Können Sie Manual-Mode?

IT SICHERHEIT Wie sieht Ihr Plan für die manuelle Auftragsabwicklung aus? Gehen Sie als Logistikunternehmen davon aus, dass nur Banken, Behörden oder Versicherungsunternehmen interessant für Cyberattacken sind? Die letzten Jahre haben etwas anderes gezeigt. Es stellte sich als trügerische Sicherheit heraus, dass die Logistikindustrie für Cyberkriminelle nicht interessant sei, weil es an hochvertraulichen Daten fehle. Denn auch Logistikunternehmen sind wiederholt von Cyberangriffen heimgesucht worden.

AUTOREN JEAN PIERRE LANG & NICHOLAS ALLAN

Als die Toll Group in Melbourne Opfer eines umfangreichen Angriffs wurde, der ihre sämtlichen IT-Systeme lahmlegte, haben sich die Mitarbeitenden vielleicht gefragt: «Können wir Manual-Mode? Wie sieht unser Plan für die manuelle Auftragsabwicklung aus?» Der Angriff auf die Toll Group war kein Einzelfall.

Die deutsche Logistikfirma Hellmann fiel 2021 einer Ransomware-Attacke zum Opfer. Hellmanns gestohlene Daten wurden auf dem Leak-Portal von der Ransomware-Gruppe «RansomEXX» veröffentlicht. Die 70 GB Daten enthielten sensible Anmeldeinformationen, Dokumente, Auftragsinformationen und Kundenvereinbarungen. Üblicherweise weist eine Veröffentlichung der Daten darauf hin, dass die Lösegeldforderung erfolglos war. Der Fall Hellmann zeigt, dass Logistikunternehmen durchaus für gezielte Attacken interessant sein können.

Die Fälle von Maersk und TNT Express, welche im Jahr 2017 «NotPetya» zum Opfer fielen, wie viele andere Firmen, zeigen auf, dass auch Logistikfirmen komplett lahmgelegt werden können. Die Unternehmen waren in diesem Fall lediglich Kollateralschäden, und nicht Ziel dieses Angriffs.

AUCH LOGISTIKUNTERNEHMEN SIND IN GEFAHR

Auch im Jahr 2022 ist die Gefahr einer Cyberattacke auf Logistikunternehmen nicht gebannt, wie es die Firma Expeditors schmerzlich erfahren musste. Sie waren mit einer Lösegeldforderung nach einem Cyberangriff konfrontiert. Wie bei allen Lösegeldforderungen, hatte auch Expeditors keine Garantie für eine Rückgabe der Daten, noch wussten sie, ob die vom Cyberangreifer getätigten Verschlüsselungen wieder aufgehoben würden.

Oft sind es nicht einmal gezielte Angriffe von Cyberkriminellen, die nach Schwachstellen suchen oder die über Pishing-E-Mails Mitarbeitende hinters Licht zu führen versuchen. Viele Malware ist ziellos im Netz unterwegs und befällt willkürlich Systeme. Gerade schwach geschützte und alte, bzw. veraltete Systeme sind besonders gefährdet. Bei Maersk – Opfer von Kollateralschaden – war dies der Fall und das Bezahlen eines Lösegeldes hätte keine Wirkung gezeigt.

Nach dem Maersk zum Kollateralschaden von NotPetya wurde, sahen sich die

Lösegeldforderung «NotPetya».

Foto: Adobe Stock #162683776

SECHS TIPPS FÜR LOGISTIKUNTERNEHMEN, MIT DEM MANUAL-MODE ZU ARBEITEN

1. Halten Sie Ihre Systeme und Software aktuell
Gezielte Angriffe, aber auch Infektionen durch zufällige Malware oder Ransomware profitieren von veralteter Software und nicht aktualisierten Systemen, da diese viel mehr Angriffsfläche bieten. Es versteht sich von selbst, dass Logistikunternehmen ihre Systeme mit den letzten Patches und Updates aktuell halten müssen.

2. Ersetzen Sie veraltete Server resp. Systeme
Des Weiteren empfehlen wir dringend, dass veraltete oder ungenutzte System ersetzt oder entfernt werden. Denn als Maersk Kollateralschaden von «NotPetya» wurde waren Server im Einsatz, welche noch unter Windows2000 liefen, obwohl der Support von Microsoft im Jahr 2010 eingestellt worden war. Dies bietet keinen vollständigen Schutz, neuere Systeme sind jedoch weniger anfällig, und machen es den Angreifern schwerer.

3. Erarbeiten Sie ein Schutz- und Resilienz-Konzept für alle Systeme
Logistikunternehmen haben oft modulare, komplexe IT-Landschaften, mit vielen internen und externen Schnittstellen zwischen dutzenden Altsystemen (Legacy-Systemen). Auch viele physische Anlagen wie Lagerhäuser oder Terminals stossen an ihre Kapazitätsgrenzen. AWK empfiehlt, Schutz- und Resilienz-Konzepte zu erarbeiten und diese einem existierenden Betriebskontinuitätsplan hinzuzufügen.

4. Schaffen Sie Kommunikationskanäle, welche nicht vom Firmen-Netzwerk abhängig sind
Die Firmentelefonnummer oder Firmen-E-Mail helfen bei den oben beschriebenen Cyber-Angriffen meist nicht weiter. Deshalb muss das Emergency-Response-Team vorbereitet und über Kanäle erreichbar sein, welche nicht im Firmen-Netzwerk integriert sind.

5. Schildern Sie auf «altmodische» Art aus, was bei einem Systemausfall zu tun ist
In Gebäuden ist ausgeschildert, was im Fall eines Feuers oder bei einer Gebäudeevakuierung zu tun ist. Informieren Sie an diesem Ort auch mit einem Aushang, was bei einem Systemausfall zu tun ist. Dieser Aushang am «Emergency Board» stellt sicher, dass die zu kontaktierenden Personen und Kontaktinformationen analog verfügbar sind.

6. Sensibilisieren und schulen Sie Ihre Mitarbeiter*innen
Stellen Sie sicher, dass Ihr BCM über die nötigen Ressourcen und Management-Unterstützung verfügt, die beteiligten Mitarbeiter*innen mit den Notfallunterlagen vertraut sind und in regelmässigen Abständen Notfallübungen durchführen.

Eins ist klar: Manuelle Massnahmen, eine firmeninterne Sensibilisierung für das Thema Cyberangriffe, sowie regelmässige Schulungen der Mitarbeiter*innen sind für diese ausserordentlichen Fälle unerlässlich.

Mitarbeiter*innen zur Kreativität gezwungen. Sie mussten in erster Linie auf private Kommunikationskanäle zurückgreifen wie WhatsApp oder private E-Mail-Konten. Sie klebten handgeschriebene Papierdokumente mit Sendungsdaten auf Fracht-Container. So entstand der Begriff «Manual-Mode», der unter den Maersk- und Hafenmitarbeitenden schnell ein vertrauter Begriff wurde.

WIE DIE MANUELLE GESCHÄFTSABWICKLUNG DIE BETRIEBSKONTINUITÄT SICHERT

Im Rahmen eines funktionierenden Business Continuity Managements (BCM) beschreibt der Betriebskontinuitätsplan, wie das Unternehmen auf die in der Geschäftsauswirkungsanalyse gefundenen Risiken zu reagieren hat. «Rechnen Sie damit, dass Sie im Fall eines Angriffs auf ihre Backup-Systeme zugreifen können? Doch was geschieht bei einem Komplettausfall, wenn sie keinen Zugriff mehr auf die IT-Systeme in der Firma haben? Wie kommunizieren Sie mit Kunden, Lieferanten und anderen Partnern oder wie nehmen Sie Bestellungen manuell entgegen?» Mit einem Plan für einen Manual Mode, der unter anderem alle Prozesse beinhaltet, die unbedingt weiterlaufen müssen, sowie diejenigen Prozesse, die für einen gewisse Zeit unterbrochen bleiben dürfen. Der Betriebskontinuitätsplan zeigt dabei alle Massnahmen auf, welche für die Weiterführung des Betriebes – oder Teile davon – notwendig sind. Dazu gehören neben manuellen Prozessen auch die Kommunikation nach innen und aussen.

Beim Fall von Toll Group, die im selben Jahr zweimal von Angriffen betroffen gewesen war, konnten die Verantwortlichen aufzeigen, dass alle manuellen Prozesse noch bekannt waren und dass diese sich bei der Bewältigung der ersten Attacke bewährt hatten. Hier stellen wir die Fragen an Sie: «Trifft das auf Ihre Betriebskontinuitätspläne auch zu? Führen Sie regelmässig Übungen durch? Sie sind vielleicht sogar verpflichtet, Ihre Prozesse manuell ausführen zu können?» Wir wissen von einem unserer Kunden im Pharmabereich, dass er im Vertrag festgehalten hat, der Spediteur müsse über Schreibmaschinen verfügen, falls die IT-Systeme ausfallen würden. Diesem Kunden war diese Absicherung so wichtig, dass er sogar die Schreibmaschine sehen wollte, um sicher zu gehen, dass der Spediteur für «Manual-Mode» ausgestattet ist.

WOHER KOMMEN DIE DATEN, WENN IT-SYSTEME NICHT MEHR ERREICHBAR SIND?

Manchmal haben Unternehmen einfach Glück. So war es im Fall des norwegischen Industrieunternehmen Norsk Hydro im Jahr 2019. Als Norsk Hydro der Cyberattacke «LockerGaga» zum Opfer fiel, konnte ihre belgische Fabrik in Lichtervelde auf die gedruckten Bestellungen eines Mitarbeiters zurückgreifen. Im Februar 2022 war auch Expeditors Opfer einer Cyberattacke und sie wussten nicht, ob der Angriff spezifisch oder nicht spezifisch gewesen war. Auch sie mussten alle Systeme offline nehmen. So wurde auch bei Expetitors der Begriff «Manual-Mode» schnell bekannt. Sie wurden gezwungen, gemäss Medienberichten, die Auftragsabwicklung auch manuell durchzuführen.

WWW.AWK.CH

DIE AUTOREN

Jean Pierre Lang ist Senior Consultant bei AWK Group AG und hat einen langjährigen Hintergrund in den Bereichen Lieferkette und IT-Management in der Logistikindustrie.

Nicholas Allan ist Senior Consultant bei AWK Group AG mit Fokus auf die Digitalisierung der Logistik. Vor AWK hat er bei DSV und Panalpina im IT-Management gearbeitet.