Die Lieferketten sicherer machen!

Von Holger Köster

Holger Köster

Geschäftsführer der HERSA-Unternehmensgruppe und Vorsitzender des Fachausschusses Wirtschaftsschutz im BDSW

„Nach den Explosionen diverser Geräte im Libanon stellt sich die Frage nach dem Vorgehen", schreibt das Schweizer Nachrichtenportal „20min.ch". Denn dies sei „ein Angriff auf die weit verstreuten Lieferketten – ein Sicherheitsrisiko, entstanden mit der Globalisierung". Auch für uns ein Grund, noch einmal nachdrücklich darauf hinzuweisen, wie wichtig es ist, die Lieferkette (oder besser gesagt: die Lieferketten) genauestens im Auge zu behalten.

Das Lieferkettengesetz umfasst strenge Regularien der unternehmerischen Verantwortung für die Einhaltung von Menschenrechten in den globalen Lieferketten. Die Vermutung des Berliner „Tagesspiegel" nach den Anschlägen in Nahost, dass diese „nun auch zur Nachahmung führen" könnten, sollte als Warnung verstanden werden.

Die Abhängigkeit von einer einzigen „Supply Chain" erhöht das Risiko erheblich, von einer existenzgefährdenden Unterbrechung der Lieferkette betroffen zu werden. Ausgelöst können diese durch regionale Ereignisse und Konflikte, wie zum Beispiel die Auseinandersetzungen am Suezkanal, die den Transport durch diese wichtige Wasserstraße seit geraumer Zeit erheblich beeinträchtigen.

Auch die Nachverfolgung des Ursprungs von Produkten und Materialien, um sicherzustellen, dass sie aus vertrauenswürdigen Quellen stammen, ist unverzichtbar. Dabei können Technologien wie Blockchain wertvolle Hilfe leisten.

Eine regelmäßige Risikobewertung kann helfen, potenzielle Schwachstellen in der Lieferkette rechtzeitig zu identifizieren. Den Unternehmen ist angeraten, Strategien zu entwickeln, welche diese Risiken minimieren. Dies kann durch die Zusammenarbeit mit Versicherungen, durch Notfallpläne oder alternative Beschaffungsstrategien erfolgen.

Eine enge Zusammenarbeit und regelmäßige Kommunikation mit den Lieferanten erhöhen die Chancen erheblich, Probleme frühzeitig zu erkennen und gemeinsam Lösungen erarbeiten zu können. Langfristige, vertrauensvolle Partnerschaften sind eine wichtige Voraussetzung für Stabilität. Diese Technologien sind eine wertvolle Unterstützung für eine bessere Überwachung und Analysen von Daten in Echtzeit.

Um die vorgenannten Maßnahmen zur Wirkung zu bringen, sollten Mitarbeiter regelmäßig geschult werden, damit sie die Bedeutung der Sicherheit in der Lieferkette verstehen und potenzielle Risiken erkennen können.

Und last, not least kann die Einhaltung internationaler Standards und Vorschriften ganz wesentlich dazu beitragen, die Qualität und Sicherheit der Produkte in der Lieferkette krisensicher zu gewährleisten.

Ihr
Holger Köster

Bild: # 1652511983 / istockphoto.com

„… Lieferketten ins Fadenkreuz!“

Von Peter Niggl

Wirtschaftsunternehmen und Sicherheitsbehörden sollten ganzheitlich agieren, dabei müsste „auch die Sicherheit von Lieferketten mit bedacht werden“. So ist es in der Bitkom-Studie „Wirtschaftsschutz 2024“ zu lesen, die im August dieses Jahres vorgestellt wurde. Cyberakteure, so heißt es dort, hätten „die gesamte Supply Chain im Blick, während Unternehmen diese häufig vernachlässigen“. Was wenige Wochen später jedoch die globale Lieferkette betreffend geschah, hatte zu diesem Zeitpunkt wohl kaum einer der Sicherheitsexperten auf dem Schirm. Am 17. September gegen 15:30 Uhr (Ortszeit) detonierten in einer ersten Welle Tausende Pager im gesamten Libanon, aber auch in Syrien. Der Angriff galt, darüber ist man sich einig, in erster Linie Milizionären der schiitischen Hisbollah, da der Angriff vor allem im Beiruter Vorort Dahiya, der als Hisbollah-Hochburg gilt, besonders heftige Wirkung entfaltete. Einen Tag später explodierten ebenfalls im Libanon zahlreiche Walkie-Talkies, welche derselben Personengruppe zugerechnet werden.

Wenige Tage nach dem Angriff, am 20. September, titelte die – von der US-Regierung finanzierte und in Washington erscheinende – arabischsprachige Zeitschrift „Alhurra“ einen Artikel: „Pager-Bombenanschläge bringen Lieferketten ins Fadenkreuz!“ Das Blatt meinte, „dass die Pager abgefangen und mit Sprengstoff bestückt wurden, nachdem sie die Fabriken verlassen hatten“.

Berichte in der „New York Times“ und der „Washington Post“ lassen auf folgende Abfolge der Ereignisse schließen. Seit Jahren hätten Geheimdienste in den Pagern eine mögliche Möglichkeit gesehen, in die Kommunikationssysteme der Hisbollah einzudringen. Bereits im Jahr 2020 hatte der – inzwischen getötete – Anführer der Hisbollah, Hassan Nasrallah, die Mitglieder der Gruppe vor der Nutzung von Mobiltelefonen gewarnt, weil er die Gefahr vermutete, man würde ihre Mobiltelefongespräche überwachen und ihre Bewegungen verfolgen. Im Februar 2024 wies Nasrallah die Mitglieder der Gruppe an, Pager anstelle von Handys zu verwenden, da er davon ausging, ihr Handynetzwerk sei infiltriert worden.

Zunächst war nur klar, dass die präparierten Kommunikationsgeräte aus Taiwan stammen sollten. Die Piepser waren, wie das „China Times Network Taiwan“ schrieb, ein Produkt der Golden Apollo Company im Distrikt Xizhi.

Am 5. Oktober dann präsentierte die „Washington Post“ in einer kurzen Meldung eine Variante, die den Ablauf der Vorbereitungen für den Anschlag beschrieb: „Im ersten Verkaufsgespräch an die Hisbollah vor zwei Jahren schien die neue Linie von Apollo-Pagern genau den Bedürfnissen einer Milizgruppe mit einem ausgedehnten Netzwerk von Kämpfern … gerecht zu sein. Der AR 924-Pager war leicht sperrig, aber robust gebaut, um die Bedingungen auf dem Schlachtfeld zu überleben. Es verfügte über ein wasserdichtes taiwanesisches Design und eine übergroße Batterie, die monatelang ohne Laden arbeiten konnte. … Die Führer der Hisbollah waren so beeindruckt, dass sie 5.000 von ihnen kauften und begannen, sie im Februar an Kämpfer der mittleren Ebene und Unterstützungspersonal zu verteilen.“

Wie jedoch genau die Geräte aus Taiwan in den Nahen Osten gekommen sind und an welcher Stelle sie präpariert wurden, ist schwer zu durchschauen. Und das ist sicher kein Zufall. Bei Gold Apollo reagierte man umgehend. Hsu Ching-Kuang, CEO des Unternehmens, sagte auf einer eiligst einberufenen Pressekonferenz, dass die explodierten Pager von seinem ungarischen Partner hergestellt worden seien. In Budapest gab man jedoch bekannt, dass eine Firma BAC Consulting, die angeblich die Kommunikationsgeräte hergestellt haben soll, lediglich ein „kommerzieller Vermittler ohne Produktionsstandort in Ungarn“ sei. Die „New York Times“ vermerkte dazu jedoch, dass das Unternehmen in Budapest „tatsächlich Teil einer Front war“, wie drei über den Einsatz informierte Geheimdienstmitarbeiter berichtet hätten. Die Beamten hätten erklärt, dass zwei weitere Scheinfirmen gegründet worden seien, „um die wahre Identität der Leute zu verbergen, die die Pager herstellen“. Eines der „hohlen“ Unternehmen sei die ungarische BAC Consulting, hieß es in der Zeitung; die beiden anderen nannten sie jedoch nicht.

Peter Niggl

Freier Journalist. Er beschäftigt sich seit Jahren mit Fragen der privaten Sicherheit.

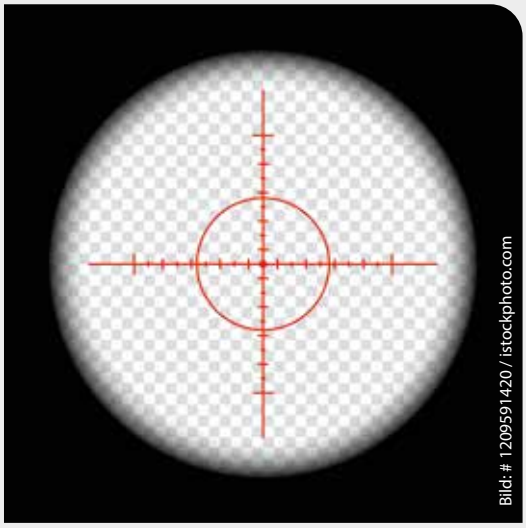

Bild: # 1209591420 / istockphoto.com

Bild: # 217278470 / istockphoto.com

Der ungarische Nachrichtendienst „Telex“ berichtete bereits am 18. September, „dass die Geschäftsführerin von BAC Consulting, Cristiana Bársony-Arcidiacono, mit einem bulgarischen Unternehmen, Norta Global Ltd. mit Sitz in Sofia, verhandelte. Obwohl es auf dem Papier BAC Consulting war, die den Vertrag mit Gold Apollo unterzeichnete, steckt hinter dem Deal tatsächlich Norta Global Ltd.“

„Norta Global“, das bulgarische Unternehmen, das als Teilnehmer an den Lieferungen beschrieben wird, existiert zwar, habe ebenfalls keine Mitarbeiter; und an der Adresse in Sofia gebe es lediglich eine „Agentur für neue Unternehmen“, so ein Reporter von „Svobodna Europa“.

Eine Überprüfung im Handelsregister ergab, dass der Eigentümer von „Norta Global“ ein Rinson Jose ist. Das bulgarische Unternehmen „Norta Global“ ist seit 2022 am Boulevard „Vitosha“ in der Hauptstadt Sofia registriert. Die bulgarische „Norta Global“ sei Teil der Lieferkette der im Libanon und in Syrien explodierten Pager. Dies stellte das ungarische Nachrichtenportal „Telex“ unter Berufung auf eine ungenannte Quelle fest.

In Sofia wiegelte man ab. „Auf dem Territorium Bulgariens wurden keine Zolloperationen (mit Pagern) durchgeführt“, ließ der bulgarische Spionageabwehrdienst DANS verlauten. RFE hat daraufhin Fragen an das Unternehmen geschickt, aber keine Antwort erhalten.

Nun konzentrierten sich die Recherchen auf die Spur „Norta Global“ und den ominösen Geschäftsmann namens Rinson Jose, der wohl schillerndsten Figur in diesem Gewirr einer undurchsichtigen Lieferkette.

Laut einem Bericht der „Times of India“ wurde Rinson Jose in der Kleinstadt Ondayangadi, Bezirk Wayanad, im indischen Bundesstaat Kerala in einfachen Verhältnissen geboren. Wie der TV-Kanal NDTV („New Delhi Television“) berichtet, sei Jose vor einigen Jahren nach Norwegen gezogen, um dort ein Studium zu absolvieren. Über das Alter von Rinson Jose gibt es unterschiedliche Angaben, die zwischen 37 und 39 Jahren schwanken.

Im April 2022 hat er die Firma Norta Global Ltd. mit Sitz im bulgarischen Sofia gegründet, welche im vergangenen Jahr Einnahmen in Höhe von 725.000 US-Dollar für Beratungstätigkeiten außerhalb der Europäischen Union auswies.

Versuche von Medienvertretern, mit Rinson Jose nach den Vorfällen im Libanon und Syrien Kontakt aufzunehmen, schlugen fehl, da er, wie


Bild: # 1915205991 / istockphoto.com

das Magazin „Newsweek“ schreibt, bei einer Geschäftsreise nach Boston (USA) verschwunden sei und es seit dem 18. September kein Lebenszeichen mehr von ihm gebe. Unni Grøndal, Pressechefin des Polizeibezirks Oslo, sagte gegenüber „Newsweek“: „Der Bezirk der Polizei von Oslo hat eine Vermisstenmeldung erhalten. Es wird bearbeitet, um möglicherweise Maßnahmen zu treffen.“ Die norwegische Polizei hat inzwischen einen internationalen Haftbefehl gegen Jose erlassen.

Holger Köster, Vorsitzender des BDSW-Fachausschusses Wirtschaftsschutz, sieht sich durch den Anschlag in seiner Ansicht bestärkt, den Vorgaben des Lieferkettengesetzes sorgsamer Rechnung zu tragen. Der Einsatz von Technologien wie Blockchain, so Köster, könne helfen, die Transparenz in der Lieferkette zu erhöhen. Dadurch könnten Unternehmen den Ursprung von Produkten und Materialien besser nachverfolgen und sicherstellen, dass sie von vertrauenswürdigen Quellen stammen. (Siehe auch den Beitrag: „Die Lieferkette sicherer machen!“ auf Seite 48)

Die Reaktionen auf diesen Angriff gingen weit auseinander. Der ehemalige Präsident des Bundesnachrichtendienstes (BND), Gerhard Schindler, hat den Angriff als „herausragend“ gewürdigt. Gegenüber dem Redaktionsnetzwerk Deutschland vertrat er die Auffassung, dass sich trotz der noch offenen Frage nach der Urheberschaft sagen lasse, „dass dies eine äußerst professionelle und herausragende geheimdienstliche Operation war“.

Deutlich anders hingegen ist die Position des früheren CIA-Direktors Leon Panetta. Gegenüber dem Sender CBS meinte er: „Ich glaube nicht, dass es irgendeinen Zweifel daran gibt, dass es sich um eine Form des Terrorismus handelt.“

Der Berliner „Tagesspiegel“ resümierte am 26. September angesichts der Vorgänge im Nahen Osten: „Die Attacke auf Pager und Walkie-Talkies im Libanon zeigt …, wie effektiv Angriffe auf Software- und Hardwarelieferketten sein können. … Das könnte nun auch zur Nachahmung führen, fürchten Analysten.“

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

Bitkom-Studie: Wirtschaftsschutz 2024

Die Zahl digitaler Angriffe auf deutsche Unternehmen steigt 2024 weiter an. 74 Prozent der Firmen sind von Datendiebstahl betroffen. Der Gesamtschaden durch Cybercrime beträgt 178,6 Mrd. Euro. Ransomware und Phishing stellen die häufigsten Angriffsformen dar. Auch analoge Angriffe wie Diebstahl physischer Dokumente und das Abhören von Gesprächen nehmen zu.
www.bitkom.org

BKA-Bundeslagebild Korruption 2023

Die Zahl der Korruptionsstraftaten ist 2023 um 6,7 Prozent auf 3.841 angestiegen. Die aktuellen Fallzahlen bleiben jedoch unter dem Durchschnittswert der letzten fünf Jahre. Die Anzahl der im Zusammenhang mit Korruption festgestellten Begleitdelikte sank hingegen deutlich um 30,9 Prozent auf 815.
www.bka.de

BKA-Bundeslagebild Organisierte Kriminalität 2023

Der wirtschaftliche Schaden aus Organisierter Kriminalität in Deutschland hat sich 2023 mehr als verdoppelt. Die Schäden erreichten mit 2,7 Mrd. Euro einen neuen Höchstwert. Besonders im Bereich Cyberkriminalität sind die Schäden stark gestiegen und machten 1,7 Mrd. Euro aus.
www.bka.de

BSI: NIS-2-Betroffenheitsprüfung

Die NIS-2-Betroffenheitsprüfung gibt eine automatisierte Ersteinschätzung, ob ein Unternehmen vom NIS-2-Umsetzungsgesetz betroffen ist. Sie erläutert, was dieser Status bedeutet und welche Pflichten durch den Gesetzgeber vorgezeichnet sind. Sie dient lediglich als Orientierungshilfe und ist im Ergebnis rechtlich nicht bindend.
www.bsi.bund.de

RA Dr. Berthold Stoppelkamp

zuständiges Geschäftsführungsmitglied für den Fachausschuss Wirtschaftsschutz im BDSW