LIEFERKETTENBEDROHUNGEN (SUPPLY CHAIN THREATS): DIE CYBERANGRIFFE AUF DIE DIGITALISIERUNG

Es war eine Lieferkettenbedrohung! Im Jahr 2021 vermutlich die Feststellung zu Cybervorfällen schlechthin, über die Experten tagelang diskutieren können. „Lieferkettenbedrohung“ ist in den letzten Jahren fast schon zu einem Modewort geworden und kann bei Cyberangriffen alles irgendwie verständlicher erscheinen lassen, ohne dabei zu sehr ins Detail zu gehen. Wir wollen Ihnen mit Stand September 2021 ein aktuelles Lagebild zu Lieferkettenbedrohungen liefern.

Lieferkette (Supply Chain), Lieferkettenmanagement (Supply Chain Management) und Lieferkettenbedrohungen (Supply Chain Threats) sind Begriffe aus der Praxis und kein in der betriebswirtschaftlichen Theorie entwickeltes Konzept, wie Karina Ankenbrand, Isabel Linß und Eric Sucky in ihrer Literaturanalyse zu Lieferkettenmanagement darstellen[1]. Denn bei Supply Chain Management handle es sich um kein in der betriebswirtschaftlichen Theorie entwickeltes Konzept, es handle sich dabei stattdessen um einen in der Unternehmenspraxis entstandenen Ansatz. Bei Cyberangriffen auf Lieferketten bzw. bei Lieferkettenbedrohungen sprechen Expertinnen und Experten in erster Linie von betroffenen Geschäftsprozessen in einem Unternehmen – und in diesem Zusammenhang mit ausgelagerter und daher mutmaßlich unsicherer Informationstechnologie.

Was ist eine praxisnahe Definition einer Lieferkettenbedrohung? Konkret handelt es sich um die mögliche Kompromittierung einer Software oder eines Cloud-/Online-Dienstes (Managed Service Provider), die zur Herstellung von Dienstleistungen oder Produkten eingesetzt wird. Etwa der Cyberangriff auf einen Rohstofflieferanten, der am Beginn eines Geschäftsprozesses beim Materialeinkauf steht, oder kompromittierte CAD-Software, die Schadsoftware verteilt, wären dafür zwei Paradebeispiele.

Warum beschäftigen wir uns bei BDO eigentlich mit diesem IT-spezifischen Fachthema? Welchen der folgenden Gründe halten Sie für den zutreffendsten?

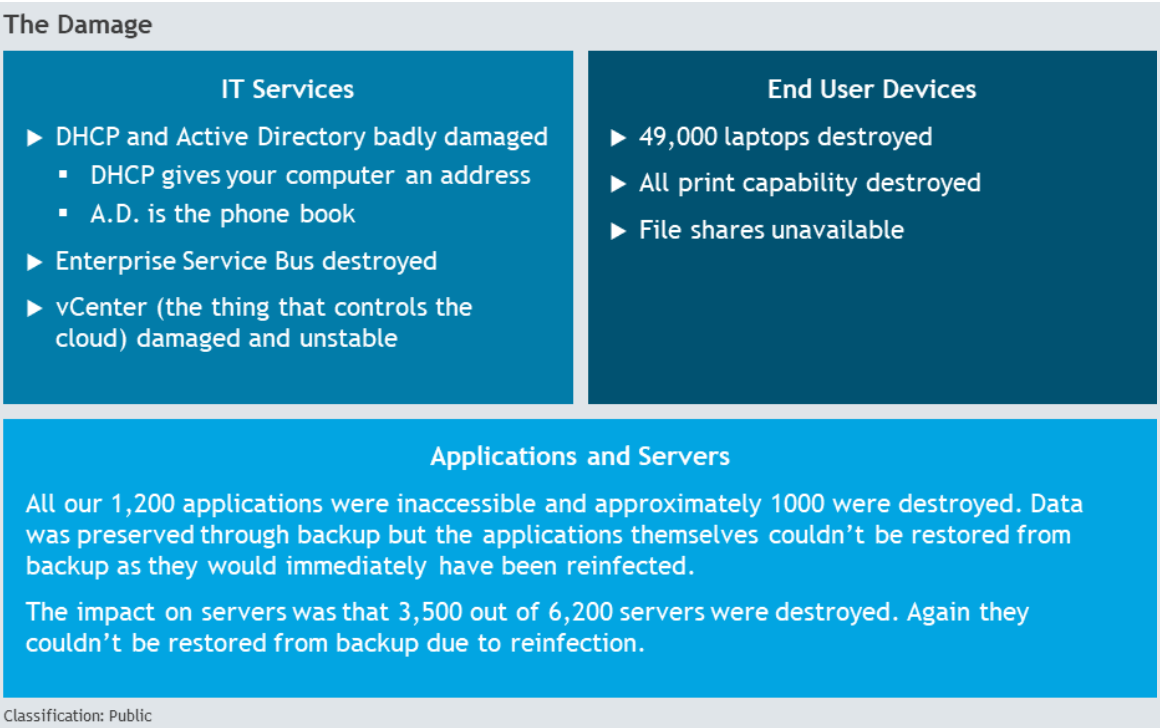
1. Lieferkettenbedrohungen stellen neben Ransomware (siehe auch „WOHIN ESKALIERT RANSOMWARE? – EIN AKTUELLES LAGEBILD ZU RANSOMWARE“) eine der größten Gefahrenquellen für vernetzte Industrie 4.0, kritische Infrastruktur und die Resilienz unserer Gesellschaft dar.
2. Technisch-organisatorische Maßnahmen können eine Lieferkettenbedrohung verhindern.
3. Cybersicherheit betrifft das Unternehmen als Gesamtes, also Management und Organe, Stakeholder, Lieferdienste als auch Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeiter.
4. Weil wir seit Jahren kontinuierlich Lieferkettenbedrohungen evaluieren und das Risiko für Kundinnen und Kunden bewerten.

Antwort: Die Punkte 1-4 treffen alle zu.

[1] vgl. Ankenbrand, Linß & Sucky. Theorie(n) des Supply Chain Managements: Eine Literaturanalyse. Bamberg: Otto-Friedrich-Universität, 2020. vgl. https://fis.uni-bamberg.de/handle/uniba/47075

LIEFERKETTEN-BEDROHUNGEN

In den meisten Fällen bleiben Cyberangriffe auf die Lieferkette für Wochen und Monate unentdeckt und verursachen dabei einen enormen bzw. existenzbedrohenden Schaden für Unternehmen. Logistikunternehmen und Reederei-Konzern A.P. Møller – Mærsk A/S (kurz Maersk) wurde im Jahr 2017 das Opfer eines solchen Cyberangriffs – und zwar eigentlich nur zufällig: Das Tochterunternehmen in der Ukraine hatte die Steuerabgaben-Software Intellect Service MeDoc eingesetzt, die von staatlichen Angreifern im Ausland (mutmaßlich Russland) kompromittiert und über Schadsoftware sabotiert worden war. Die darauffolgende Lieferkettenbedrohung bei Maersk war existenzbedrohend, wie Maersks CTIO und CISO im September 2019 eindrucksvoll bei einem öffentlichen Vortrag präsentierten:



Präsentation zu dem NotPetya-Vorfall bei Maersk vom September 2019 bei der Veranstaltung Information Security Europe 2019[2]

Die Gesamtschadenssumme dieses Geschäftsausfalles von mehreren Wochen durch die NotPetya-Sabotage-Attacke und über alle großen Geschäftsbereiche wie Maersk Line, APM Terminals & Damco, bezifferte der Reederei-Konzern schließlich mit einer Höhe von USD 300 Millionen[3]. Der ehemalige Maersk-IT-Mitarbeiter Gavin Ashton schrieb zu dem Vorfall einen bedeutenden Satz in seinem persönlichen und lesenswerten Blogbeitrag[4]:

„Organisations need to draw a connection between cyber risk and human capital. The lower the value they place on IT, on cyber risk, the lower the value they inherently place on the people turning the wheels."

[2] vgl. https://www.youtube.com/watch?v=_MwsxIS3tG8

[3] vgl. https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million

[4] vgl. https://gynshtn.com/maersk-me-notpetya

Ein Angriff auf die Liefer- oder Wertschöpfungskette?

In Medien hat sich der Begriff *Lieferkette* durchgesetzt, obwohl er nicht wie der Deckel zum Topf passt. Man denke bei Wertschöpfung zum Beispiel an virtuelle Güter, die in einer physischen Welt nicht mehr existieren (z.B. Kryptowährungen, soziale Netzwerke, Online-Computerspiele, Non-Fungible Token oder Cloud-Dienstleistungen), aber einen finanziellen Wert darstellen bzw. ökonomische Vorteile erzeugen. Wir meinen, *Wertschöpfungskette* wäre als Begriff adäquater, dieser hat sich aber nicht durchgesetzt.

Im Fokus unserer Betrachtung stehen daher Cyberangriffe auf die Lieferkette – kurzum virtuelle Lieferkettenbedrohungen. Neben dem Cyberspace gibt es durchaus physische Angriffe auf Lieferketten (z.B. unerlaubte Entnahme im Warenlager) oder dolose Bauteile in Computer-Hardware, die nachträglich von unautorisierten Dritten in der Auftragsproduktion hinzugefügt wurden. Zu den physischen Angriffen zählen beispielsweise die bewusste Verunreinigung von Rohstoffen in der Konsumgüterindustrie zum Zweck einer Erpressung oder auch gefälschte Produkte, die in die Lieferkette eingeschleust über einen Großhändler beim Konsumenten landen[5]:

Die internationalen Behörden EUROPOL und INTERPOL beschlagnahmten – über lokale Partnerbehörden – im Zeitraum von Dezember 2020 bis Juni 2021 über 15.000 Tonnen an gefälschten Nahrungsmitteln, wie bspw. Energy Drinks, Olivenöl oder Milchpulver, die von Fälschern in Lieferketten eingeschleust und betrügerisch weiterverkauft wurden.

Auch die nachträgliche Veränderung von Computer-Hardware, zwecks Sabotage oder Spionage, gehört zur Lieferkettenbedrohung, wird jedoch im Expertenkreis äußerst kontrovers diskutiert. Bis heute wird der Artikel „*The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*“ in Bloomberg Businessweek[6] stark kritisiert, da der tatsächliche Nachweis von gefälschten Chips auf den Platinen des Computer-Herstellers Supermicro von den Autoren und deren anonymen Quellen nicht erbracht werden konnte.[7]

Diese und vermeintlich weitere Bloomberg-Enthüllungen[8] wurden zeitweise zu einem ernsthaften Problem für das Herstellerunternehmen Supermicro, das wichtige Großkunden und somit an Börsenwert verlor, obwohl ein professionelles Gutachten keine Implantate auf der Server-Hardware feststellen konnte. Sogar der Nachrichtendienst der Vereinigten Staaten (NSA) konnte die Bloomberg-Enthüllungen zu Spionage-Chips in Stellungnahmen nicht weiter nachvollziehen.

Auch die N.S.A. selbst wurde der Manipulation von Netzwerkroutern der Firma Cisco bezichtigt, wie ein Foto aus den Enthüllungen von Edward Snowden belegt:

[5] vgl. https://www.europol.europa.eu/newsroom/news/15-000-tonnes-of-illegal-food-and-beverages-market

[6] vgl. Robertson, Jordan & Riley, Michael. „The Big Hack: How China Used a Tinoy Chip to Infiltrate U.S. Companies.” In: Bloomberg Businessweek, 4.10.2018 unter https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[7] vgl. https://www.datacenterdynamics.com/en/news/years-later-bloomberg-doubles-down-disputed-supermicro-supply-chain-hack-story

[8] vgl. https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom

NSA-Mitarbeitende öffnen eine Cisco-Lieferung für einen ahnungslosen Kunden.
Beitrag aus dem Jahr 2015 zu „Intercept-and-Implant" der NSA.[9]

In Summe sind die öffentlichen Informationen zur Kompromittierung von Computer-Hardware in Lieferketten bis dato eher spärlich. Eine der vermutlich spannendsten Enthüllungen der letzten Jahrzehnte wurde dann im Jahr 2020 publik:

Von Kryptomaschinen, Raclette und Schoki

Seit den 1960er-Jahren bis in die späten 1990er-Jahre soll die verschlüsselte Kommunikation von Regierungen, Botschaften, Banken und Konzernen durch manipulierte kryptographische Algorithmen erfolgreich kompromittiert worden sein. Die schweizerische Crypto AG, ein Hersteller kryptographischer Kommunikationslösungen aus dem Kanton Zug, soll über Jahrzehnte unbekannterweise von zwei ausländischen Aktionären gesteuert worden sein: Dem Auslandsgeheimdienst der Vereinigten Staaten (CIA) und dem deutschen Bundesnachrichtendienst. Aufgeflogen ist das Ganze nur, weil der ehemalige Verkaufschef Hans Bühler im Jahr 1994 seinen Arbeitgeber nach der Verhaftung im Iran auf Schadenersatz klagen wollte. Die Schweizer Chefs wollten nämlich von Bühler die im Iran hinterlegte Kaution zurück und baten ihren Ex-Verkaufschef doch bitte schön Regress gegen *„unseren deutschen Aktionär"*[10] einzulegen, den ihm aber keiner nennen wollte oder konnte. Das Verhalten der Crypto AG Geschäftsführung gegen Bühler, der wegen den Schwachstellen in den Produkten seiner Firma im Iran mutmaßlich gefoltert worden war, löste bei ehemaligen Mitarbeitenden eine Flutwelle von Enthüllungen über die Crypto AG aus: Bereits seit ihrer Gründung im Jahr 1955[11] wurden die kryptographischen Algorithmen systematisch aufgeweicht, dawmit Regime wie der Iran, das damalige Libyen unter Gaddafi oder internationale Großbanken von Nachrichtendiensten abgehört werden konnten. Im Sommer 2020 erlangten internationale Medien die geheimen Dokumente zu den Aktionären Thesaurus und Rubicon, was ein veritables Politgewitter im

[9] vgl. https://www.techdirt.com/articles/20150320/08335930383/cisco-shipping-hardware-to-bogus-addresses-to-throw-off-nsa-intercept-and-implant-efforts.shtml

[10] vgl. https://www.infosperber.ch/index.cfm?go=Artikel/FreiheitRecht/NSA-BND

[11] vgl. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Schweizer Bundestag auslöste. Schließlich wurde dann auch noch die Infoguard AG aus dem Kanton Zug als zweites (ehemaliges) CIA-Tochterunternehmen enttarnt und verlor damit seine Reputation als Schweizer IT-Sicherheitsunternehmen.

ZARF und wie alles begann

Die Lieferkette hat, wie einleitend bereits erwähnt, in der betriebswirtschaftlichen Praxis die Aufgabe, dass Produkte gebrauchsfertig bei Konsumenten landen. Im Jahr 1985 behandelte Michael Porter in seinem Klassiker „*Competitive Advantage: Creating and Sustaining Superior Performance*“[12] die Wertschöpfungskette (Value Chain), wobei Porter sich auf die notwendigen Prozesse in einem Unternehmen bezog, um die angelieferten/abgebauten Rohstoffe in ein fertiges Produkt zu transformieren. Wann wurde die Lieferkettenbedrohung in der IT-Welt etabliert? Der erste dokumentierte Angriff auf eine Lieferkette in der Informationstechnologie – Codename ZARF – erfolgte im Jahr 1973 und wurde erst im Jahr 1979 in einem Aufsatz veröffentlicht[13]:

Die US Air Force beauftragte den damaligen Computer-Hersteller Honeywell Information Systems mit der Auslieferung von besonders sicheren Computer-Systemen für die Radaraufklärung. Auf den Großrechnern von GE und Honeywell lief das Betriebssystem Multics, das für damalige Verhältnisse bereits sehr komplex und mächtig war sowie über eine Benutzersegmentierung mit Passwörtern verfügte[14] – der Vorläufer heutiger Unix-Betriebssysteme. Bei einem Testangriff der US Air Force durch ein „Tiger Team“[15] auf Honeywell, konnte der Code im Betriebssystem Multics über eine Hintertür im Quellcode manipuliert werden, was bei Honeywell nicht entdeckt und somit an Kundinnen und Kunden weiterverteilt wurde: „*The manufacturer could not find it, even when he knew it existed and how it worked. Furthermore, since the trap door was inserted in the master copy of the operating system programs, the manufacturer automatically distributed this trap door to all Multics installations.*”[16]

Die erste Lieferkette in der Informationstechnologie war somit als Machbarkeitsstudie erfolgreich kompromittiert worden.

Roger Schell, damaliger Air Force Oberstleutnant, Professor und IT-Unternehmer, ist heute eine Legende der IT-Sicherheit und ein Urgestein von eCommerce-Sicherheit im Internet. Sein damaliges Tiger Team bestand neben der US Air Force auch aus Experten der MITRE Corporation, einem amerikanischen Think-Tank, der im Jahr 1958 gegründet wurde. Seine Methodik für die Risiko-Analyse von kritischen Schwachstellen findet auch heute bei BDO Anwendung.

[12] vgl. Porter, M. E. The Competitive Advantage: Creating and Sustaining Superior Performance. NY: Free Press, 1985

[13] Einige historische Quellen erwähnen das Jahr 1974 statt 1973.

[14] vgl. https://en.wikipedia.org/wiki/Multics

[15] Damals gängiger und militärischer Fachbegriff für heutige „Red Teams“: Eine Gruppe von zivilen und/oder militärischen Spezialistinnen und Spezialisten, die Sicherheitsvorkehrungen im Cyberspace und der realen Welt unbemerkt umgehen kann, dabei aber keinen nachhaltigen Schaden hinterlässt.

[16] vgl. https://web.archive.org/web/20021018132314/http://www.airpower.maxwell.af.mil/airchronicles/aureview/1979/jan-feb/schell.html

Von Stillhaltevereinbarungen und Machtansprüchen

Im Jahr 2021 überraschte das IT-Magazin WIRED mit dem aufsehenerregenden Artikel *„The Full Story of the Stunning RSA Hack Can Finally Be Told“*[17]: Nach dem Auslaufen eines zehnjährigem Embargos durften erstmals (ehemalige) Mitarbeiterinnen und Mitarbeiter des amerikanischen Unternehmens RSA Security[18] in der Öffentlichkeit zu einem Sicherheitsvorfall sprechen: Im März 2011 konnten mit China-assoziierte Hacker die geheimen Startwerte (Seeds) der RSA SecureID-Verschlüsselungstechnologie entwenden und somit selbstständig alternative Zugangscodes für die hardwarebasierte Mehrfaktor-Authentifizierung erzeugen.

Kurz erklärt: Computer können keine wirklichen Zufallswerte generieren, sondern nur Pseudozufallszahlen und benötigen dafür Startwerte. Beispielsweise ist die aktuelle Uhrzeit in Sekunden plus Datum ein typischer Startwert für einen Pseudozufallszahlengenerator, was aber heutzutage leicht nachgerechnet werden kann. In 10 Jahren vergehen 315.360.000 Sekunden, was für moderne Computer auch keine rechnerische Herausforderung mehr ist.[19] Daher erzeugte die RSA damals schon ihre eigenen Startwerte (Seeds) nach einer geheimen Methode. Der für viele als Goldstandard geltende Mehrfaktorschutz von RSA konnte so von Cyberspionen für eigene Zwecke umgangen und sensitive Ziele in den USA ausspioniert werden. Der WIRED-Journalist Andy Greenberg bezeichnet das Vorgehen rund um RSA als den vermutlich ersten wirklichen Cyberangriff auf eine Lieferkette, der über den Datendiebstahl bei RSA amerikanische Rüstungsfirmen wie Lockheed, Northrop Grumman and L-3 zum Ziel einer staatlichen Spionagekampagne machte.

Unsere erstmalige Berührung mit dem Thema erfolgte 2017, als Cyberspione die Computer-Optimierungssoftware CCleaner kompromittierten, um bei Millionen von Anwendern nur gezielte 40 auszuspionieren – darunter hauptsächlich Unternehmen aus Taiwan. Auch wir waren kurzfristig ein Opfer dieser Kampagne, konnten die Software aber noch rechtzeitig entfernen. Wenig später wurde im Jahr 2018 der taiwanesische PC-Hersteller ASUSTek Computer Inc. (kurz ASUS) zum Opfer einer Lieferkettenbedrohung, als virtuelle Eindringlinge den Update-Server von ASUS missbrauchten, um die PCs seiner taiwanesischen Kundinnen und Kunden über ASUS-Software-Updates zu kompromittieren.

Bis dato entkamen viele Internetnutzerinnen und -nutzer einer Lieferkettenbedrohung dadurch, da sie weder ASUS noch kompromittierte Software wie CCleaner verwendeten. Aufmerksame Leserinnen und Leser erkennen bereits, welche weitere Wirtschaftsmacht sich hier für Lieferkettenangriffe zum Zwecke der Spionage interessiert.

Über Bedrohungen, Schwachstellen und Gefährdungen

Wie und wo ordnen Sicherheitsexperten die Lieferkettenbedrohung fachlich ein? Trifft eine Bedrohung auf eine durch insbesondere technische oder organisatorische Mängel ausgelöste Schwachstelle, so entsteht – gemäß Definition[20] des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) – eine Gefährdung:

Bedrohung + Schwachstelle ⇒ Gefährdung

[17] vgl. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told

[18] vgl. https://en.wikipedia.org/wiki/RSA_Security

[19] vgl. https://www.heise.de/news/Kasperskys-Passwort-Manager-gefaehrdete-Benutzer-mit-ratbaren-Passwoertern-6130796.html

[20] IT-Grundschutz-Kompendium, 2. Edition 2019, Reguvis Bundesanzeiger Verlag

Das BSI definiert in seiner taxativen Sammlung diverse Beispiele für Bedrohungen wie höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen.

Ewald Kager, Partner bei BDO, erkennt folgende Bedrohungsszenarien im Cyberspace (Internet):

1. *Fernbedrohung: Netzwerkattacke über das Internet*
2. *Nahbedrohung: Angriff aus nächster Entfernung über drahtlose Netzwerke (Bluetooth, WiFi)*
3. *Insiderbedrohung: Kompromittieren des Systems vor Ort durch Insider*
4. *Lieferkettenbedrohung: Kompromittieren von Systemen durch Liederanten (z.B. Electronic-Data-Interchange, USB-Sticks, Festplatten, Outsourcing, etc.)*

Die hier genannten Bedrohungen im Internet sind grundsätzlich vorsätzlich, auch wenn es irrtümlich andere Benutzerinnen und Benutzer oder Unternehmen trifft. Sowohl das Bundesamt für Sicherheit in der Informationstechnik, die amerikanische MITRE Organisation, als auch internationale Cybersicherheitsfirmen kennen detaillierte Verfeinerungen in ihren Bedrohungsstufen und Gefährdungen. Vereinfachend beobachten wir immer eine von drei der folgenden Grundgefährdungen – umgangssprachlich die Cyberrisiken – als Resultat einer vorsätzlichen Handlung durch Aktivisten, kriminelle Banden/Gruppierungen/Täter oder staatliche Angreifer:

- **Cyberkriminalität:** Diebstahl/Erzeugung/Erpressung/Umleitung von Geldwerten (z.B. Angriffe auf Bezahlungssysteme, Cryptojacking von Kryptowährungen, Erpressung mit Ransomware). Die MITRE Organisation etwa kategorisiert den Angriff für Cryptojacking als „T1496 Resource Hijacking“ (Ressourcenklau).
- **Cybersabotage:** Verhinderung von Diensten durch die Versklavung von massenweise kompromittierten Computern (Botnets) für massive Cyberangriffe auf Internetserver, die Verunstaltung von Webseiten oder die Erstellung und Verteilung von gefälschten Nachrichten über soziale Medien. Das BSI kategorisiert die elementare Gefährdung einer Sabotage beispielsweise als „G040 Verhinderung von Diensten (Denial of Service)“.
- **Cyberspionage:** Verschaffung von Vorteilen durch den Diebstahl von schützenswerter Information (z.B. Eindringen und Erkunden, Keylogger, Datenlecks, Spyware), worunter auch Industriespionage und Stalking fallen. Das BSI kategorisiert die elementare Gefährdung einer Spionage beispielsweise als „G014 Ausspähen von Informationen (Spionage)“ oder als „G015 Abhören“.

Die von uns gewählte Vereinfachung in nur drei Grundgefährdungen mag zwar für Expertinnen und Experten vielleicht weniger befriedigend sein, ermöglicht jedoch Ihnen in Lagebildern und Analysen eine schnelle allgemeinverständliche Darstellung. Expertinnen und Experten erhalten immer ein Gesamtbild, da wir bei Analysen ebenso ergänzend die ATTACK-Methodik der MITRE Organisation darstellen.

Die Agentur der Europäischen Union für Cybersicherheit (ENSIA) definiert in einem aktuellen Arbeitspapier[21], welche Unternehmenswerte (Assets) es bei Cyberangriffen auf die Lieferkette zu schützen gilt – wir haben die Aufzählung der ENSIA übernommen und adaptiert:

- **Unternehmensdaten:** Dabei handelt es sich um alle Daten, die von einem Unternehmen eingekauft, generiert/erzeugt oder verkauft werden. Viele Unternehmensdaten stellen wertvolles intellektuelles Eigentum dar, das den Marktwert in Kapitalmärkten oder den Umsatz beeinflussen kann.
- **Personenbezogene Daten:** Dazu gehören beispielsweise Ausweiskopien von Kundeninnen und Kunden, aber auch u.a. Reisepasskopien von Mitarbeitenden, die für den Nachweis einer Mittelherkunft oder zum Zwecke einer Geschäftsreise gemacht wurden.

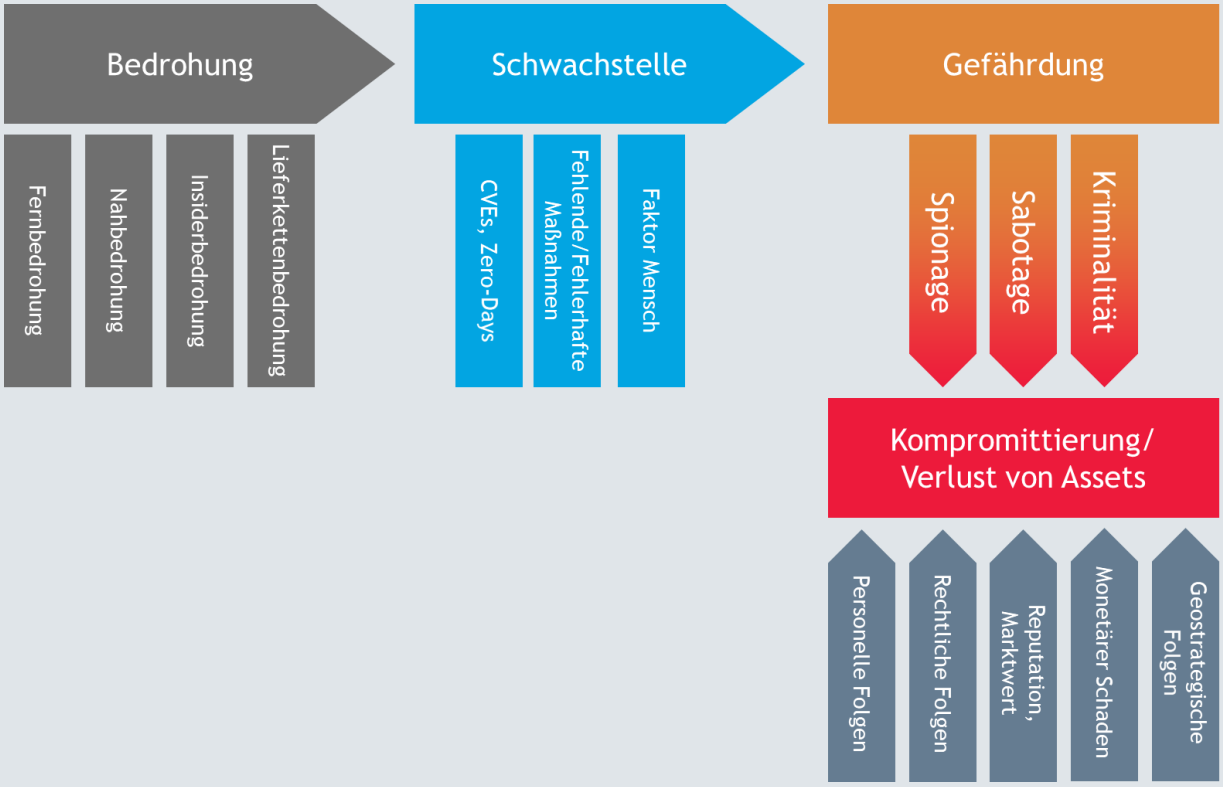
[21] vgl. „*ENISA Threat Landscape for Supply Chain Attacks*“ mit Stand Juli 2021

- **Software-Quellcode:** Dazu gehört der Quellcode, der ein eigenes Produkt (z.B. Anwendung) oder eine Dienstleistung (z.B. Vermittlung über ein Online-Portal) betrifft. Das kann von harmlosen Sammlungen von Fragmenten aus öffentlichen Bibliotheken, bis hin zu komplexen Software-Bibliotheken für industrielle Steueranlagen (z.B. SCADA) in kritischen Sektoren reichen.
- **Prozesse:** Viele Geschäftsprozesse werden mittlerweile über Unternehmensdaten und Software abgebildet oder in elektronischen Systemen gespeichert bzw. stellen die dafür notwendigen Datenbanken intellektuelles Eigentum dar. Das Wissen zu Prozessen durch unbefugte Dritte ermöglicht weitere Angriffe auf andere Werte, beispielsweise der Freigabeprozess für eine Geldüberweisung oder die Erstellung von virtuellen Gütern.
- **Bereitstellung von Diensten:** Die Verhinderung von Diensten wie Internetbandbreite, Speicherplatz in der Cloud oder Prozessorkapazitäten auf einem Server kann Unternehmen oder Institutionen lähmen und somit finanziell schädigen. Verteilte Angriffe über Zombie-Netzwerke (Distributed Denial of Service) und das illegale Erzeugen von Kryptowährungen sind dabei die Hauptgefahrenquellen. Im Jahr 2020 wurden mehrfach Cyberangriffe auf europäische Supercomputer-Zentren bekannt, wobei später eine illegale Erzeugung von Kryptowährungen nachgewiesen werden konnte.
- **Finanzielle Werte:** In diese Kategorie fallen Cyberangriffe auf alle Arten von Zahlungssystemen, die einen unmittelbaren finanziellen Schaden auslösen. In den meisten Fällen sind diese Werte unwiderruflich verloren oder nur unter hohem ökonomischen Einsatz und nur teilweise rückholbar. Der im August 2021 erfolgte Cyberangriff auf das DeFi Network, eine Blockchain-Alternative zu Kreditinstituten, hätte einen bis dato rekordverdächtigen Gesamtschaden von USD 600 Mio. verursachen können, wenn der/die Angreifer nicht freiwillig die kurzfristig entwendeten Kryptowährungen retourniert hätte.
- **Virtuelle Werte:** Eine neue Unterkategorie der finanziellen Werte stellen Kryptowährungen oder rein-virtuelle Güter (Stichwort: Tokenisierung bzw. „Non-Fungible Token“) dar, wozu auch fiktive Ausrüstungsgegenstände in Computerspielen (z.B. Schwerter, Markenturnschuhe), animierte Kurzfilme, Smileys oder sogar historische Twitter-Benutzerbeiträge[22] gehören können. Bis dato waren es hauptsächlich online-registrierte Markennamen in sozialen Medien und vor allem Domains. Für die Erstellung und Ausgabe von virtuellen Gütern werden mittlerweile hohe und bis zu fünfstellige Summen geboten. In Asien gibt es bereits eine Gruppierung (WINNTI), die sich – neben Industriespionage – auf den Diebstahl solcher virtuellen Werte spezialisiert hat. Da viele Start-ups auf virtuelle Werte fokussieren, wird auch diese Kategorie in naher Zukunft an Bedeutung zunehmen.
- **Personen:** In der heutigen Zeit gilt es auch die Reputation der eigenen Mitarbeiterinnen und Mitarbeiter zu schützen, da diese unmittelbare Auswirkungen auf die Kreditwürdigkeit oder Karriere einer betroffenen Person haben kann. Bestimmte kriminelle Gruppierungen versuchen etwa mit sensiblen Inhalten Führungskräfte zu erpressen (Stichwort „Revenge Porn“), um so das Unternehmen zu Lösegeldzahlungen zu motivieren.

Die taxative Aufzählung der möglichen Unternehmenswerte (Assets) ist insofern relevant, da wir in Projekten bereits teilweise feststellen müssen, dass diese den Unternehmen mitunter nicht gänzlich bekannt sind oder wegen fehlender technisch-organisatorischer Maßnahmen vernachlässigt wurden. Noch überraschender mag es für Leserinnen und Leser erscheinen, wie viele vertrauliche Details wir zu und aus Unternehmenswerten (Assets) über öffentliche Quellen (Open Source Intelligence) identifizieren können.

In Kombination lassen sich Bedrohungen, Gefährdungen und Schwachstellen sowie die betroffenen Unternehmenswerte (Assets) folgendermaßen darstellen:

[22] vgl. https://www.bloomberg.com/news/articles/2021-03-23/nft-art-jack-dorsey-s-2-9-million-tweet-sets-off-scramble-to-determine-value



Bedrohungen, Schwachstellen und Gefährdungen

„Eine kritische Schwachstelle erzeugt nicht gleich eine Gefährdung. Es müssen ebenso Faktor Mensch und fehlende bzw. fehlerhafte technisch-organisatorische Maßnahmen im Gesamtkontext mit relevanten Assets berücksichtigt werden. Genau diese Sichtweise fehlt oft in der Praxis.“

Lorenz Szabo

Die moderne Verwaltung, Überwachung und der Schutz der IT-Umgebung („*manage, monitor, and protect your environment*“[23]) wird in vielen Fällen durch Threat Intelligence unterstützt, die technisch-organisatorische Maßnahmen (TOMs), IT-Sicherheit (Security Operations Center) und IT-Sensorik (Security Incident Event Management) ergänzen soll. Das Identifizieren von ungeschützten Unternehmenswerten (Assets) und möglichen Angriffsvektoren ist ein wesentlicher Bestandteil davon.

[23] vgl. https://www.securityweek.com/reveal-first-pillar-industrial-cybersecurity

Resilienz in der Lieferkette aufbauen

Folgende Ansätze[24] der letzten Monate und Jahre sind Vorschläge von Expertinnen und Experten, die Unternehmen zum Schutz vor einer Lieferkettenbedrohung anwenden können:

- Aus- und Weiterbildungsmaßnahmen bei der Erkennung von Betrugsversuchen (Phishing war gestern; Deepfakes sind morgen)
- Backups werden oft über Monate hinweg inkrementell erstellt und viele Backup-Strategien berücksichtigen die Notwendigkeit einer raschen Wiederherstellung nicht
- Blockchain, Ledger, Smart Contracts und Token locken mit dem Versprechen, unterschiedlichste Werte (Assets) über ein „Peer-to-Peer"-Netzwerk zu schützen, ohne dafür eine kostenpflichtige Zentralstelle zu benötigen → die Umsetzung und die dafür geeignete Blockchain müssen jedoch ebenfalls auditiert werden
- Datenaustausch zu Risiken und Sicherheitspannen mit und bei anderen Kettengliedern (Third Parties) in der Lieferkette sowie regelmäßige Lieferanten-Audits mit Schwerpunkt Cyber- und Reputationsrisiken
- Kritische Geschäftsdaten und geistiges Eigentum (z.B. CAD-Dateien) aus der öffentlichen Cloud (Managed Service Provider) in die eigene IT-Umgebung zurückholen, wenn diese grenzübergreifend von mehreren (Zu-)Lieferdiensten geteilt werden
- Reduktion der Administratoren-Benutzerrechte auf ein absolutes Minimum; vgl. auch unten die zitierten Beispiele von Gavin Ashton
- Eliminierung von Schatten-IT (z.B. cloudbasierte Projektmanagement-Software, öffentliche Quellcode-Depots) und Reduktion von internetbasierten Geräten (Internet of Things) im Geschäftsalltag
- Reduktion von Anwendungen, Software-Bibliotheken von Dritten und Benutzerkonten sowie einer beruflichen und privaten Segmentierung (z.B. MDM auf Smartphones; Verbot von freizeitorientierten sozialen Netzwerken mit Firmenbenutzerkonto)
- Standardisierte Anwendungen (z.B. Office 365, Google Docs) hingegen in die Cloud (Managed Service Provider) auslagern
- Verhinderung von Datenlecks durch geeignete Schutzmaßnahmen, z.B. Mehrfaktor-Authentifizierung

Logischerweise sind nicht alle Ansätze sofort immer und überall umsetzbar. Beispielsweise empfiehlt die EU-Behörde ENSIA sogenannte „Code-Checks" zur Validierung von Software von Drittanbietern[25], was Medien wie The Register[26] oder Golem[27] als praktisch kaum durchführbar bezeichnen. Hingegen ist es empfehlenswert, sich mit den gelernten Erfahrungen anderer zu beschäftigen, wie zum Beispiel der ehemalige Maersk-IT-Mitarbeiter Gavin Ashton zu Administratoren-Benutzerrechten („controls") schreibt[28]:

„Service accounts should not be used across multiple applications.
End user productivity accounts should not have admin privileges anywhere.
Server admin accounts should not have admin privileges on workstations."

[24] vgl. https://securityintelligence.com/articles/global-supply-chain-security-threats-how-to-handle

[25] vgl. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[26] vgl. https://www.theregister.com/2021/07/31/enisa_supply_chain_attack_report/

[27] vgl. https://www.golem.de/news/supply-chain-angriffe-eu-behoerde-empfiehlt-code-checks-fuer-abhaengigkeiten-2108-158595.html

[28] vgl. https://gvnshtn.com/maersk-me-notpetya

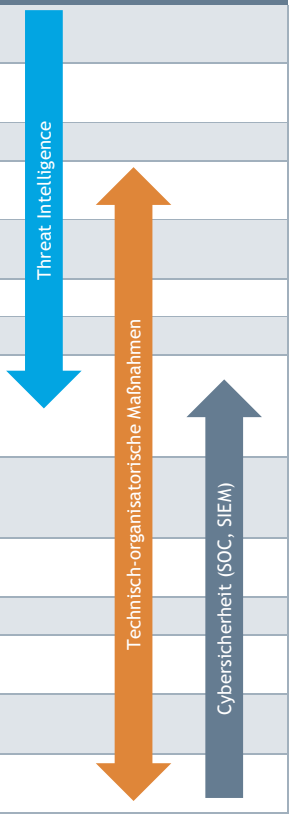
Lieferkette oder Ransomware: Ja schon, aber nein!

Wenn der Schaden bei einem Unternehmen der gleiche ist, nämlich der komplette Stillstand durch Schadsoftware (z.B. NotPetya) oder Ransomware (z.B. Petya), warum unterscheiden Expertinnen und Experten dann akribisch zwischen solchen Angriffsformen? Ein anderes Beispiel: Kritische Schwachstellen in der Accellion File Transfer Appliance (FTA) wurden von staatlichen Angreifern und anschließend der kriminellen Hacker-Gruppierung Clop ausgenutzt – im Grunde genommen eigentlich egal für das Opfer, wer hier angreift?

„*We beg to differ*“ und aus gutem Grund: Nicht-zerstörerische Lieferkettenbedrohungen fallen oft in die Kategorie von Cyberspionage, während zerstörerische Lieferkettenbedrohungen zum Zwecke der Sabotage eher selten sind und als Vorstufe für einen Cyberkrieg eingestuft werden. Beispiele von extrem gefährlicher Sabotage-Schadsoftware sind BlackEnergy, Shamoon, Stuxnet und Olympic Destroyer[29], die aus geopolitischen Gründen (z.B. Aktivismus, Rache, Vergeltung) eingesetzt wurden und einen hohen Schaden an Maschinen und indirekt an Menschen hätten verursachen sollen.

Cyberkriminalität in Form von Bitcoin-Erpressung wird seit Monaten als Ransomware immer relevanter und bedrohlicher. Und genau deswegen wird auch eine Unterscheidung zwischen Ransomware und Lieferkettenbedrohung für Unternehmen immer relevanter:

Ablauf	Bedrohungskette	Ransomware	Lieferkettenbedrohung	Aufklärung und Schutz
1	**Auslöser**	Staatliche Duldung wegen Sanktionen	Staatlicher Auftrag zur Vorteilsverschaffung	
2	**Zielauswahl**	Unternehmen und öffentliche Einrichtungen im Westen	**Millionen von Anwendern weltweit (z.B. Minderheit im Ausland)**	
3	**Zielselektion**	**Tendetiell zufällig**	Sehr gezielt	
4	**Zielobjekte**	Unternehmen und (staatliche) Betreiber von kritischer Infrastruktur	Userinnen und User einer bestimmten Plattform	
5	**Angriffsmotivation**	Primär kriminell; sekundär politisch-motivierter Aktivismus	Primär idologisch und sekundär zur Vorteilsverschaffung	
6	**Angriff**	**Erpressung (Geldbeschaffung)**	Spionage und/oder Sabotage	
7	**Angriffsdauer**	Wenige Stunden	**Mehrere Monate**	
8	**Angriffsmethodik**	Schneller Angriff auf kritische Schwachstellen mit vorhandener Ransomware (RaaS) bzw. Social Engineering	Beständiger (gemächlicher) Angriff über Zero-Days, Manipulation von Infrastruktur (Cloud-Dienste) und eigener Schadsoftware	
9	**Schadensausmaß**	Von Kriminellen kalkuliertes Schutzgeld plus Kosten einer Wiederherstellung und allfälliger Strafen	Existenzielle Bedrohung durch kompletten Stillstand und/oder Reputationsverlust	
10	**Schaden**	Verschlüsselung und Datenabfluß	Trojaner, Stealer (Datenabfluss), Wiper, Cryptominer	
11	**Schadenshöhe (durchschnittlich)**	**100.000 bis 10.000.000**	Millionen bis Milliarden	
12	**Verantwortlichkeiten**	Unternehmensführung	Behörden, Stakeholder, Unternehmensführung	
13	**Behebung im Regelfall**	IT-Fachabteilung	Externe Spezialistinnen und Spezialisten	
14	**Verhinderung im Idealfall**	Warnungen durch Behörden (BSI, CISA, CERTs)	**Verhinderung durch Nachrichtendienste (GCHQ, NSA)**	



Die primären Unterscheidungskriterien zwischen Ransomware und Lieferkettenbedrohung sind farblich hervorgehoben.

[29] vgl. https://arstechnica.com/tech-policy/2020/10/six-russians-accused-of-the-worlds-most-destructive-hacks-indicted und https://www.theregister.com/2012/08/29/saudi_aramco_malware_attack_analysis

Eine eindeutige Zuordnung wird immer schwieriger, wenn beispielsweise Cyberangriffe hintereinander erfolgen und dabei unterschiedliche Motive verfolgt werden. Ebenso sind nicht alle Lieferkettenbedrohungen staatlicher Natur, was jedoch nicht immer im ersten Moment festgestellt werden kann. Beispielsweise waren Cyberangriffe auf europäische Hochleistungscomputer (HPC) im Sommer des Vorjahres im ersten Moment wegen der Forschung zu Covid-19 verdächtig, entpuppten sich nach eingehender Analyse als plumper Versuch in der Nacht unbemerkt nach Kryptowährungen zu schürfen.

Accellion File Transfer Appliance (FTA), Aisino Golden Tax Invoicing Software (Baiwang Edition), Avast CCleaner/NordVPN, Codecov, HashiCorp, Intellect Service MeDoc, PASSWORDSTATE, SolarWinds Orion, u.v.a. sind Beispiele, wie Lieferkettenbedrohung einen enormen Schaden in Kundennetzwerken verursachen konnten. PASSWORDSTATE war vermutlich einer der schwerwiegendsten Angriffe, der jedoch medial unterging: Viele IT-Fachabteilungen von Unternehmen verwalten in diesem Passwort-Manager die gesamten Administrationspasswörter und Zugänge – also die Schlüssel zum Königreich (Keys To The Kingdom).

Im Dezember 2020 schockierte ein Hacker-Angriff auf amerikanische Behörden die weltweite Öffentlichkeit. Angeblich war es russischen Hackern gelungen, in streng vertrauliche amerikanische Netzwerke einzudringen und systematisch „alles“ auszuspionieren. Der Schaden, der zurückblieb, war enorm: Zwei Drittel der amerikanischen Fortune-500-Unternehmen, diverse Cybersicherheitsfirmen, Betreiber kritischer Infrastruktur, fast alle amerikanischen Ministerien und militärische Einrichtungen waren bzw. sind noch bis dato betroffen. In Europa dürften einige große Firmen und EU-Institution ebenfalls betroffen sein. In vielen Fällen wurde die Öffentlichkeit nie darüber informiert, wie mit der Bedrohung umgegangen wurde bzw. ob eine Kompromittierung überhaupt nachgewiesen werden konnte. Acht Monate später wurde im August 2021 publik, dass an die 27 amerikanischen Staatsanwaltschaften[30] bis dato von den Hackern ausspioniert worden waren, darunter auch die New Yorker Staatsanwaltschaft, die regelmäßig Cyber- und Wirtschaftskriminelle aus China und Russland anklagt.

Entdeckt wurde der Cyberangriff auf SolarWinds eher zufällig. Es begann mit einem Datenleck bei der Sicherheitsfirma FireEye. Unbekannte hatten deren geheime „Red Team“-Werkzeuge[31] im Internet veröffentlicht und FireEye musste nach dieser Entdeckung anschließend den Nachrichtendienst der Vereinigten Staaten (NSA) und das Pentagon vor Cyberangriffen zu SolarWinds Orion warnen.

Die Vorgehensweise der Angreifer war schlichtweg genial: Über einen schlecht geschützten Zugang wurde der Update-Server von SolarWinds insofern manipuliert, dass bei jeder neuen Version von Orion vollautomatisch die Schadsoftware der Angreifer dazu gepackt wurde. Diese holte und verteilte dann weitere zusätzliche Schadsoftware, wenn sie vor Ort im Kundennetzwerk angelangt war. Glücklicherweise endete die Genialität des Angriffs bei der Verwendung von „Cobalt Strike Beacons“[32] zur Erkundung im gegnerischen Netzwerk, was bis dato nur kriminellen Hacker-Gruppierungen zugetraut wurde und der Angriff für IT-Expertinnen und -Experten somit leichter identifizierbar wurde. In der Öffentlichkeit verwunderte danach der Erklärungsversuch des ehemaligen SolarWind CEOs vor einem Untersuchungsausschuss: „*A mistake that an intern made…*“[33]

---

[30] vgl. https://apnews.com/article/technology-europe-russia-election-2020-5486323e455277b39cd3283d70a7fd64

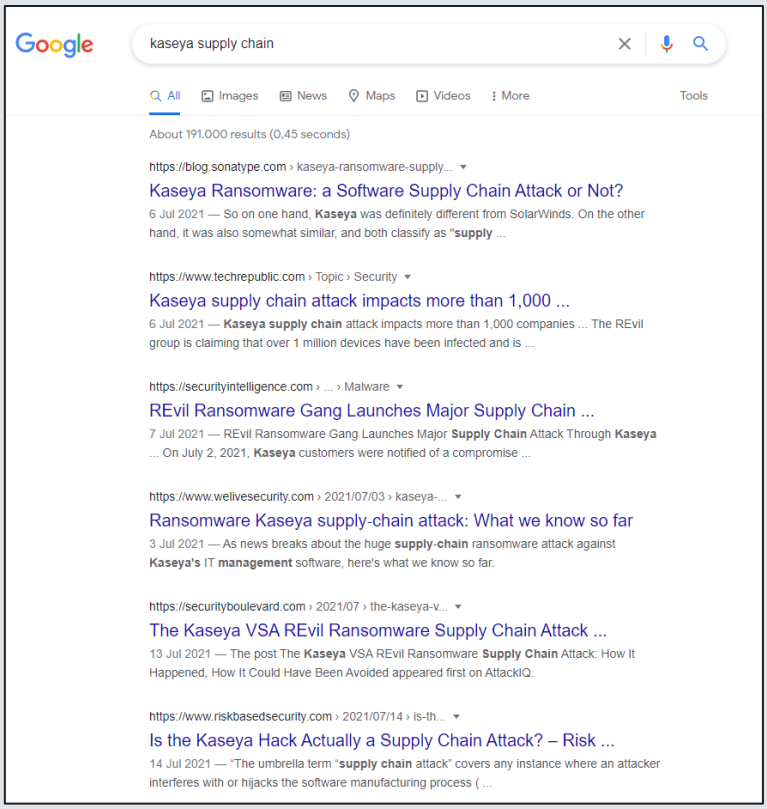
[31] Software zum Testen von Netzwerkzugängen, die entweder legitim (defensiv) aber auch für Angriffe (offensiv) verwendet werden kann.

[32] Cobalt Strike ist ebenfalls eine spezielle Software für „Red Teams“. Dummerweise haben professionelle Anwender größte Probleme, eine legale Lizenz zu erwerben, während Cyberkriminelle einfach Raubkopien einsetzen. Mittlerweile gibt es gute Referenzen in öffentlichen Quellen, wie man Cobalt Strike im eigenen Firmennetzwerk erkennen/blockieren kann oder sogar die Server austricksen könnte (was wir nicht empfehlen).

[33] vgl. https://thehackernews.com/2021/03/solarwinds-blame-intern-for-weak.html und https://medium.com/digital-diplomacy/hey-executives-interns-are-never-the-root-cause-of-your-security-breach-46781f41ea1

Mittlerweile weiß man, dass ebenso die Empfehlung bestimmte Ordner von der Überprüfung durch Anti-Virus-/Endpoint-Detection-Software auszuklammern, diesen Angriff überhaupt erst möglich machte. Es ist jedoch fraglich, diesen Angriff auf ein unsicheres Passwort und eine schlechte Empfehlung zu reduzieren. Im Laufe der letzten Monate wurden unzählige weitere Angriffsvektoren entdeckt, die diverse Sicherheitslücken in Software-Produkten anderer Hersteller, in Verkettung mit dem Angriff auf SolarWinds Orion, ausgenützt haben. In der KW22/2021 lag die Liste der Schadsoftware des mutmaßlichen Angreifers, dem Auslandsgeheimdienst der Russischen Föderation, bei SUNBURST, SUPERNOVA, SUNSPOT, Teardrop und Raindrop. Der Startzeitpunkt dieser Lieferkettenbedrohung bei SolarWinds wird auf September 2019 geschätzt, also bereits vor Beginn der Corona-Pandemie. Erste Server und Cloud-Dienste wurden bereits in den Monaten davor vorbereitet und eingerichtet, wie man mittlerweile weiß.

Vor kurzem erfolgte dann der Ransomware-Angriff auf Kaseyas Virtual System Administrator (VSA), einer Software ähnlich SolarWinds Orion, die von Netzwerkadministratoren eingesetzt wird. Das amerikanische Software-Unternehmen Kaseya wurde gemäß Medienberichten das Opfer eines mutmaßlich hochkomplexen Angriffs durch die Ransomware-Gruppierung REvil. Was im ersten Moment nach einem Angriff auf die Lieferkette von Kaseya aussah, entpuppte sich wenige Tage später als alter Hut: Über einen SQL Injection Angriff konnten die Angreifer die VSA-Software manipulieren, von Kaseya empfohlene Ausnahmeregeln verhinderten die Entdeckung von Computerviren und so konnte über kompromittierte Updates die REvil-Ransomware an weit über tausend Endkunden verbreitet werden. Der Mythos einer Lieferkettenbedrohung war geboren, wurde entkräftet und blieb weiterhin bestehen…



Ein Blick auf Kaseya und Supply Chain

Auch Software-Entwicklungsumgebungen wie Xcode, Brew, GitHub, oder wissenschaftliche Python-Erweiterungen zur Datenanalyse eignen sich für Lieferkettenbedrohungen, da unzählige Entwickler weltweit solche Software-Tools einsetzten. Dabei macht es auch keinen Unterschied mehr, unter welchem Betriebssystem eine solche virtuelle Bedrohung eingeschleust wird. In diesen Fällen sind es meist Kriminelle, die Kreditkartendaten (z.B. Magecart), Bitcoin-Wallets (z.B. Clipboard Hijacker) oder Telebanking-Zugänge stehlen oder Kryptowährung wie Monero auf (virtuellen) Servern der Entwickler erzeugen wollen. Dabei wäre dies einfach zu erkennen gewesen, wenn beispielsweise Erweiterungen für Python falsch geschrieben sind (z.B. diango, djago, dajngo, djanga statt Django[34]) oder Xcode aus Bequemlichkeit illegal und ohne Registrierung über einen Torrent geladen wurde.

Am Ende des Tages reduzieren sich die Empfehlungen zum Schutz vor Lieferkettenbedrohungen auf bewährte Methoden und Best Practices: Eine regelmäßige Aktualisierung von Betriebssystemen und Anwendungen, die Beschaffung von Software und Bibliotheken von seriösen Anbietern, der generelle Einsatz von Multi-/Zwei-Faktor-Verfahren zur Authentifizierung, keine beruflichen Benutzerkonten für private Zwecke (z.B. Netflix oder Facebook), der Austausch zu aktuellen Bedrohungsszenarien und Schwachstellen in Industriegremien sowie mit Behörden (z.B. CERTs) und das allgemeine Bewusstsein für die Notwendigkeit von internen Kontrollsystemen. In vielen Fällen hätten hochkomplexe Cyberangriffe erkannt oder deren Ausbreitung zumindest erschwert werden können. Beispielsweise hatten SolarWinds-Supportmitarbeitende über Monate hinweg Vorgesetzte vor dem unsicheren Passwort (solarwinds123) des Updateservers gewarnt, das bereits seit 2017 im Internet veröffentlicht worden war, nur sah sich niemand für eine Neuvergabe des Passwortes zuständig[35].

[34] vgl. https://www.zdnet.com/article/twelve-malicious-python-libraries-found-and-removed-from-pypi

[35] vgl. https://www.zdnet.com/article/solarwinds-security-fiasco-may-have-started-with-simple-password-blunders/

Die fünf wichtigsten Erkenntnisse zu Lieferkettenbedrohungen mit Stand September 2021

1. Lieferketten in der Informationstechnologie (IT) werden seit 1973 kompromittiert, auch wenn es beim ersten erwähnten Angriff noch eine Machbarkeitsstudie war. Seit 2011 häufen sich Angriffe auf Lieferketten und die Anzahl der Betroffenen wird aufgrund der heutigen Netzwerkeffekte bzw. durch offene Softwarebibliotheken immer größer. Software für die Entwicklung von Anwendersoftware oder beliebte Phyton-Bibliotheken sind Paradebeispiele für eine anschließend wellenartige Ausbreitung im Internet. In Summe sind bis dato die folgenden Lieferkettenbedrohungen[36] bekannt und dokumentiert:
   a. Kompromittierte Software und Bibliotheken von Dritten/Drittanbietern
   b. Physische Eingriffe in der Lieferkette, die über eine dolose Entnahme von Rohstoffen hinausgehen
   c. Weiterverbreitung von Schadsoftware durch ein kompromittiertes „Kettenglied“ bzw. einen Managed Service Provider (MSP)
   d. Weiterverbreitung von dolosen Inhalten über Distributionsnetzwerke (Content Delivery Network)
   e. Verwendung gestohlener Benutzerkonten eines Kettenglieds, um in die Gesamtkette eindringen zu können

2. Lieferkettenbedrohungen sind ein präferiertes Werkzeug für staatliche Spionage und Industriespionage, weil Zugriffe und somit der Datenabfluss auf Monate hinweg unentdeckt bleiben. Ransomware befällt im Vergleich dazu in nur wenigen Stunden, fällt durch plumpe Vorgehensweise auf (z.B. Bildschirmhintergrund) und soll möglichst schnell viel Lösegeld einbringen. Der Schaden durch Lieferkettenbedrohungen ist hingegen nicht sofort erkennbar oder feststellbar.
   Lieferkettenbedrohungen lassen sich vereinfachend zusammenfassen:
   - Extrem hohe Betroffenheit bei Millionen von Anwenderinnen und Anwendern
   - Verdeckte Angriffe über einen Zeitraum von mehreren Monaten
   - Einem generellen Versagen einer Vorabwarnung durch Hersteller, Behörden und sogar durch Nachrichtendienste

3. Medial mögen Cyberangriffe mit Ransomware oder auf Lieferketten ein- und dasselbe sein, in der Realität ist ein deutlicher Unterschied erkennbar. Warum ist dieser Unterschied überhaupt relevant? Die Relevanz entsteht durch eine geostrategische, ökonomische und rechtliche Betrachtungsweise, denn die Form eines Cyberangriffs wirkt sich auf Verantwortlichkeiten, Reputation, Schadenshöhe und die Folgekosten der Schadensbehebung aus. Sicherheitsfirmen sehen „Info Stealer“-Schadsoftware bereits als problematischen nächsten Evolutionsschritt nach Ransomware. Der richtige und proaktive Umgang mit unterschiedlichen Bedrohungsszenarien kann zumindest in einigen Bereichen das Schadensausmaß minimieren. Plakativ vereinfacht: Mancher ehemaliger CEO wäre vielleicht heute noch CEO…

4. Technisch-organisatorische Maßnahmen dürfen nicht als lahme Arbeitsvorschriften, fade Prozessbeschreibung oder verstaubte Handbücher abgetan werden. Wir alle sind als Mitarbeiterinnen und Mitarbeiter kollektiv die Maßnahme: „*Jeder Mitarbeiter [Banker] muss im Herzen ein Risikomanager sein*“, um das Lieblingszitat vom Credit Suisse Bankpräsidenten António Horta-Osório[37] abzuwandeln. Eine Quizfrage: Wie schnell finden Sie an Ihrem Arbeitsplatz einen Notfallplan in

[36] vgl. https://www.riskbasedsecurity.com/2021/07/14/is-the-kaseya-hack-actually-a-supply-chain-attack

[37] vgl. https://www.finews.ch/news/banken/47519-credit-suisse-archegos-patrice-lescaudron-ellina-volkova-risiko-unternehmertum

Papierform, der nicht älter als sechs Monate ist? Diese Quizfrage hat schon manche Opfer von Cyberangriffen mehrere Millionen an Stillstand gekostet, mutmaßlich erst vor kurzem eine internationale Beratungsfirma, weil deren Mitarbeiterinnen und Mitarbeiter den Befall durch Ransomware nicht zeitgerecht an die ausgelagerte IT melden konnten. Fehlende Notfallpläne für den Verdacht auf Ransomware, Sabotage & Spionage, nicht mehr aktuelle Information zu Zuständigkeiten und defekte Backups sind vermutlich die drei häufigsten Probleme bei der raschen Wiederherstellung eines Geschäftsbetriebs. Fehler machen kann und darf jeder, daraus erst die Resilienz zu lernen, sollte aber nicht nur Praktikantinnen und Praktikanten…

5. Unternehmen müssen ihre Unternehmenswerte (Assets) kennen, katalogisieren und auf sie achten wie auf einen Augapfel. Die Vernachlässigung einzelner Assets aus monetären Gründen (z.B. Budgetknappheit), Unwissenheit oder wegen Befindlichkeiten durch konkurrierende Interessen innerhalb einer Organisation (Stichwort: Silodenken) führen unwiderruflich zu einer Gesamtgefährdung. Etablierte Methoden und Werkzeuge sind vorhanden.

KONTAKTDATEN

Ewald Kager
Partner

+43 5 70 375 - 4211
+43 664 60 375 - 4211
ewald.kager@bdo.at

Lorenz Szabo
Manager

+43 5 70 375 - 1836
+43 664 60 375 - 1836
lorenz.szabo@bdo.at