Trickreiche Versuche

Modernes Risk-Management

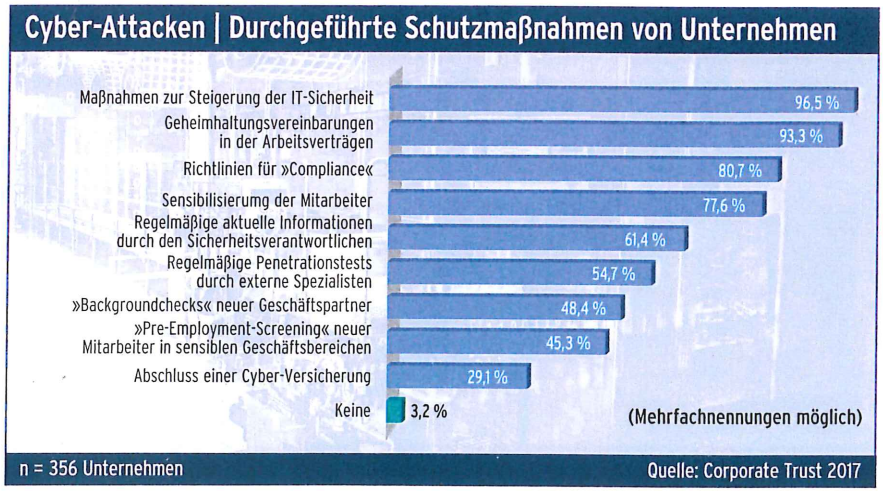
Deutsche Unternehmen erleiden jedes Jahr große Schäden durch Angriffe Krimineller. Die zunehmende Digitalisierung erleichtert es den Tätern immer mehr, in eine IT einzudringen, vertrauliche Daten abzusaugen, Geldtransaktionen auszulösen oder aber »Fake news« zu streuen. Da die Angreifer trickreich sind, müssen Unternehmen im »Risk Management« neu denken. Außer technischen Schutzmaßnahmen sind die organisatorischen Regeln und der Faktor Mensch sehr wichtig.

Christian Schaaf

Die Digitalisierung bietet zahlreichen Unternehmen durch automatisierte Produktionsabläufe, schnellere Lieferprozesse und neue Absatzwege große Chancen. Diese positive Entwicklung birgt jedoch gravierende Gefahren. Maschinen werden ans Internet angeschlossen, um schadhafte Teile früh zu erkennen und sie fernzuwarten. In der Verwaltung von Firmen wird die Office-IT aus Effizienzgründen und aus Kostengründen in die »Cloud« verlagert. Die Integration von Privatgeräten in die Firmenkommunikation schreitet voran, auch, damit Mitarbeiter geschäftliche E-Mails auf ihren eigenen Smartphones empfangen können. Dies alles aber eröffnet Cyberkriminellen ihre Einfallstore.

Für Unternehmen stellt dies eine große Herausforderung dar. Während man vor Jahren noch darauf vertrauen durfte, dass die IT-Abteilung den Schutz der eigenen Infrastruktur mit Hard- und Softwareprodukten im Griff hatte, ändern sich die Gelegenheiten für die Angreifer und damit das Bedrohungsspektrum gerade ganz erheblich. Immer öfter werden bekannte, klassische Betrugsmaschen mit dem professionellem Know-how von Hackern kombiniert, um an ein kriminelles Ziel zu kommen. Für die meisten Mitarbeiter sind solche Angriffe nur schwer zu erkennen.

Die IT-Abteilungen in den Unternehmen können den Schutz der Systeme daher nicht mehr ohne Weiteres bewerkstelligen. Zum einen fehlt ihnen das Wissen und meist auch die Zeit, um ständig über die immer raffinierteren Angriffe informiert zu sein und immer wieder neue Schutzmaßnahmen zu etablieren. Zum anderen, weil der Einkauf in vielen Unternehmen zu schwerfällig ist, um in Echtzeit auf sich ständig verändernde Bedrohungen zu reagieren. Soll eine neue Software oder gar ein komplexes System beschafft werden, sind die Verhandlungen und die Freigabeprozesse oft so langwierig, dass die Implementierung erst erfolgt, wenn sich die Welt schon wieder weiter gedreht hat, so dass eigentlich bereits auf die nächste bekannte Bedrohung reagiert werden müsste.



Darüber hinaus herrscht in vielen Geschäftsleitungsetagen noch zu wenig Verständnis für die heutige Situation und die Anforderungen rund um die Cybersicherheit. Dies spiegelt sich in zu kleinen Budgets und zu geringen personellen Ressourcen für den eigenen IT-Bereich wider, aber auch im zu geringen Stellenwert des Themas. Dem Management wird allerdings nichts anderes übrig bleiben, als sich permanent und intensiv mit den digitalen Entwicklungen auseinander zu setzen, um am Ball zu bleiben und schnelle Entscheidungen zu treffen. Das Thema ist zu wichtig, um es liegen zu lassen und zu hoffen, dass irgend jemand im Haus es im Zweifel schon richtig machen wird.

In diesem Sinne hat Corporate Trust mit dem Bayerischen Verband für Sicherheit in der Wirtschaft (BVSW) und der Brainloop AG 2017 einen »Future Report« (»Weltweite Megatrends und ihre Sicherheitsherausforderungen«) erarbeitet, der 4.738 Vorstände und Geschäftsführer bzw. Leiter der Bereiche »Compliance«, Risiko-Management, Unternehmenssicherheit, Informationsschutz, Finanzen, Controlling, Recht, Interne Revision, IT und Personal zu den Schäden in ihren Unternehmen befragt. Die Resultate zeigen klar, wie verwundbar die Wirtschaft ist.

In knapp 30 % der befragten Unternehmen gab es bereits einen festgestellten Informationsabfluss oder Spionage. Über die Hälfte der Unternehmen wurde in den letzten beiden Jahren Opfer eines Angriffs aus dem Reich der Organisierten Kriminalität, sei es durch »Spear-Phishing«-Mails oder »Fake President«-Attacken (»CEO-Frauds«).

Gerade der »CEO-Fraud« illustriert die Veränderung der Bedrohungslage gut. Dabei geht es um falsche E-Mails, die scheinbar von einem Mitglied der Geschäftsleitung kommen und oft an Mitarbeiter in der Buchhaltung gehen. In ihnen wird, aus vermeintlich berechtigten Gründen, die Überweisung eines hohen Geldbetrags auf eine ausländische Bankverbindung beauftragt. Die Täter setzen auch gefälschte Briefe oder Formulare zur Unterstützung dieser Anweisung ein. Sie können Logos, Freigaben von Vorständen und Geschäftsführern und andere interne Identifikationszeichen enthalten.

Für die Mitarbeiter sind solche E-Mails oder Briefe nicht als Fälschung zu erkennen und sie weisen die hohen Geldbeträge an. Eigentlich ist es eine klassische Betrugsmasche der Organisierten Kriminalität (OK), Menschen durch geschickte Manipulation hinters Licht zu führen und ihnen Geld aus der Tasche zu ziehen, doch in diesem Fall tritt sie gepaart mit sehr viel IT-Know-how auf. Die Täter müssen genau recherchieren, wie der interne Sprachgebrauch ist, welche Mitarbeiter für solche Vorgänge verantwortlich sind, wie die Stellenbezeichnungen lauten und wie Vorstände oder Geschäftsführer unterschreiben. In der Regel gehen einem »CEO-Fraud« also Hackerangriffe voraus, durch die sich die Täter Zugriff auf das Firmennetzwerk und die interne Kommunikation verschaffen. Zudem bedarf es großen IT-Know-hows, um E-Mails so zu fälschen, dass sie aussehen, als kämen sie vom Chef.

Generell gilt, dass die Organisierte Kriminalität ihre Aktivitäten immer mehr in den Cyberraum verlagert. Während sie ihr Geld früher mit Falschgeld, Rauschgift und Waffenhandel verdiente, erbeutet sie heute bereits viel Geld durch Cyberangriffe. Die Täter sitzen an ihrem PC ohne ihren sicheren Bereich für ihre kriminellen Angriffe zu verlassen. Da viele Aktivitäten aus dem Ausland kommen, und zwar oft aus Ländern mit viel geringerem Verfolgungsdruck durch Ermittlungsbehörden, ist die Gefahr, bei einer solchen Masche aufgedeckt und festgenommen zu werden, deutlich geringer als bei herkömmlichen Formen von Kriminalität.

Ein weiterer Angriffspunkt ist das »Next big thing« in der IT, das Internet der Dinge (»Internet of Things«, IoT). Gemeint ist die Vernetzung diverser Geräte, Assistenzsysteme, »Wearables«, tragbarer kleiner Computer, die Körperfunktionen messen, und von »Gadgets«, die eher Freizeitthemen bedienen, über das Internet. Wir steuern ja unsere Heizung heute schon per Smartphone, befragen »Alexa« (Amazon Echo) nach dem Wetterbericht und geben Ziele im Fahrzeug sprachgesteuert ein. Außerdem wird natürlich das Büro der Zukunft digital. Das Licht geht an, wenn jemand mit seinem Smartphone den Raum betritt. Die Anmeldung am PC erfolgt mit »Face ID«. All dies macht unser Leben leichter, aber wir geben auch ein Stück weit die Kontrolle über unsere Daten ab, teilweise ohne zu wissen, an wen. Das bietet Angreifern zahlreiche Ansatzpunkte.

Um mehr Sicherheit zu realisieren, sollte es also technische Schutzvorkehrungen geben, vor allem aber permanente Schulungen des Managements und der Mitarbeiter sowie neu geregelte organisatorische Prozesse, etwa schnellere und flexiblere Einkäufe und Implementierungen. Unternehmen müssen das Dilemma gestalten, ihr Know-how verteidigen (Wettbewerbsvorteils) und zugleich internationale Kooperationen eingehen, um global produzieren und absetzen zu können. Wer nur Zäune baut, kann die Welt nicht erobern. Man wird sich daher auf den Schutz seines wirklich essentiellen Know-hows beschränken müssen, wobei es sich in den meisten Firmen um 5 bis 10 % ihrer verfügbaren Informationen handelt.

Bald wird sich auch niemand mehr leisten können, ohne Serverstrukturen in der »Cloud« auszukommen. Dabei sollte man sich im Zeichen der Datenschutzgrundverordnung (DSGVO) fragen, wie man es angehen will und soll. Soweit es nicht aus anderen Gründen erforderlich ist, Daten in die USA oder nach Asien auszulagern, sorgen Lösungen in Europa dafür, nicht allen denkbaren Datenabgriffen ausgeliefert zu sein.

Im Risk-Management wird eine Hauptaufgabe sein, den Schutzbedarf von Informationen und des Know-hows sowie aktuelle Bedrohungslagen permanent zu evaluieren. Dafür muss es einen standardisierten, geregelten Prozess geben, an dem die relevanten Bereiche im Unternehmen beteiligt sind. Die IT-Abteilungen können sich erst dann über technische Maßnahmen Gedanken machen, wenn die Geschäftsleitung den Schutzbedarf von Informationen festgelegt und anhand des realistischen Bedrohungspotenzials über die Umsetzungstiefe entschieden hat. Das setzt voraus, dass man eine Menge von der Materie versteht und sich immer wieder über den Stand der Dinge informiert. Im Übrigen gilt, dass Sicherheitskonzepte so effektiv und diskret sein sollten, dass sie am besten gar nicht wahrgenommen werden. Das ist die Mission. Wer es gut in seinem Unternehmen macht, schafft Umgebungen, in denen man sich sicher und ungestört auf seine Ziele und auf die Ziele des Unternehmens konzentrieren kann. Im Mittelpunkt steht dabei stets der Mensch. ■

Christian Schaaf, Geschäftsführender Gesellschafter Corporate Trust, Business Risk & Crisis Management GmbH, München