SCHUTZ GEGEN CYBERANGRIFFE

In die Medien schaffen es nur die spektakulären Fälle, also Datenlecks und Datenklau im grossen Stil. Das erweckt den Eindruck, Cyberkriminalität sei ein Thema, das nur grössere Firmen betreffe. Das ist leider falsch, die Zahl der Fälle nimmt laufend zu. KMU sind zuweilen besonders leichte Beute, hier besteht Nachholbedarf.

Digitale Kriminalität (Cyberkriminalität) hat viele Gesichter. Wir alle kennen sie, diese Nachrichten im privaten E-Mail-Eingang, mit denen uns ein unbekannter, aber wohlmeinender Mensch an seiner Millionenerbschaft oder seinem Kryptovermögen beteiligen möchte. Nicht jeder Betrugsversuch ist so einfach zu durchschauen. Zudem sind Angriffe auf Unternehmen in der Regel etwas ausgefeilter, sie erfolgen aus dem Hinterhalt und nutzen unterschiedliche (technische) Einfallstore. Und wenn Cyberkriminelle die Schwachstellen im Informationssystem einer Firma entdeckt und überwunden haben, ist es für das betroffene Unternehmen schon zu spät. Die Statistiken machen klar, dass parallel zur fortschreitenden Digitalisierung auch die digitalen Angriffe und Betrugsdelikte zügig zunehmen. Nicht zuletzt begünstigt übrigens die vermehrte Nutzung des Homeoffice die Kriminellen, weil es oft an den nötigen Sicherheitsvorkehrungen fehlt.

Es kann jeden treffen

Die Annahme, dass für Cyberkriminelle vor allem grosse Unternehmen interessant sind, stimmt nicht. Um es etwas salopp zu sagen: «Kleinvieh macht auch Mist.» Nehmen wir als Beispiel eine Bäckerei mit mehreren Filialen: Ein wichtiger Umsatzträger ist das Geschäft mit Firmenkunden, namentlich Lunch-Lieferungen sowie Catering für interne und externe Anlässe. Dieses Geschäft, das mehrheitlich Stammkunden bedient, läuft im Grossen und Ganzen digital ab. Die Kunden bestellen online. Offert- und Rechnungswesen sind mit dem Bestellsystem verknüpft und funktionieren weitgehend automatisiert. Ebenso wird die Fahrtenplanung für die Auslieferungen direkt aus diesem System heraus erstellt. Insgesamt ist das eine sehr interessante Ausgangslage für Cyberkriminelle. Wenn es ihnen gelingt, in das IT-System einzudringen und die Daten verschwinden zu lassen, legen sie auf einen Schlag das ganze Bäckereigeschäft mit den Firmenkunden lahm. Die Bäckerei wird damit leichte Beute für Erpressung. Das Angebot der Cyberkriminellen: ein sofortiges Lösegeld von 25 000 Franken gegen die Rückgabe der Daten. Unter Zeitdruck und mit Blick auf das potenzielle Chaos, den geschäftlichen und den Imageschaden ist die Chance sehr gross, dass die Bäckerei dem Erpressungsversuch nachgibt – sich also gewissermassen mit einem blauen Auge aus der Affäre zieht und den Fall auch nicht an die grosse Glocke hängt.

Ein weiteres «Geschäftsmodell» der Cyberkriminellen ist der Weiterverkauf von gestohlenen Daten an Dritte. Im skizzierten Beispiel der Bäckerei ist der Wiederverkaufswert der entwendeten Daten vermutlich gering. In einem anderen KMU sieht das aber wieder anders aus: zum Beispiel bei einem Autohändler, in dessen Informationssystem umfassende persönliche und finanzielle Daten seiner Kundschaft gespeichert sind. Der Diebstahl solcher Daten lässt sich für Cyberkriminelle gut in bare Münze umwandeln.

Daten fischen per E-Mail

Die häufigste Form der Cyberkriminalität kommt in Unternehmen unter dem Deckmantel einer falschen Identität daher. Wer kennt sie nicht, diese E-Mails, in denen ein vermeintlich seriöses Unternehmen – ein Kurierdienst, die Post, die Bank – um vertrauliche Daten, Kontoangaben oder die Herausgabe von Passwörtern bittet. Solche Versuche, an die Daten von ahnungslosen Nutzern zu kommen, werden als Phishing bezeichnet. Hier braucht es einerseits organisatorische Massnahmen (z. B. Sensibilisierung der Mitarbeitenden), andererseits technische Vorkehrungen.

Informationssicherheit im KMU erhöhen

Das System von Cyberkriminellen besteht nicht unbedingt darin, besonders zahlungskräftige Firmen zu betrügen oder zu erpressen. Ihre Bemühungen zielen darauf ab, Schwachstellen in den Informationssystemen zu identifizieren. Je weniger ein System gesichert ist, desto einfacher ist der Zugriff. Eben deshalb muss sich jedes Unternehmen, unabhängig von der Grösse, mit der Sicherheit seiner Informationssysteme befassen.

Einen guten Einstieg in die Thematik bietet ein Merkblatt des Nationalen Zentrums für Cybersicherheit (NCSC), ein Kompetenzzentrum des Bundes. Das Merkblatt zeigt im Sinn einer Checkliste auf, was KMU in zwei Bereichen – organisatorisch und technisch – vorkehren können, um sich besser gegen Cyberangriffe zu schützen. Für weitere Informationen scannen Sie bitte den QR-Code oder verlinken Sie sich mit: **www.ncsc.admin.ch:** «Merkblatt Informationssicherheit für KMUs»

Lukas Herzog
Vizepräsident des Schweizerischen Treuhänderverbands
TREUHAND|SUISSE, Sektion Zürich