Handelsblatt
MONTAG, 21. DEZEMBER 2020, NR. 247

Lebensgefahr aus dem Netz

Deutsche Unternehmen vernachlässigen Cyber- und Transportsicherheit. Das kann beim Corona-Impfstoff lebensbedrohlich werden, warnt **Thomas R. Köhler.**

privat [M]

Thomas R. Köhler ist Research Professor am Institute for International Innovation der Hankou University in Wuhan (CN) und berät Unternehmen beim Aufbau sicherer Infrastrukturen und der Absicherung ihrer Wertschöpfungsketten.

Das Jahr 2020 hat uns vor Augen geführt, wie anfällig unsere westliche Welt für Cyberrisiken geworden ist: Im Herbst verstarb eine Notfallpatientin auf dem Weg in die Uniklinik Düsseldorf. Sie war nach einem Cyberangriff als Notfall abgewiesen worden, den Transport in das weiter entfernt gelegene Krankenhaus in Wuppertal hat sie nicht überlebt. Ähnliche Attacken gab es zuvor auf Krankenhäuser in Großbritannien, das Pharmaunternehmen Merck und die Logistikfirmen Maersk und TNT Express.

Erst kürzlich meldete die Europäische Arzneimittelagentur (Ema) einen massiven Hackerangriff. Die Angreifer hatten es auf Informationen zu den Corona-Impfstoffen von Biontech/Pfizer abgesehen. Erfolgreiche Cyberspionage würde einem Angreifer im weltweiten Wettbewerb potenziell Milliarden an eigenen Entwicklungsaufwendungen sparen. Die US-amerikanische Arzneimittelbehörde FDA geht nun auf Nummer sicher und lässt sensible Informationen der Impfstofffirmen durch das FBI transportieren – physisch, per USB-Stick statt Internet. *Eigentlich ein klares Warnsignal auch für deutsche Unternehmen und die Regierung, Cybersicherheit endlich ernst zu nehmen.*

Geschehen ist – mit Ausnahme von Absichtserklärungen – wenig. Sowohl Gesundheitswesen als auch Logistik fallen in Deutschland unter „kritische Infrastrukturen" (Kritis) und unterliegen damit besonderen Anforderungen an die IT-Sicherheit. Doch die Pandemie offenbart die Schwächen dieses Systems. Dabei sah es Anfang März noch so aus, als würde es eine Verschnaufpause in Sachen IT-Sicherheit geben, als Betreiber großer Schadsoftwarenetzwerke ankündigten, Krankenhäuser und andere Einrichtungen des Gesundheitswesens während der Pandemie zu verschonen.

Doch wie jede Strategie, die auf die moralische Integrität und Kooperation von kriminellen Akteuren setzt, hat auch diese nicht funktioniert. Bereits kurz nach der Ankündigung machte eine Ransomware-Attacke auf das Universitätsklinikum im tschechischen Brünn (Brno) Schlagzeilen, als das wichtige Behandlungs- und Testzentrum für Covid-19 zeitweise lahmgelegt war. Die Rechnung der Cyberkriminellen ist einfach: Dort, wo es um Leben und Tod geht, ist die Zahlungsbereitschaft hoch. Mit der Verfügbarkeit von Impfstoffen stellt sich nun die Frage nach der sicheren Verteilung vom Produktionsort bis zur durchgeführten Impfung.

Für Logistikexperten sieht das zunächst eher einfach aus, wenn – wie derzeit geplant – Impfzentren angefahren werden: Ein gängiger Impfstoffbehälter hat fünf Milliliter Volumen – also etwa so viel wie ein Fläschchen Augentropfen – und ergibt zehn Impfdosen. Ein gut geschulter Arzt mit funktionierender Administration kann vielleicht 100 Dosen pro Tag an Patienten verabreichen, ein handtellergroßes Paket reicht für einen Tagesbedarf. Selbst hochgerechnet auf die Gesamtbevölkerung sind die reinen Mengen zu vernachlässigen, wenn man von einer Verteilung über einige Monate ausgeht. Knapp 9000 Paletten transportiert etwa allein der Pharmalogistiker „Trans-o-flex" – pro Tag. Eine Herausforderung sind eher die Vorgaben von Biontech/Pfizer von minus 70 Grad Transporttemperatur.

Die wirklichen Gefahren lauern woanders, denn es wird zu Beginn der Verteilung einen Run auf den Impfstoff geben. Die auf dem Transportweg von China verschwundenen Gesichtsmasken für die Berliner Polizei sollten eigentlich Mahnung genug sein. Interpol sieht die Impfstoff-Logistikkette bereits im Visier des organisierten Verbrechens. Detlef Trefzger, Konzernchef der Logistikfirma Kühne + Nagel, warnte bereits vor möglichen Raubüberfällen auf Impfstofftransporte. Mehr Bewachung – etwa durch Polizei oder Bundeswehr – löst das Problem aber nicht vollständig.

Denn die Impfkette wird dort attackiert werden, wo sie am verwundbarsten ist – bei der Informationssicherheit. Schnellerer Zugriff auf den Impfstoff per Cyberattacke? Die Erfahrungen mit Manipulationsversuchen an Systemen für die Terminvergabe bei Behörden lassen Schlimmstes für die Impfstoffvergabe befürchten. Wer schafft es auf die Liste der besonders Bedürftigen und damit bei der Vergabe zu bevorzugenden Personen? Wer erhält den nächsten Slot im lokalen Impfzentrum? Darüber wird ein erbitterter Kampf hinter den Kulissen ausbrechen, ebenso wie um die Information, auf welchem Laster auf welcher Straße gerade welche Menge Impfstoff unterwegs ist.

Die Sicherheit von Informations- und Transportketten wird mit der Verfügbarkeit des Corona-Impfstoffs wichtiger denn je werden, doch die Akteure sind nicht ausreichend darauf vorbereitet. Häufigste lapidare Entschuldigung der Unternehmen: Bei uns ist noch nie etwas passiert. Das Kernproblem dahinter: Investitionen in Sicherheit lassen sich schlecht rechnen, und mangelnde Vorsorge erkennt man meist erst ex post. Doch dann ist es längst zu spät. Höchste Alarmstufe für Politik, öffentliche Hand und Verantwortliche in den Unternehmen, endlich ins Handeln zu kommen. Cybersicherheit ist Chefsache!