

Schutz vor dem (digitalen) Stillstand

Die Logistik ist vernetzt und wird zunehmend digitaler. Was auf der einen Seite in einer modernen Welt zur Grundvoraussetzung für logistische Prozesse zählt, erhöht auf der anderen Seite die digitale Angriffsfläche — und den Bedarf an Schutzsystemen. Sollte ein Logistikunternehmen dennoch Opfer von Cyberkriminellen werden, kann es gerade aufgrund der direkten digitalen Anbindung an Partner und Kunden zum Worst Case kommen: dem absoluten Stillstand. Nicht nur in der digitalen, sondern auch in der echten Welt.

Eine solche Unterbrechung der Lieferkette wirkt sich auf viele weitere Unternehmen aus, der Schaden kaskadiert. Neben den wirtschaftlichen Konsequenzen spürt dann auch die Gesellschaft schnell die Folgen eines Cyberangriffs, etwa wenn es zu Produktions- oder Lieferengpässen kommt. Bei der Auswahl ihrer Logistikpartner achten Unternehmen dementsprechend verstärkt auf Cybersicherheit. Nicht nur, um entsprechende Compliance-Anforderungen zu erfüllen, sondern auch, um eine sichere Lieferkette zu gewährleisten. Für digital resilient aufgestellte Unternehmen entstehen so Wettbewerbsvorteile.

Cybersicherheit vs. Cyberresilienz

Seit Jahren versuchen Unternehmen, sich mit immer neuen technischen und organisatorischen Maßnahmen gegen digitale Angreifer zu verteidigen. Mittlerweile ist aber klar, dass die Kreativität der Cyberkriminellen nicht zu unterschätzen ist — und diese häufig einen Weg an den Schutzmaßnahmen vorbei finden. Ehrlich gesagt: Sie können im übertragenen Sinne Ihre Mauer immer höher bauen, Stacheldraht und Bärenfallen verwenden. Wenn der Angreifer aber einen Mitarbeiter Ihrer Festung davon überzeugen kann, ihm Zugriff zur Alarm- und Toranlage zu gewähren, sind diese Maßnahmen hinfällig.

Daher ist in den letzten Jahren die sogenannte Cyberresilienz zum eigentlichen Ziel geworden. Im ersten Schritt setzt diese voraus, zu akzeptieren, dass kein Sicherheitskonzept hundertprozentigen Schutz bietet. Stattdessen beschäftigt sie sich aktiv damit, erfolgreiche Angriffe frühzeitig zu erkennen, die Auswirkungen dieser zu begrenzen und sich schnell zu erholen.

Angriffe lassen sich bspw. anhand von ungewöhnlichem Nutzerverhalten erkennen und dann durch automatisierte Gegenmaßnahmen adressieren. Ist ein Verhalten ungewöhnlich, aber noch nicht eindeutig schädlich, können die Nutzer z.B. aufgefordert werden, erneut eine Multi-Faktor-Authentifizierung durchzuführen. Sollte das Verhalten eindeutig bösartig sein, etwa

wenn eine Kopie aller im Unternehmen geteilten Ordner angelegt wird, kann ein Zugriff (temporär) blockiert werden.

Cyber-Antifragilität

Die nächste Ausbaustufe nach der Cyberresilienz wird häufig als Antifragilität bezeichnet. Hier sollen Schäden nicht nur begrenzt und die vorherige Betriebsfähigkeit wiederhergestellt werden. Stattdessen sollen die Systeme zusätzlich aus Angriffen lernen und sich kontinuierlich verbessern, um zukünftig auch gegen abgewandelte Angriffswege standzuhalten.

Durch Regulierungen wie die NIS2-Richtlinie wird ein gewisses Maß an Cyberresilienz für viele Unternehmen verpflichtend. Cybersicherheit ist längst nicht mehr ein Problem, mit dem sich nur die IT-Abteilung auseinandersetzen muss. Sie ist zu einer zentralen Führungsaufgabe geworden und kann bei Nichteinhaltung hohe Strafen für die Geschäftsführung nach sich ziehen.

Wie kommen Angreifer in Ihre Systeme?

In den Medien wird häufig über die Auswirkungen von Cyberangriffen berichtet. Nach einem Datenleak ließ ein Unternehmen z.B. die Lösegeldforderung verstreichen und die gestohlenen Daten wurden im Darknet veröffentlicht. Im schlimmsten Fall muss das betroffene Unternehmen daraufhin Insolvenz anmelden.

Steckt hinter solchen Angriffen ein geheimes digitales Supertalent, gegen das Sie keine Chance haben? Immer häufiger sehen wir: Nein. Teilweise sind die Angreifer, die sich hinter bedrohlich klingenden Online-Pseudonymen verbergen, noch Teenager.

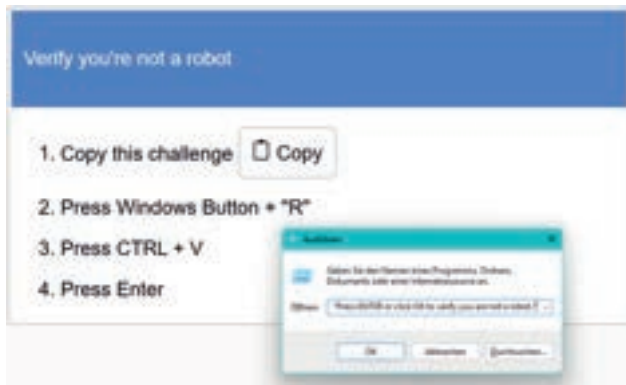
Sie agieren oft arbeitsteilig. So gibt es Personen, die Zugangsdaten von Mitarbeitern oder externen Dienstleistern stehlen und diese dann im Darknet anbieten. Cyberkriminelle können diese Zugangsdaten dann kaufen, sich als Mitarbeiter einloggen und so ungestört an allen Sicherheitsmaßnahmen vorbeilaufen. Wieder andere sorgen dafür, dass der bösartige Login-Versuch auch möglichst unbemerkt bleibt und bspw. nicht mit einer auffälligen IP-Adresse aus einem weit entfernten Land stattfindet.

Einblick in Darknet-Leak

Zugangsdaten werden heute längst nicht mehr nur durch klassische Phishing-E-mails gestohlen, denn die Cyberkriminellen haben in den letzten Jahren einiges hinzugelernt. So werden heute vermehrt manipulierte

Werbeanzeigen geschaltet, die Sie als Endnutzer auf eine betrügerische Website leiten sollen. Dort erscheint dann ein Hinweis, dass Sie zunächst bestätigen müssen, kein Roboter zu sein. Solche CAPTCHA-Abfragen, in denen Sie Ampeln und Fahrräder anklicken sollen, sind Ihnen mittlerweile vertraut.

In der Variante der Cyberkriminellen sollen Sie nun aber eine vermeintliche „Challenge“ in Ihre Zwischenablage kopieren, dann über ein Tastenkürzel ein Programm auf Ihrem Computer öffnen und diese Challenge dort einkopieren. Wenn Sie darauf reinfallen, infizieren Sie Ihren Computer sofort mit Schadsoftware. Diese Software kann dann Daten von Ihrem Gerät extrahieren. Das umfasst bspw. gespeicherte Passwörter, Ihren Browserverlauf, wertvolle Dokumente, aber auch Informationen zu installierten Programmen auf Ihrem Gerät oder Ihrem Standort. Und genau diese gestohlenen Daten landen dann gebündelt im Darknet auf Marktplätzen, wo andere Cyberkriminelle sie kaufen können, um damit Schaden anzurichten. Mit den Daten könnten sie etwa Ihre Geräte verschlüsseln, welche erst nach Zahlung eines Lösegelds wieder entsperrt werden.



Fake-CAPTCHA, das Schadsoftware einschleusen möchte.

Kriminelle stoppen nicht bei Ihren Daten

Logistikunternehmen stellen ein interessantes Ziel für Kriminelle dar. Dieselben Methoden, mit denen Systeme geknackt und Daten gestohlen werden, gefährden auch Ihre physischen Güter. Denn Frachtdiebstahl wird durch digitale Hinweise für Cyberkriminelle deutlich einfacher. Wer Zugriff auf Ihre Kundendaten, Transportpapiere und Live-GPS-Daten hat, weiß genau, wann besonders wertvolle Fracht unterwegs ist und wo der Fahrer Pause macht.

KI: Chance oder Gefahr?

Zunehmend wird auch vor den Gefahren von Künstlicher Intelligenz (KI) gewarnt. Zwar kann KI zur Stärkung der Cyberresilienz genutzt werden, indem sie Angriffsvektoren erkennt, Abwehrmaßnahmen optimiert und durch kontinuierliche Tests Systemlücken schließt. Auf der Seite der Angreifer allerdings beschleunigt KI das Handeln und ermöglicht auch weniger erfahrenen Cyberkriminellen, komplexe Systeme zu verstehen. Dass Angreifer von immer fortschrittlicheren Software-Tools

profitieren, ist nicht neu: Laut CrowdStrike sinkt die durchschnittliche Zeit, die ein digitaler Angreifer braucht, um sich vom anfänglichen Zugang zu einem Computersystem im Netzwerk auf weitere Systeme auszubreiten, bereits seit Jahren, zwischen 2021 und 2025 zuletzt um 70 Prozent auf nur noch 29 Minuten.

Eine weitere Bedrohung durch KI stellt die sogenannte „Shadow AI“ („Schatten-KI“) dar. Dieser Begriff bezeichnet die Nutzung von KI-Tools wie bspw. ChatGPT, Claude oder Gemini durch Ihre Mitarbeitenden ohne das Wissen – und die Erlaubnis – Ihrer IT-Abteilung. Klar, manch Arbeit nimmt einem die KI ab. Aber wenn Ihre Unternehmensdaten in den Eingaben oder Uploads enthalten sind, wandern diese zum Betreiber der KI ab.

Die Lösung dafür sollte i.d.R. nicht sein, KI vollständig zu verbieten. Die Vergangenheit zeigt: Mitarbeitende finden immer Wege, ein Verbot zu umgehen. Im Zweifel werden die Unternehmensdaten dann auf einem privaten Laptop oder Smartphone in ChatGPT und Co. eingegeben. Stattdessen sollten Sie klar kommunizieren, was erlaubt ist und was nicht. Und sich zusätzlich absichern: Längst gibt es Analyse-Software, die Ihnen aufzeigt, welcher Mitarbeiter welche KI-Systeme nutzt. Zusätzlich lässt sich mit solcher Software oft auch technisch verhindern, dass personenbezogene Daten oder schützenswerte Dokumente bei den KI-Anbietern landen. Beispielsweise werden personenbezogene Daten in Eingaben durch Sternchen (*) ersetzt oder Uploads von bestimmten Dateitypen (z.B. Excel-Dateien) unterbunden.

Fazit

Logistikunternehmen, die Cyberresilienz als strategisches Thema begreifen, gewinnen.

Cyberresilienz ist keine reine IT-Aufgabe. Es ist eine Managementaufgabe, eine Kulturaufgabe und zunehmend eine Wettbewerbsfrage. Kunden und Partner fragen heute explizit nach Sicherheitszertifizierungen und Resilienzkonzepten. Versicherungen machen ihre Deckung von diesen Nachweisen abhängig.

Die gute Nachricht: Der Aufbau von Cyberresilienz ist kein Alles-oder-Nichts-Projekt. Jede Maßnahme, die umgesetzt wird, macht das Unternehmen widerstandsfähiger. Jeder Vorfall, aus dem gelernt wird, stärkt die Organisation. Und jedes Unternehmen, das Cyberresilienz lebt, sendet ein klares Signal an Markt und Angreifer: Hier lohnt sich der Aufwand nicht.



Merlin Stottmeister ist Consultant für IT-Sicherheit bei der Bechtle AG. Er recherchiert im Darknet und informiert Kunden, wenn dort gestohlene Daten von ihnen auftauchen. Viel lieber zeigt er aber, was Unternehmen tun müssen, damit es gar nicht erst dazu kommt.
merlin.stottmeister@bechtle.com