Frankfurter Allgemeine Zeitung vom 08.11.2021

Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND

Familienunternehmer vor schwarzen Bildschirmen

Die enorme Zunahme von Cyberattacken macht viele Firmen hilflos. Sie brauchen Schutz vom Staat. Und sie müssen das Thema Cybersecurity endlich zur Chefsache machen.

Von Klaus-Dieter Sohn

Es ist ein normaler Samstagmorgen im Familienunternehmen. Der Inhaber will kurz seine Mails abrufen, aber der Computer macht nicht mit. Der Monitor bleibt schwarz. Auf dem Display erscheint nur eine kleine Datei mit dem Namen "read me". Der Unternehmer weiß, er sollte jetzt selbst wissen, was zu tun ist. In der IT-Abteilung seines Unternehmens ist niemand erreichbar, denn es ist eben samstags um 10 Uhr. Fälle wie diese sind ständig Realität in deutschen Unternehmen - Höhepunkte von Cyberattacken, die meist schon Wochen oder Monate zuvor unbemerkt begonnen haben und dann bevorzugt an einem Wochenende oder Feiertag ihr hässliches Gesicht zeigen. Die Betroffenen ärgern sich dann, dass sie dem Thema Cybersecurity nicht genügend Aufmerksamkeit gewidmet haben. Aber sie ärgern sich auch über Staat und Justiz, die sie immer noch nicht ausreichend schützen vor diesen Angriffen, die sie in ihrer Existenz bedrohen können.

Lösegeld per Bitcoin

Die Vorgehensweise der Täter ist bekannt: Sie schleusen erst Schadsoftware in die Unternehmens-IT ein, stehlen dann die Daten und verschlüsseln schließlich das ganze System. Lösegeld gegen den Code für die Entschlüsselung, so lautet das unwiderstehliche Angebot. Das Zahlungsmittel der Wahl ist der Bitcoin, dessen Routen Ermittlungsbehörden nicht oder nur mit großem Aufwand nachverfolgen können.

Während im Jahr 2021 die Zahl der Cyberangriffe in Deutschland um mehr als 60 Prozent anstieg und die Lösegeldforderungen sich Schätzungen zufolge verzehnfachten, sind Ermittlungserfolge Mangelware. Wie dramatisch die Lage ist, verdeutlichen die Zahlen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Fachleute registrierten allein im Februar 2021 pro Tag durchschnittlich 553 000 neue Schadprogramm-Varianten. Der BSI-Lagebericht 2021 berichtet von 144 Millionen neuen Varianten im Berichtszeitraum, was einem Zuwachs von 22 Prozent gegenüber dem Vorjahr entspricht. Vor diesem Hintergrund erscheint die Feststellung des BSI-Präsidenten Arne Schönbohm, man habe "zumindest in Teilbereichen Alarmstufe Rot", schon beinahe als eine Untertreibung.

Die deutschen IT-Sicherheitsprobleme liegen dabei auch an der föderalen Struktur: Es ist nicht nachvollziehbar, weshalb es keine zentrale Anlaufstelle für Cyberkriminalität gibt, in welcher der Staat seine Kapazitäten bündelt. Selbst das Bundeskriminalamt hat für das Jahr 2020 rund 108 000 Delikte der Cyberkriminalität im engeren Sinne registriert, was eine Steigerung von 7,9 Prozent im Vergleich zum Jahr 2019 bedeutet. Das zeigt: Die organisierte Cyberkriminalität baut derzeit ihre Kapazitäten massiv aus, beflügelt von ihren großen Erfolgen und der Straffreiheit in ihren Heimatländern außerhalb der Europäischen Union. Dort drücken die Strafverfolgungsbehörden oft beide Augen zu, solange einheimische Angriffsziele von den Tätern ausgespart werden - so jedenfalls berichten es immer wieder Vertreter verschiedener Nachrichtendienste.

Die Bedrohung ist also ernst, doch die deutschen Behörden fühlen sich oft nicht zuständig. Wer etwa als bayerischer Unternehmer im Notfall Hilfe sucht, staunt nicht schlecht, wenn er im Internet auf den Seiten des bayerischen Verfassungsschutzes landet. Dort findet sich der Hinweis, dass es sich bei der "Cyberabwehr Bayern" nicht um eine neue Behörde oder eine öffentlich erreichbare Anlauf- oder Informationsstelle handele, sondern um ein internes Gremium, das für den Bürger nicht zu erreichen ist. Man möge sich bitte an eine der anderen sechs Behörden wenden, die dort aufgelistet sind. Ein Unternehmen, das mit einer akuten Cyberattacke zu kämpfen hat, verliert nicht nur wertvolle Zeit, sondern schnell auch das Vertrauen in den Staat.

Nur Austausch unter Behörden

Dabei unterhalten Bund und Länder eigentlich schon eine durchaus leistungsfähige Cyber-Sicherheitsarchitektur, zu der unter anderem das Nationale Cyber-Abwehrzentrum (NCAZ) gehört. Bislang werden über diese Plattform aber nur die Erkenntnisse der verschiedenen Behörden und Dienste untereinander geteilt. Die Wirtschaft sollte in diesen Austausch einbezogen werden. Denn hier sind die Innovationskraft und der technologische Vorsprung gebündelt, auf den es die Cyberattacken meist abgesehen haben. Es ist unbefriedigend, dass nur die Betreiber kritischer Infrastrukturen (KRITIS) in den Informationsfluss des NCAZ eingebunden werden.

Das NCAZ könnte zu einem echten Cyber-Abwehrzentrum ausgebaut werden. Dazu gehört eine zentrale Anlaufstelle für die Wirtschaft genauso wie für IT-Forensiker, die Beweise sichern können. Dazu gehört außerdem eine Strafverfolgungsbehörde, die Ermittlungen durchführen und Täter zumindest innerhalb der EU dingfest machen kann. Wichtig wäre eine Kontaktstelle zu Europol und eine gute Informations-

kette zu den Vertretern der Wirtschaft, damit staatliche Analysen und Handlungsempfehlungen zu erkannten IT-Vorfällen, Verwundbarkeiten und Angriffsformen den Unternehmen zugutekommen.
Und auch der Gesetzgeber ist gefordert. Die Cyberkriminalität wird durch Kryptowährungen wie den Bitcoin enorm begünstigt. Die Blockchain-Technologie bietet Kriminellen die Möglichkeit, nahezu unbehelligt ihr Werk zu verrichten. Der Gesetzgeber sollte Kryptowährungen also zumindest derart regulieren, dass die Rückverfolgbarkeit für Strafverfolgungsbehörden möglich wird - und die sogenannte Wallet, also die digitale Geldbörse, gelöscht oder eingefroren werden kann. Hier wäre ein global abgestimmtes Vorgehen wünschenswert, der EU-Gesetzgeber sollte aber jedenfalls den Anfang machen.

Nicht auf zerstörerische Kräfte geeicht

Bis der Staat tätig wird, muss die Wirtschaft ihre Abwehrkräfte stärken. Doch dort wird das Thema Sicherheit oft noch so behandelt, als müsste man sich wie früher nur vor echten Einbrechern schützen. Zwar ist der Werkschutz weiter relevant, von der Alarmanlage bis zur Zugangskontrolle. Aber mit der Digitalisierung sind neue Themen hinzugekommen. Weit weg vom unternehmerischen Alltag lauern die Gefahren, und der Gegner ist unsichtbar. Das Personal ist dafür nicht oder nur unzureichend ausgebildet. Zwar hat jeder Mittelständler eine IT-Abteilung. Aber deren Kernkompetenz liegt in der Systemadministration. Wenn die firmeneigenen Systeme störungsfrei laufen, alle Komponenten miteinander kompatibel sowie Firewall und Virenscanner vorhanden sind, breitet sich häufig Zufriedenheit aus - auf die nun wachsenden zerstörerische Kräfte von außen sind diese Abteilungen nicht geeicht.
Cybersicherheit muss daher Chefsache sein. Die Geschäftsführung muss den aus der analogen Welt kommenden Sicherheitsleiter damit beauftragen, auch die mit der Digitalisierung einhergehenden Gefährdungen zu analysieren und in ein sinnvolles Sicherheitskonzept zu überführen. Organisatorische und personelle Entscheidungen sind zu treffen. Hat das Unternehmen ausreichend Ressourcen, um die Cybersicherheit selbst aufzustellen? Oder sollte ein externer Dienstleister zur Unterstützung herangezogen werden? Wie viel Geld soll investiert werden für eine Sache, für die es keinen unmittelbar messbaren "Return on Investment" gibt?
In jedem Fall sollte in dieser Abwägung berücksichtigt werden, was die Wiederherstellung der IT-Systeme kostet, wie groß ein mehrtägiger Umsatzausfall ist und ob Vertragsstrafen bei Lieferausfall drohen. Klar ist, dass insbesondere kleine und mittelgroße Unternehmen schnell an ihre Grenzen stoßen. Hier bieten sich möglicherweise standardisierte Lösungen an, wie sie unter anderem das BSI bereitstellt. Was den Schutz der eigenen Daten anbelangt, könnte die Speicherung in der Cloud eine Lösung sein. Denn die Anbieter der Cloud-Lösungen haben ein besonders großes Interesse am Schutz ihrer Systeme und profitieren von Größenvorteilen. Aber es muss klar sein, dass die Daten möglicherweise auf Servern außerhalb der EU gespeichert werden, was Fragen zum Datenschutz aufwirft. Für die pauschale Furcht vor der Cloud, wie sie manchen Unternehmen eigen ist, besteht indes kein Grund.
Es ist aber auch schon viel gewonnen, wenn die Geschäftsleitungsebene das Problem erkennt und einfache Präventionsmaßnahmen ergreift. Denn der häufigste Angriffspunkt ist der Mensch. Er wird regelmäßig dazu verleitet, eine digitale Tür zu öffnen, damit die Kriminellen ihre Schadsoftware unbemerkt einschleusen können. Unternehmen sollten ihre Mitarbeiter sensibilisieren. Wer eine gefälschte Mail von einer echten Mail unterscheiden kann, klickt im Zweifel nicht auf das angehängte Dokument, sondern schiebt die Mail in einen Quarantäne-Ordner, wo sie von der IT-Abteilung geprüft werden kann.
Außerdem sollten sämtliche USB-Anschlüsse für unerwünschte Speichermedien blockiert werden. Dass das nötig ist, zeigt der Fall eines großen Familienunternehmens aus dem Konsumgüterbereich, das seinen Mitarbeitern zur Gefahr externer Speichermedien extra Schulungsvideos vorgeführt hatte. Kurz danach legte es auf dem Unternehmensparkplatz einen Köder aus: einen Umschlag mit einem USB-Stick und dem Hinweis "zur Erinnerung an diesen besonderen Urlaub". Es verging keine Viertelstunde, und der präparierte USB-Stick fand den Weg in den Rechner eines Mitarbeiters.

Krisenstab für die Betriebsunterbrechung

Im nächsten Schritt sollten die "Kronjuwelen" definiert werden, also jene Daten, die für das Unternehmen von existenzieller Bedeutung sind. Für diese Daten muss der technisch beste Schutz aufgesetzt werden. Auch das Business-Continuity-Management (BCM) ist zu betrachten, mit dem vorgesorgt wird für Krisenzeiten, wie wir sie jüngst mit der Corona-Pandemie erlebt haben - auf dass der Betrieb in jedem Fall weiterläuft. Das BCM ist unbedingt um den hypothetischen Fall einer Cyberattacke zu ergänzen. Es muss ein Krisenstab her, mit festen Mitgliedern und einem Katalog von Maßnahmen, die im Vorfeld eingeübt werden. Welche Behörden sind einzuschalten, welche Dienstleister sind abrufbereit? Auch die Kommunikation mit Kunden und Lieferanten gilt es festzulegen. Wer als Zulieferer befürchten muss, für Wochen auszufallen, weil die Produktion aufgrund einer Cyberattacke stillsteht, der vernichtet Vertrauen, wenn er falsch kommuniziert.
Eine wichtige Frage lautet überdies: Gibt es eine Cyberversicherung, die Unterstützung bietet? Und die bezahlbar ist? Denn bei den Versicherern macht sich die Häufigkeit der Schadenfälle mittlerweile deutlich bemerkbar. So berichtet etwa die Spezialversicherung der Allianz über 1000 Cyberschäden im Jahr 2020 gegenüber rund 80 im Jahr 2016. Die Zahl der Schäden aus Ransomware (also aus den eingangs beschriebenen Schadprogrammen) stieg im Vergleich zu 2019 um rund 50 Prozent. Entsprechend hätten sich die Preise für die Policen entwickelt. Neukunden berichten, sie erhielten Verträge nur noch, wenn sie alle Möglichkeiten ausschöpften, um sich vor Cyberangriffen zu schützen.
Ebenfalls sehr wichtig ist die Verfügbarkeit von Sicherheitskopien der Unternehmensdaten, um den Betrieb schnellstmöglich wieder in Gang zu setzen. Ein großes Familienunternehmen für Flüssiggas und Kraftstoffe hat nach einem Angriff das Magnetband als Sicherungselement wieder eingeführt. Es hatte gelernt, wie aufwendig es ist, die Geschäftsvorgänge auch nur weniger Wochen von Hand zu rekonstruieren.
Stets muss man sich bewusst machen, dass infolge einer Cyberattacke die gesamte EDV ausfällt. Nicht mehr verfügbar sind demnach sämtliche Zugangsdaten, die in aller Regel gespeichert werden, um sie nicht bei jedem Zugriff auf die diversen Accounts eingeben zu müssen. Es müssen also Listen

mit Zugangsdaten in ausgedruckter Form in einem Schließfach lagern. Auch das BCM-Handbuch sollte als Printversion vorliegen, einschließlich der Telefonnummern der wichtigsten Mitarbeiter. Das klingt alles selbstverständlich, wurde aber dem Krisenmanagement eines Onlinehändlers in Familienhand zum Verhängnis; zwar gab es entsprechende Verzeichnisse, aber eben nur auf dem Firmenserver.

Die Lieferkette als Angriffspunkt

Ein letzter Gedanke gilt dem neuesten Trend, der Supply-Chain-Attacke, also der Angreifbarkeit der Lieferkette. Weiß der Unternehmer eigentlich, welche elektronischen Bauteile in seinen Vorprodukten eingebaut sind? Und kann er gewährleisten, dass darunter keine Bauteile sind, die eine Hintertür für unbemerkte Zugriffe aus der Ferne enthalten? In der Diskussion um das autonome Fahren wurde das deutlich: Was, wenn die Steuerungselektronik, die mit dem Internet verbunden ist, von außen manipuliert werden kann? Automobilhersteller und deren Zulieferer haben deshalb mittlerweile Sicherheitsstandards definiert und überprüfen regelmäßig, ob sie entlang der gesamten Lieferkette eingehalten werden.

Besonders schwierig aber wird die Situation, wenn viele Kunden ihre Software-Updates von ein und demselben Zulieferer beziehen und dieser Opfer eines Angriffs wird. Im Fall von Kaseya, einem amerikanischen IT-Dienstleister, wurde das Ausmaß dieser Gefahr deutlich. Infolge einer Cyberattacke fielen etwa sämtliche Kassen des schwedischen Lebensmittelhändlers Coop aus.

Bei Kaseya allerdings gab es die Staatshilfe, die wir in Deutschland noch weitgehend vermissen. Am 2. Juli 2021 bemerkte das Unternehmen den Angriff durch "REvil", eine in Russland geduldete Hackerbande. Am 8. Juli sagte eine Sprecherin des Weißen Hauses, dass die amerikanischen Sicherheitsbehörden eine Aufforderung an die russischen Sicherheitsbehörden adressiert hätten, sie in der Abwehr des Angriffs zu unterstützen. Am 13. Juli wurden sämtliche bekannten Internetseiten der besagten Bande vom Netz genommen. Am 22. Juli teilte Kaseya schließlich mit, einen "Masterkey" erhalten zu haben, um sämtliche verschlüsselten Daten ihrer Kunden wieder entschlüsseln zu können.

Auch wenn keine weiteren Details bekannt wurden, ist die Wahrscheinlichkeit groß, dass es einen Zusammenhang zwischen der staatlichen Intervention und der positiven Entwicklung der Ereignisse gegeben hat. Die Frage drängt sich auf: Hätte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) genug Gewicht, um mit russischen Sicherheitsbehörden zu verhandeln?

Klaus-Dieter Sohn ist Leiter Wirtschaftspolitik der Stiftung Familienunternehmen.