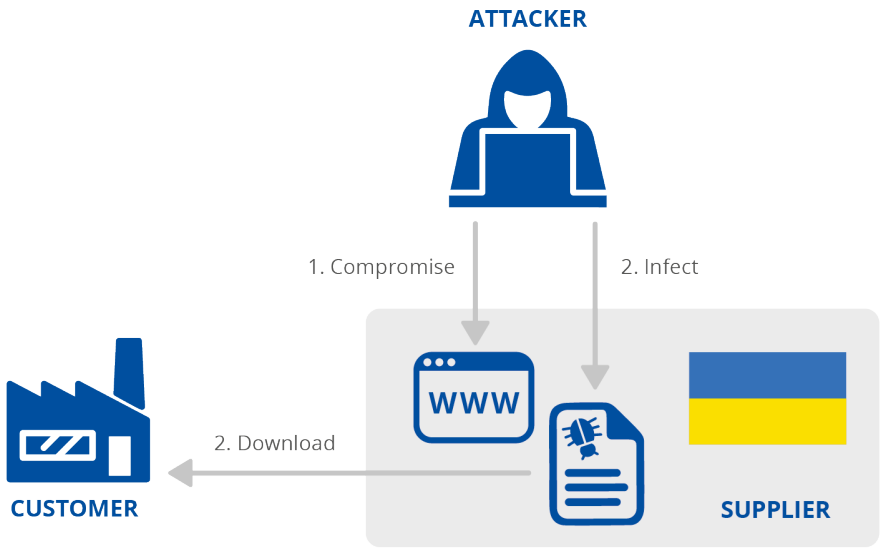
[97] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Zugriff am 9.7.2021.
[98] Orion Platform, SolarWinds, https://www.solarwinds.com/solutions/orion. Zugriff am 9.7.2021.
[99] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Zugriff am 9.7.2021.
[100] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Zugriff am 9.7.2021.
[101] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, ireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Zugriff am 9.7.2021.
[102] SUNBURST Additional Technical Details, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html. Zugriff am 9.7.2021.
[103] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Zugriff am 9.7.2021.


ATTACKER
4. Exfiltrate data
1. Compromise
2. Infect Orion
3. Update Orion
CUSTOMER
Orion NMS
Orion Code
solarwinds
SUPPLIER

A.15 UKRAINE SEI EB: SYSTEM OF ELECTRONIC INTERACTION OF EXECUTIVE BODIES

Die ukrainische Regierung und öffentliche Stellen nutzen das Webportal SEI EB (System of Electronic Interaction of Executive Bodies) zum Austausch von Dokumenten.[104] Im Februar 2021 wurde berichtet, dass das Portal von Angreifern durch das Hochladen von Dokumenten mit Schadcode kompromittiert worden war.[105] Über die Dokumente mit dem Schadcode wurden die Systeme der Nutzer später mit Schadprogrammen zum Sammeln und Abgreifen von Informationen infiziert. Der Angriff wurde mit mehreren APT-Gruppen in Verbindung gebracht. Eine Zuordnung zu einer bestimmten Gruppe war jedoch nicht möglich.[104]

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code	Infektion mit einem Schadprogramm	Menschen, Daten



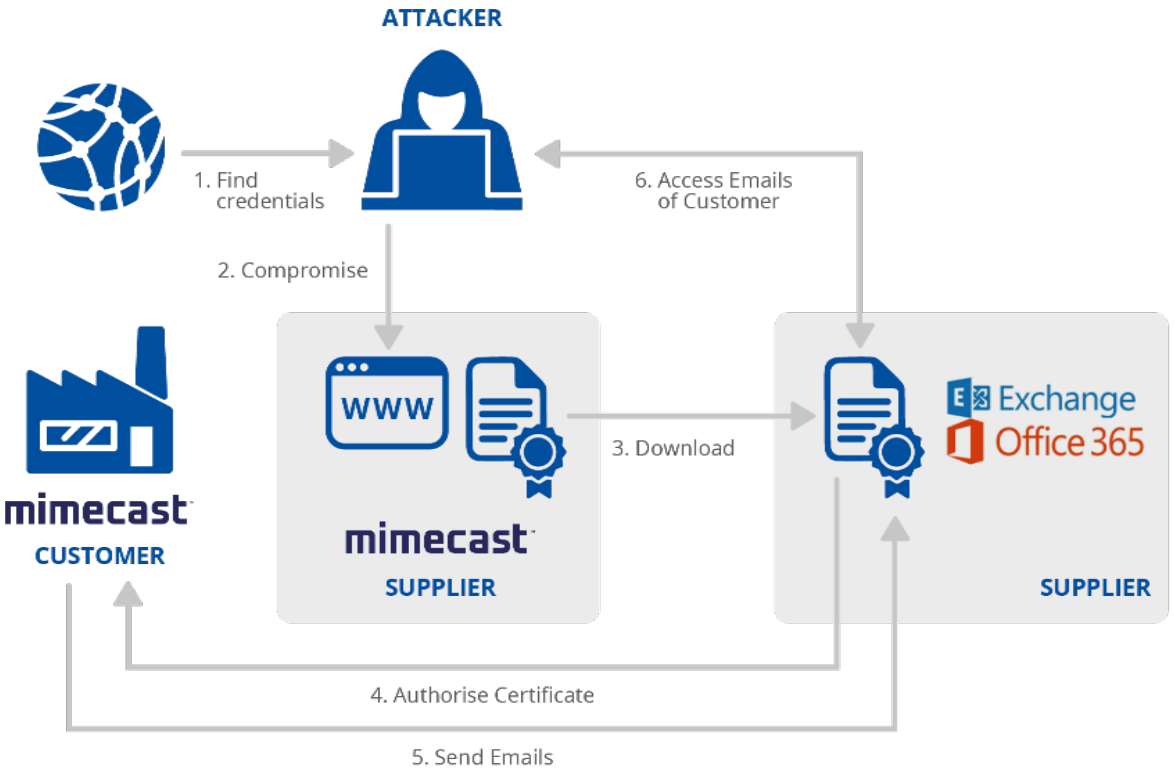
[104] Russian hackers aim cyber attack on Ukrainian government agencies, Teiss News, https://www.teiss.co.uk/russian-hackers-targeting-ukrainian-government-agencies/. Zugriff am 9.7.2021.
[105] The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies, National Security and Defense Council of Ukraine, https://www.rnbo.gov.ua/en/Diialnist/4823.html. Zugriff am 9.7.2021.

A.16 MIMECAST: CYBERSICHERHEITSDIENSTE IN DER CLOUD

Mimecast ist ein Anbieter von Cloud-basierten Cybersicherheitsdiensten.[106] Das Unternehmen bietet unter anderem E-Mail-Sicherheitsdienste an, bei denen die Kunden eine sichere Verbindung zu den Mimecast-Servern herstellen müssen, damit sie ihre Microsoft-365-Konten nutzen können. Im Januar 2021 wurde entdeckt, dass Angreifer Mimecast (über den Lieferanten SolarWinds) kompromittiert hatten. Nach der Kompromittierung hatten die Angreifer Zugriff auf ein von Mimecast ausgestelltes und von Kunden für den Zugriff auf Microsoft-365-Dienste verwendetes Zertifikat. Anschließend konnten sie die Netzwerkverbindungen abfangen und sich mit den Microsoft-365-Konten verbinden, um Informationen abzugreifen.[107, 108] Der Angriff wurde der Gruppe APT29 zugeschrieben.[109] Die Kompromittierung des Lieferanten wurde Berichten zufolge mit SolarWinds in Verbindung gebracht, es liegen jedoch keine zuverlässigen Informationen darüber vor, wie der Angriff im Einzelnen erfolgte.

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Daten

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Vertrauensbeziehung [T1199]	Daten



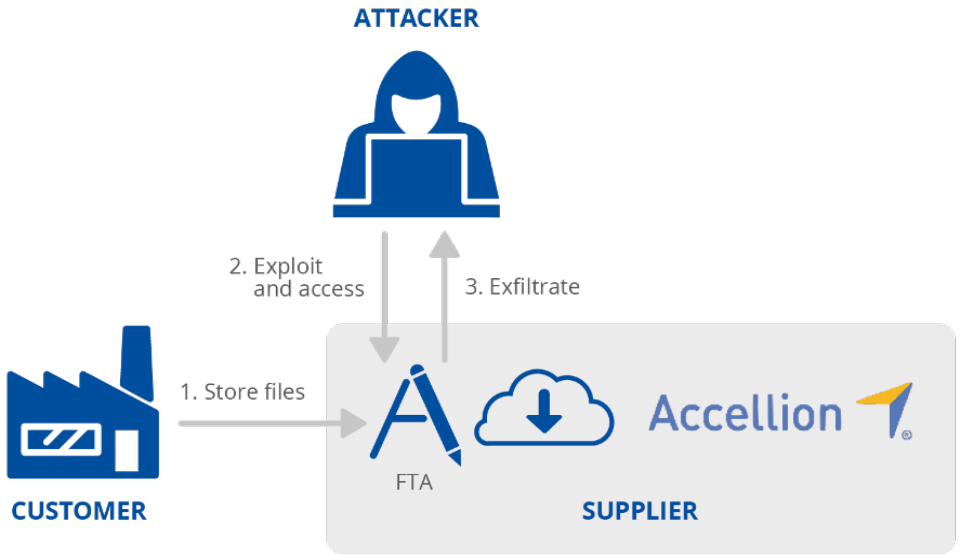
[106] Our Company, Mimecast, https://www.mimecast.com/company/. Zugriff am 9.7.2021.
[107] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. Zugriff am 9.7.2021.
[108] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Zugriff am 9.7.2021.
[109] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Zugriff am 9.7.2021.

A.17 ACCELLION: FTA-SOFTWARE (FILE TRANSFER APPLIANCE)

Accellion ist ein Unternehmen, das Sicherheitssoftware für Unternehmen anbietet, insbesondere Anwendungen zum sicheren Austausch von Dateien (Filesharing) und Kollaborationsanwendungen.[110] Im Dezember 2020 meldete Accellion, dass Angreifer mehrere Zero-Day-Sicherheitslücken in ihrer FTA-Software ausgenutzt hatten, um sich Zugang zu Kundendaten zu verschaffen[111, 112] und diese über eine Webshell abzufangen. Viele Unternehmen, die von diesen Sicherheitslücken betroffen waren, wurden unter Androhung einer Veröffentlichung der entwendeten Daten erpresst. Der Angriff wurde einer Gruppe von Cyberkriminellen mit der Bezeichnung UNC2546 zugeschrieben.[112]

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Software	Code

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Vertrauensbeziehung [T1199]	Daten



[110] About Accellion, Accellion, https://www.accellion.com/company/. Zugriff am 9.7.2021.
[111] File Transfer Appliance (FTA) Security Assessment, Accellion, https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf. Zugriff am 9.7.2021.
[112] Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion, FireEye Inc, https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html. Zugriff am 9.7.2021.

A.18 DAS FLUGGASTABFERTIGUNGSSYSTEM SITA

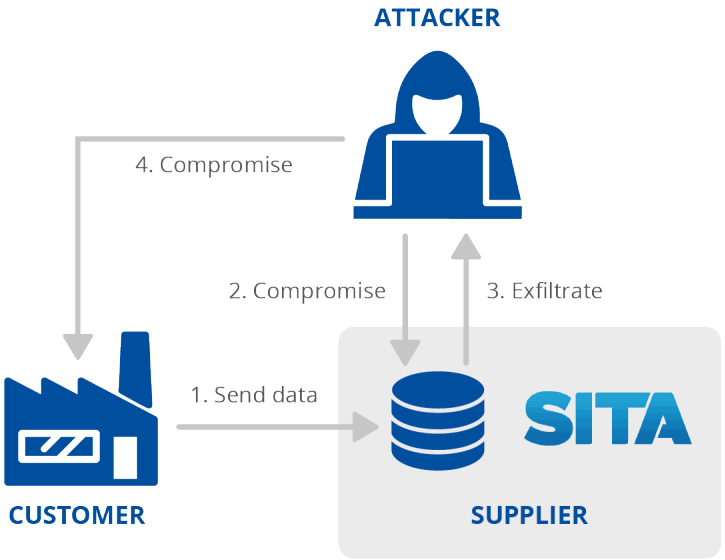
SITA ist ein Unternehmen, das sich auf IT-Anwendungen für den Luftverkehr und auf Verkehrsinformationen spezialisiert hat.[113] Das Fluggastabfertigungssystem von SITA dient dazu, den Fluggesellschaften beim Boarding Informationen über die Fluggäste zu liefern, u. a. zum Risiko, das die Fluggäste für ein Land darstellen könnten.[114] Im März 2021 wurde bekannt, dass Angreifer in die SITA-Server eingedrungen waren, um sich Zugang zu den Passagierdaten der Kunden von SITA zu verschaffen. Zudem meldeten einige Kunden von SITA Datenschutzverletzungen, u. a. Air India, Singapore Airlines und Malaysia Airlines.

Nach Berichten über Datenverluste im Internet meldete auch Air India, dass seine Netzwerke kompromittiert und Daten gestohlen wurden. Bei der Kompromittierung der internen Netzwerke von Air India wurde ein Zusammenhang mit dem Vorfall bei SITA vermutet, da ein Sicherheitsunternehmen feststellte, dass ein System von Air India die Bezeichnung „SITASERVER4“ trug.

Bislang ist weder bekannt, wie die Angreifer auf die SITA-Server zugreifen konnten, noch, wie sich die Angreifer Zugang zu Air India verschafft haben könnten oder ob ihnen dies tatsächlich gelungen ist. Der interne Angriff auf die Netzwerke von Air India wurde der Gruppe APT41 zugeschrieben.[115]

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Daten

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Personenbezogene Daten



[113] About us, SITA, https://www.sita.aero/about-us/. Zugriff am 9.7.2021.
[114] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Zugriff am 9.7.2021.
[115] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Zugriff am 9.7.2021.

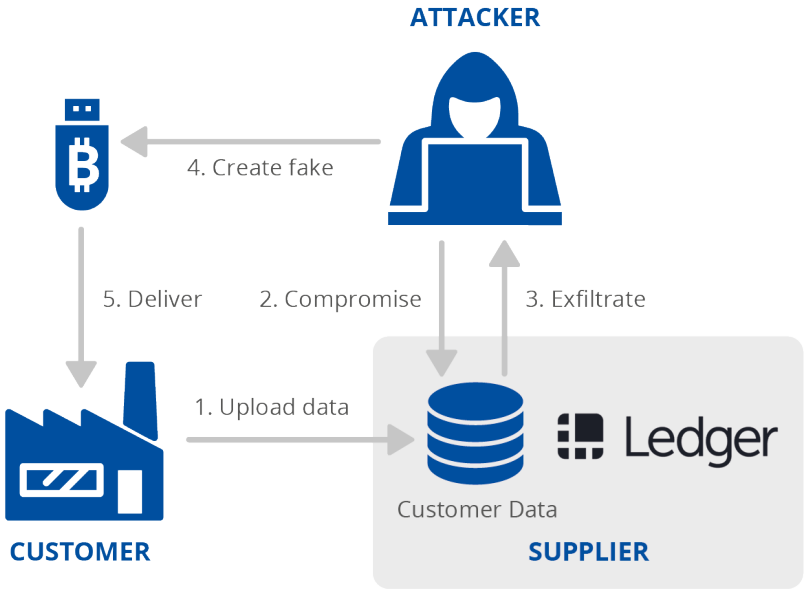
A.19 LEDGER: HARDWARE-WALLETS

Ledger ist ein Unternehmen, das Hardware-Wallet-Technologie für Kryptowährungen anbietet.[116] Im Juli 2020 verschafften sich Angreifer gültige Anmeldedaten, um auf die E-Commerce-Datenbank von Ledger zuzugreifen.[117] Wie die Angreifer auf die Anmeldedaten zugreifen konnten, ist nicht bekannt. Die gestohlenen Daten wurden in einem Online-Forum veröffentlicht.[118]

Die Angreifer nutzten die gestohlenen Daten für Online-Phishing und für die Erpressung von Nutzern[119, 120] sowie für den Diebstahl von Geldern der Nutzer durch einen physischen Angriff. Dazu übermittelten sie den Nutzern gefälschte Ledger-Wallets, die nach dem Aufbau einer Verbindung zu einem System die Nutzer nach ihren Sicherheitsschlüsseln fragten, das System mit einem Schadprogramm infizierten und die gestohlenen Informationen an die Angreifer zurückschickten[121]. Der Angriff konnte nicht zugeordnet werden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Daten	Ausnutzen einer Vertrauensbeziehung [T1199], Phishing [T1566], Fälschung	Finanzieller Schaden

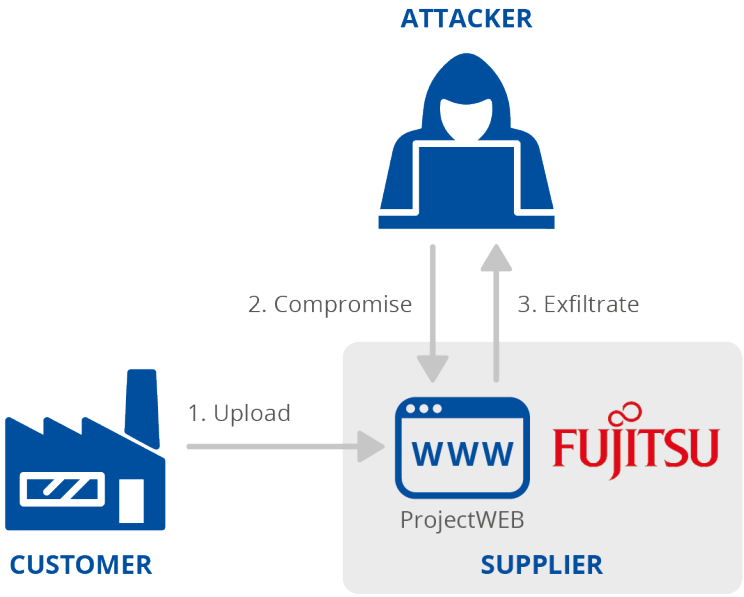
[116] Hardware Wallet, Ledger, https://www.ledger.com/. Zugriff am 9.7.2021.
[117] Addressing the July 2020 e-commerce and marketing data breach − A Message From Ledger's Leadership | Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Zugriff am 9.7.2021.
[118] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. Zugriff am 9.7.2021.
[119] Message by LEDGER's CEO − Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Zugriff am 9.7.2021.
[120] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html. Zugriff am 9.7.2021.
[121] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Zugriff am 9.7.2021.


ATTACKER
4. Create fake
5. Deliver
2. Compromise
3. Exfiltrate
1. Upload data
Ledger
Customer Data
CUSTOMER
SUPPLIER

A.20 FUJITSU PROJECTWEB: KOLLABORATIONS- UND PROJEKTMANAGEMENT-SOFTWARE

Fujitsu ProjectWEB ist eine Cloud-basierte Software, die Unternehmen zur Online-Kollaboration, zum Software-Management und zum Filesharing nutzen.[122] Das Tool ist bei japanischen Regierungsbehörden sehr beliebt. Im Mai 2021 verschafften sich Angreifer unter Ausnutzung von Sicherheitslücken in ProjectWEB-Installationen Zugang zu Daten der japanischen Regierung.[123. 122, 124] Wegen des Standorts der kompromittierten Server wurden bei dem Angriff auch Daten der japanischen Luftverkehrskontrolle entwendet.[122,125] Der Angriff konnte nicht zugeordnet werden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code, Daten	Unbekannt	Daten



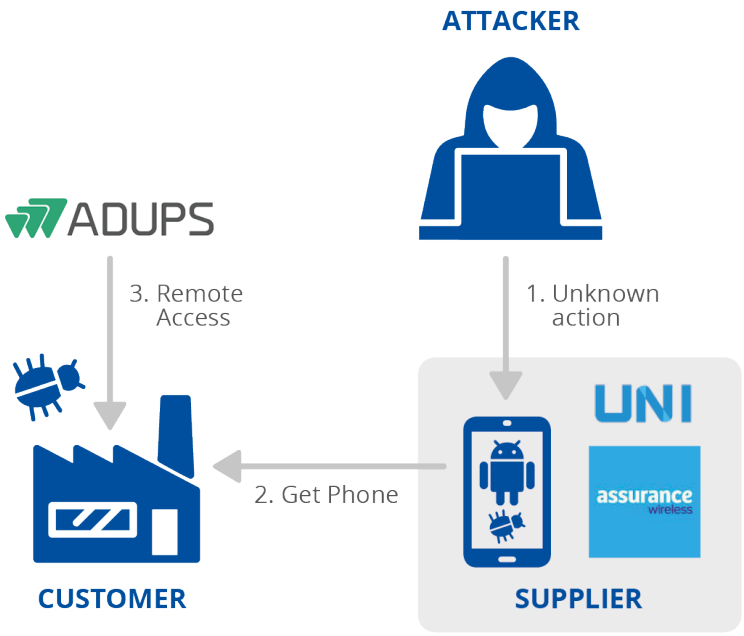
[122] Japanese government agencies suffered breaches after ProjectWEB hack, Teiss News, https://www.teiss.co.uk/japanese-government-agencies-suffered-breaches-following-fujitsus-projectweb-hack/. Zugriff am 9.7.2021.
[123] Japanese government agencies suffer data breaches after Fujitsu hack, Bleeping Computer, https://www.bleepingcomputer.com/news/security/japanese-government-agencies-suffer-data-breaches-after-fujitsu-hack/. Zugriff am 9.7.2021.
[124] Data theft via Fujitsu ProjectWEB, INCIBE-CERT, https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/data-theft-fujitsu-projectweb. Zugriff am 9.7.2021.
[125] Fujitsu pulls ProjectWEB tool offline after apparent supply chain attack sees Japanese infosec agency data stolen, The Register, https://www.theregister.com/2021/05/27/fujitsu_projectweb_supply_chain_attack/. Zugriff am 9.7.2021.

A.21 UNIMAX MOBILTELEFONE

Unimax, auch bekannt als UMX, liefert kostengünstige mobile Geräte. UMX-Telefone wurden auch von Personen genutzt, die ihre Telefone über das Lifeline Assistance Program der US-Regierung bezogen.[126] Im Januar 2020 berichteten Forscher, dass die mobilen Geräte mit nicht zu entfernenden, vorinstallierten Schadprogrammen ausgerüstet waren, die dafür vorgesehen waren, die Nutzer zu überwachen.[127, 128] Selbst mit einem Hard-Reset war es nicht möglich, die Schadprogramme zu entfernen. Transsion, ein weiterer Mobiltelefonhersteller, bei dem das vorinstallierte Schadprogramm gefunden wurde, beschuldigte einen nicht ermittelten Anbieter in der Lieferkette.[126] Der Angriff konnte nicht zugeordnet werden.[126]

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Unbekannt	Code

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Vertrauensbeziehung [T1199], Infektion mit einem Schadprogramm	Menschen

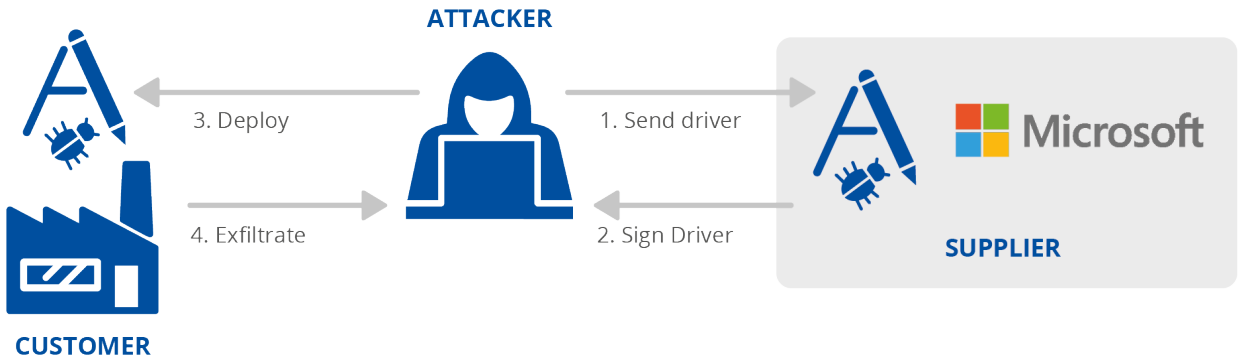


[126] Chinese Cell Phones Ship Preloaded with Malware, BlueVoyant, https://www.bluevoyant.com/blog/chinese-cell-phone-malware/. Zugriff am 9.7.2021.
[127] UMX Phone: US-funded Gov Phones come pre-installed with malicious apps, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/. Zugriff am 9.7.2021.
[128] We found yet another phone with pre-installed malware via the Lifeline Assistance program, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/07/we-found-yet-another-phone-with-pre-installed-malware-via-the-lifeline-assistance-program/. Zugriff am 9.7.2021.

A.22 MICROSOFT: WINDOWS-HARDWARE-KOMPATIBILITÄTSPROGRAMM

Im Juni 2021 wurde mitgeteilt, dass die Prozesse zur Code-Signierung, die Microsoft zur Validierung von Treibern von Drittanbietern verwendet, von Angreifern kompromittiert wurden, um ein Rootkit-Schadprogramm einzuschleusen und zu verbreiten.[129] Aufgrund der gültigen Signatur konnte das Schadprogramm auf den Systemen der Nutzer installiert werden.[130] Ziel des Angriffs war offenbar der Glücksspielsektor in China.[129] Der Angriff konnte nicht zugeordnet werden.

LIEFERANT		KUNDE	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte	Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Social Engineering	Prozesse	Ausnutzen einer Vertrauensbeziehung [T1199]	Daten



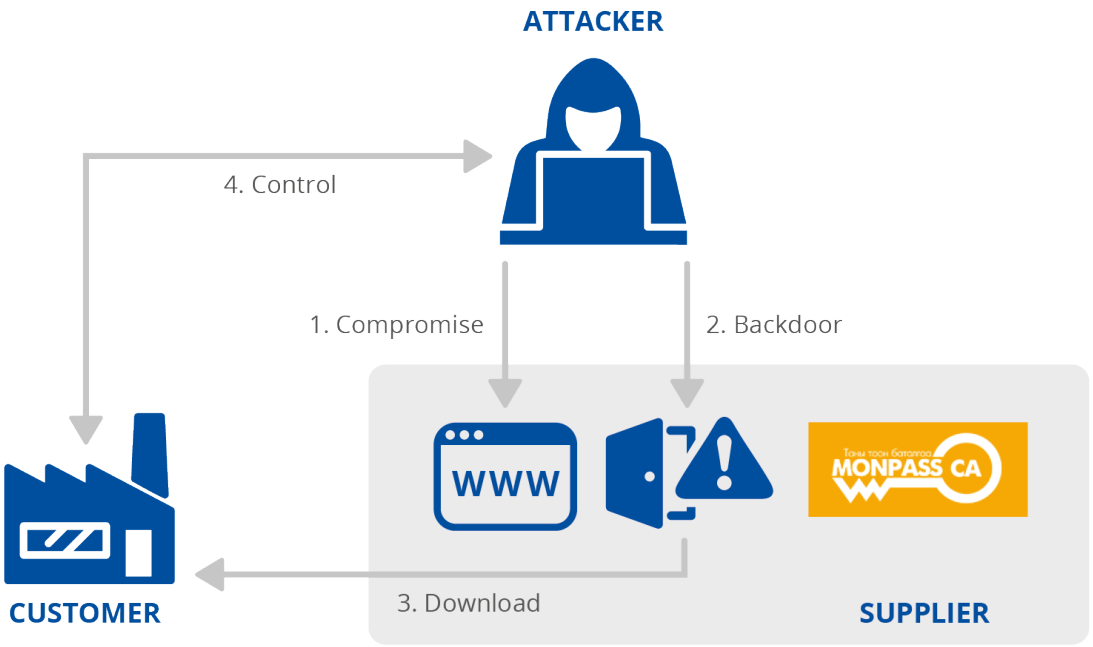
[129] Microsoft admits to signing rootkit malware in supply-chain fiasco, Bleeping Computer, https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/. Zugriff am 9.7.2021.
[130] Microsoft signed a malicious Netfilter rootkit, G DATA, https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit. Zugriff am 9.7.2021.

A.23 MONPASS: ZERTIFIZIERUNGSBEHÖRDE

MonPass ist die wichtigste Zertifizierungsbehörde der Mongolei. Im Februar 2021 wurde die MonPass-Website kompromittiert, und in mindestens ein Installationsprogramm wurde über Cobalt Strike ein Backdoor-Programm eingeschleust.[131] Die Website wurde mehrfach kompromittiert, und es wurden mehrere Webshells und Backdoor-Programme gefunden.[132] Das Schadprogramm wurde von Besuchern der MonPass-Website heruntergeladen, die das Schadprogramm nach dem Herunterladen ausführten. Von einer Avast-Software wurde eine Infektion bei mindestens einem Kunden nachgewiesen.[131]

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Software	Code

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Drive-by Compromise [T1189], Infektion mit einem Schadprogramm	Unbekannt



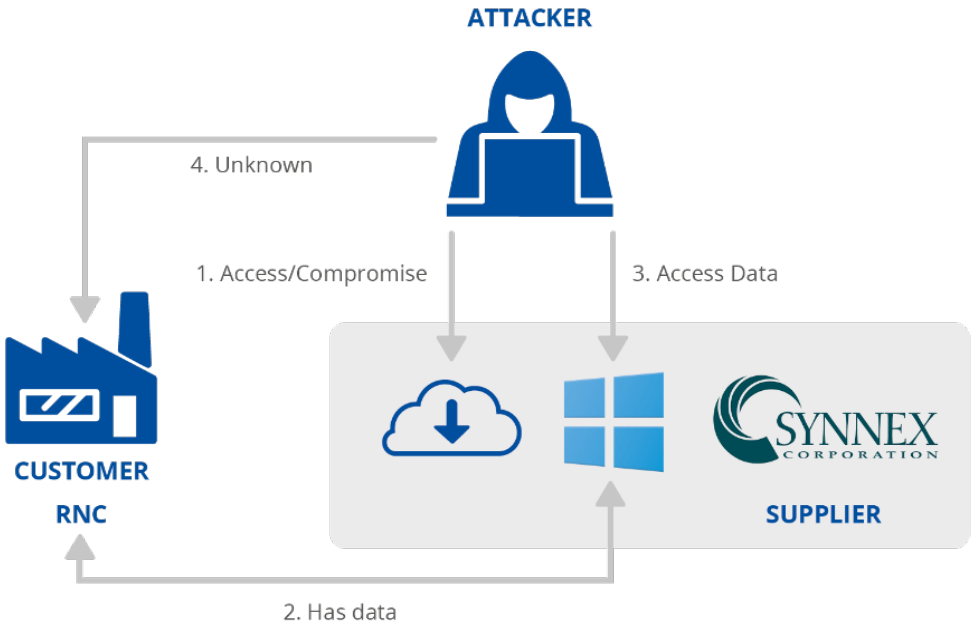
[131] Backdoored Client from Mongolian CA MonPass, Avast Threat Labs, https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/. Zugriff am 9.7.2021.
[132] Mongolian Certificate Authority Hacked to Distribute Backdoored CA Software, The Hacker News, https://thehackernews.com/2021/07/mongolian-certificate-authority-hacked.html. Zugriff am 9.7.2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.24 SYNNEX IT: ANBIETER VON TECHNOLOGIEPRODUKTEN

Synnex ist ein Anbieter und Integrator von Technologieprodukten. Im Juli 2021 wurde in die Systeme des Unternehmens eingedrungen.[133] Synnex räumte ein, dass die Angriffe möglicherweise im Zusammenhang mit den jüngsten Angriffen auf Kaseya-MSPs standen.[134] Die Angreifer nutzten Synnex, um auf Kundenanwendungen innerhalb der Microsoft-Cloud-Umgebung zuzugreifen. Zu diesen Anwendungen gehörte auch das National Committee der US-amerikanischen Republikanischen Partei (RNC), das berichtete, dass Angreifer über Synnex in seine Systeme eingedrungen waren.[135]

LIEFERANT	
Angriffstechniken zur Kompromittierung der Lieferkette	Lieferanten-Assets, auf die der Lieferkettenangriff abzielte
Ausnutzen einer Sicherheitslücke in einer Software	Code

KUNDE	
Angriffstechniken zur Kompromittierung des Kunden	Kunden-Assets, auf die der Lieferkettenangriff abzielte
Drive-by Compromise [T1189], Infektion mit einem Schadprogramm	Unbekannt



[133] Mega-distie SYNNEX attacked and Microsoft cloud accounts it tends tampered, The Register, https://www.theregister.com/2021/07/07/synnex_rnc_microsoft_attack/. Zugriff am 9.7.2021.
[134] SYNNEX Responds to Recent Cybersecurity Attacks and Media Mentions, SYNNEX Corporation, https://ir.synnex.com/news/press-release-details/2021/SYNNEX-Responds-to-Recent-Cybersecurity-Attacks-and-Media-Mentions/default.aspx. Zugriff am 9.7.2021.
[135] Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit, The Washington Post, https://www.washingtonpost.com/business/on-small-business/russia-cozy-bear-breached-gop-as-ransomware-attack-hit/2021/07/06/3e9e200a-de9b-11eb-a27f-8b294930e95b_story.html. Zugriff am 9.7.2021.

TP-05-21-171-DE-N

ÜBER DIE ENISA

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Sie wurde im Jahr 2004 gegründet und durch den Rechtsakt zur Cybersicherheit in ihrem Mandat weiter gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen und Einrichtungen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Kapazitätsaufbau und Sensibilisierung arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und nicht zuletzt ein sicheres digitales Umfeld für die Gesellschaft und die Bürgerinnen und Bürger Europas zu gewährleisten. Weitere Informationen über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-509-8
DOI: 10.2824/168593