Luther.

Newsflash | Mai 2023

Cyberattacken in der Lieferkette

I. Hintergrund

Hellmann, Meyer&Meyer, Maersk, Swissport, Hapag-Lloyd, TST, aber auch Ferag, die ÖBB und die Lürssen-Werft – es sind einige prominente Namen, die in den letzten Monaten im Zusammenhang mit Cyberattacken öffentlich bekannt geworden sind. Cyberattacken zielen ganz besonders gern auf kritische Infrastrukturen wie Logistik.

Es gehört ersichtlich zur Strategie von Angreifern, Unternehmen aus der Supply-Chain zu attackieren[1]. Der Durchschlagseffekt betriff dann die gesamte Wertschöpfungskette[2].

Laut dem Rat der Europäischen Union erfolgten im Jahr 2021 17 % aller Zwischenfälle unberechtigter Cybereinbrüche im Zusammenhang mit Lieferketten; zum Vergleich: Im Jahr 2020 lag der Anteil nur bei 1 %[3]. Laut Risk Barometer des Versicherungskonzerns Allianz stehen Cyberangriffe in Deutschland auf Platz 2, weltweit sogar auf Platz 1 der Top 10 Geschäftsrisiken für Unternehmen[4].

Die Bedrohungen reichen dabei vom Ausspionieren von Daten, über Manipulation von Systemen – wie Distributed Denial of Service-Bedrohungen (bei denen Nutzer am Zugang zu Informationen und Systemen gehindert werden) – bis hin zum Einsatz von Data-Wiper Malware (bei der Daten von infizierten System gelöscht werden) und Ransomware-Angriffen, über die Kriminelle Lösegeld für ein gekapertes System fordern.

Was alle gemeinsam haben: Einerseits führt eine Cyberattacke zur erheblichen Störung des Geschäftsbetriebs und geht

1 Allianz Risk Barometer 2022, Allianz Risk Barometer 2022, Abruf vom 28. April 2023.
2 Rat der Europäischen Union, Infografik – Häufigste Cyberbedrohungen in der EU, Häufigste Cyberbedrohungen in der EU - Consilium (europa.eu), Abruf vom 28. April 2023.
3 Vgl., wie vor.
4 Allianz Risk Barometer 2022, Allianz Risk Barometer 2022, Abruf vom 28. April 2023.

regelmäßig mit dem Verlust von geschäftskritischen Daten sowie Geschäftsgeheimnissen einher. Andererseits setzen solche Attacken betroffene Unternehmen auch erheblichen vertraglichen sowie datenschutz- und informationssicherheitsrechtlichen Haftungsrisiken aus.

Klar ist: Cyberattacken sind längst zum allgemeinen Risiko geworden und einen absoluten Schutz gibt es nicht.

Wenn der Ernstfall dann eintritt, geht es drunter und drüber und das sofortige Umschalten in den Krisenmodus fällt vielen Unternehmen offenbar schwer. Zu allem Überfluss wimmelt es dann noch von rechtlichen Fallstricken. Es ist deshalb unerlässlich, sich proaktiv klar zu machen, was auch aus rechtlicher Sicht zu tun ist, um im Ernstfall strukturiert vorzugehen.

II. Abwehrstrategie und -maßnahmen

Status identifizieren

Es klingt banal: Der erste Schritt ist, herauszufinden, was überhaupt geschehen ist. Welche Systeme sind betroffen? Ist Schadsoftware installiert? Sind Daten blockiert ? Was für Daten sind eigentlich betroffen – personenbezogene Daten? Geschäftsdaten? Davon hängen nicht nur die technischen Maßnahmen ab, sondern auch die rechtlichen Folgen.

Dokumentieren

All diese Prüfungen müssen dokumentiert werden, um eine spätere Analyse des Vorfalls zu erleichtern – einschließlich der Fertigung von Back-ups von betroffenen Systemen. Eine Dokumentation ist dabei nicht nur aus technischer Sicht wichtig. Sie ist besonders relevant für den Nachweis gegenüber Strafverfolgungsbehörden, der Datenschutzaufsicht, Versicherern und zur Abwehr oder Geltendmachung eventueller Ansprüche von und gegen Vertragspartner wie Kunden oder Lieferanten/Subunternehmern. So kämen zum Beispiel mögliche Ansprüche von und gegen Kunden oder Dienstleister und Lieferanten insbesondere in Betracht, wenn entweder der Logistiker selbst oder sein Geschäftspartner ein Einfallstor für den Angriff offen ließ.

Meldepflichten beachten

Es bestehen umfangreiche Meldepflichten. Häufig wird übersehen, dass nicht nur die DSGVO Meldepflichten vorgibt, sondern dass auch Sondergesetze, etwa im Bereich der Kritischen Infrastruktur Meldepflichten enthalten. Daneben bestehen häufig umfangreiche Pflichten aus Verträgen.

Attacke beseitigen

Unternehmen müssen ihre IT-Sicherheitsexperten so schnell wie möglich einschalten und ihren – idealerweise vorhandenen – betrieblichen Notfallplan (sog. Incident Response Plan) aktivieren.

Spätestens nach der ersten Bestandsaufnahme müssen die zuständigen Personen im Unternehmen informiert werden. Wichtig ist, Systemnutzern mitzuteilen, dass die betroffenen Systeme nicht mehr genutzt werden sollen. Genauso wichtig ist, dass betroffene Systeme zwar vom Internet getrennt werden, um weiteren Schaden zu verhindern. Jedoch müssen die Systeme trotzdem eingeschaltet bleiben, um eventuellen Datenverlust zu vermeiden und eine spätere Aufklärung – einschließlich Dokumentation des Vorfalls – zu ermöglichen.

Sofern Kunden und Geschäftspartner vom Angriff betroffen sein sollten, muss selbstverständlich so schnell wie praktikabel der Kontakt zu diesen gesucht und zwecks gemeinsamen Vorgehens aufrecht erhalten werden. Achtung Falle: Spätestens hier muss vorher geprüft werden, welche konkreten Pflichten aus Verträgen bestehen. Sehr häufig enthalten Verträge Sonderregelungen, wann und wie zu informieren ist oder auch dazu, welche Anforderungen an die IT-Sicherheit gestellt werden (etwa ISO 27001). Die Erfahrung zeigt, dass dies im Vertragsmanagement häufig untergeht.

Besteht eine Cyberversicherung, muss der Vorfall schnellstmöglich dem Versicherer gemeldet werden, ansonsten droht ein Verlust der Versicherungsdeckung.

III. Vorbereitung ist der Schlüssel zum Erfolg

So offensichtlich das Vorgehen im Krisenfall ist, so sehr wird die Vorbereitung im Alltagsgeschäft vernachlässigt. Kann und muss man sich also schon vorab gegen Attacken rüsten?

Die Antwort lautet: ja! Ein präventiver betrieblicher Notfallplans ergibt Sinn. Unternehmen dürfen nicht erst warten, bis der Ernstfall eintritt. Wenn es ernst wird, sind alle Kapazitäten plötzlich gebunden. Ein solides vorbeugendes Maßnahmenkonzept ist wesentlich zur Minimierung eines durch die Attacke verursachten Schadens. Eigentlich unnötig zu sagen,

dass sichergestellt sein muss, dass der Zugriff auf dieses Maßnahmenkonzept auch im Fall eines Cyberangriffs sichergestellt sein muss – auf einem verschlüsselten Server nützt das beste Notfallkonzept nichts. Daher sollten Unternehmen jetzt schon Folgendes sicherstellen:

- Das Unternehmen sollte seine Kommunikation mit Behörden (z. B. Polizei und Datenschutzbehörden), Kunden und Geschäftspartnern vorbereiten. Unternehmen sollen jetzt schon wissen, wen genau sie im Ernstfall kontaktieren müssen. Wer das nicht vorbereitet, muss das dann prüfen, wenn der Fall bereits eingetreten ist und es dringendere Prioritäten gibt. Dies kann auch insbesondere aus juristischer Sicht entscheidend sein, um im Ernstfall den Schaden zu minimieren und gesetzlich vorgeschriebene Fristen einzuhalten.
- Sind vom Angriff personenbezogene Daten betroffen, ist schnelles Handeln gefragt. Gegebenenfalls sind

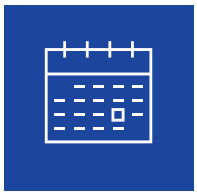
  - die Datenschutzaufsicht sowie
  - betroffene Personen (bei Daten, die als Verantwortlicher verarbeitet werden) und auch
  - Auftraggeber (für Daten, die als Auftragsverarbeiter verarbeitet werden, etwa in der e-commerce-Logistik)

- zu informieren. In der Regel hat dies unverzüglich, spätestens aber innerhalb der gesetzlich vorgeschriebenen Maximalfrist von 72 Stunden nach dem Angriff zu geschehen. Ein verbreiteter Irrtum: Man hat nicht etwa stets 72 Stunden Zeit, sondern muss sofort reagieren. Das geht nur, wenn bereits ohne Anlass Maßnahmen und Notfallkontakte vorbereitet sind und bereitgehalten werden. .
- Zudem sollten im Ernstfall Strafverfolgungsbehörden informiert werden, um die Aufnahme von Ermittlungen zu ermöglichen und von deren ersten Erkenntnissen zu profitieren. Bei kritischen Infrastrukturen muss darüber hinaus eine Meldung an das Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft werden. Ein Notfallkonzept muss also bereits die richtigen Ansprechpartner und Kontakte enthalten.
- Ein vorbereitendes Notfallkonzept enthält auch bereits das Ergebnis einer rechtlichen Bewertung von Verträgen mit Lieferanten und Kunden. In welchen Verträgen bestehen die größten Risiken? Wen muss man wie haftbar halten? Wer erst im Ernstfall in die Verträge schaut, ist zu spät. Solange noch kein Fall vorliegt, kann man Verträge noch anpassen, danach ist es zu spät.
- Eine Versicherung kann nicht nachträglich eingedeckt werden. Unternehmen sollten zudem nicht erst nach dem Ernstfall überlegen, ob es für sie Sinn ergibt, eine Cyberversicherung zu unterhalten. Der Abschluss einer Versicherung sollte vor dem Eintritt des Ernstfalls erwogen werden. Der Markt für solche Versicherungen und deren Anforderungen an die Deckung werden immer herausfordernder und wer bereits einen Schadenfall hatte, erhält häufig keine neue Versicherung mehr.
- Kaum ein Unternehmen wird die Herausforderungen aus einem Cyberangriff mit eigenen Bordmitteln bewältigen können. Externe Hilfe, insbesondere bei der Analyse, Eingrenzung, Abwehr und Wiederherstellung sind unerlässlich. Zur guten Vorbereitung gehört auch, mit qualifizierten Firmen entsprechende Verträge inklusive Notfallbereitschaft zu schließen, die dann auch vorab mit der IT-Infrastruktur vertraut sind.

Ihr Kontakt:

Dr. Maximilian Dorndorf
Rechtsanwalt, Partner
Essen
T +49 201 9220 24027
maximilian.dorndorf@luther-lawfirm.com

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Maximilian Dorndorf
Luther Rechtsanwaltsgesellschaft mbH
Gildehofstraße 1, 45127 Essen, Telefon +49 201 9220 0
maximilian.dorndorf@luther-lawfirm.com

Bildnachweis: Seite 1: Denis Putilov / Adobe Stock, Seite 3: Jörg Modrow

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Stand: Mai 2023