Ernstes Thema
Cyber-Sicherheit in Unternehmen

VOLKSWIRTSCHAFT Die Sache ist, wie sie ist: Das Internet ist ganz überwiegend ein Segen, aber es ist auch ein Fluch. Die grenzenlose Offenheit des Netzes und die weitgehende Anonymität, in der sich Straftäter ihrer Verfolgung entziehen, sind ein Nährboden für kriminelle Attacken auf die Integrität und auf sensible Informationen von Unternehmen. Im Erfahrungswissen darum, dass es auch aufgrund der technologischen Komplexität keine Unangreifbarkeit gibt, bleibt nur, stets ein Möglichstes zur Abwehr zu tun.

Kein Mittelständler kommt heute mehr ohne zuverlässige, vor allem aber sichere Informations- und Kommunikationssysteme aus, wobei die Digitalisierung in der Produktion und hinsichtlich der Prozesse ständig fortschreitet, während die personelle und die finanzielle Ausstattung der IT oft nicht Schritt mit dieser Entwicklung hält. In dieses Delta stoßen international Cyber-Kriminelle und Wirtschaftsspione vor. Untersuchungen zeigen aber auch, dass das Bewusstsein in der deutschen Wirtschaft wächst, dass solche Cyber-Angriffe die Existenz bedrohen können.

Grundsätzlich entstehen in der vernetzten digitalen Welt immer mehr Schauplätze und Abhängigkeiten. Das Internet ist für die Kommunikation mit Kunden und Lieferanten unverzichtbar, die Produktion wird von Computern gesteuert, während Hersteller und Wartungsfirmen Zugriff auf die interne IT-Infrastruktur haben. Die neuen Möglichkeiten im Hinblick auf das »Internet der Dinge«, aber auch die Vernetzung von Systemen und Prozessen in der Produktion machen ein störungsfreies Funktionieren dieser Infrastrukturen unabdingbar. Indessen nehmen Angriffe auf die IT von Jahr zu Jahr zu.

Große Gefährdung der Unternehmen ▸ In der Anfang 2018 publizierten Umfrage über den Stand der Dinge in der Cyber-Sicherheit, die das BSI im Rahmen der Allianz für Cyber-Sicherheit in rund 900 Unternehmen und Institutionen durchgeführt hat, gaben tatsächlich 70 % der Betriebe an, in den letzten beiden Jahren bereits Opfer von Cyber-Angriffen geworden zu sein. In knapp der Hälfte der Fälle waren die Angreifer erfolgreich und konnten sich Zugang zu IT-Systemen verschaffen oder die Funktionsweise von IT-Systemen beeinflussen oder Auftritte im Internet manipulieren. Jeder zweite dieser erfolgreichen Angriffe löste Produktions- bzw. Betriebsausfälle aus. Damit sind Cyber-Angriffe eine der größten Bedrohungen für den Erfolg der Digitalisierung der deutschen Wirtschaft. Dabei steht der Mittelstand mit seinem enormen, teils weltmarktführenden Know-how ausdrücklich im Fokus der Täter.

> »Eine Welt, die sich sehr von der unterscheidet, in der man dauernd hört, wir geben so viel wie möglich nach draußen.«

Ständig auftretende neue Schwachstellen und Sicherheitslücken bieten Cyber-Kriminellen ständig neue Angriffsflächen und sehr weitreichende Möglichkeiten, um Informationen und Forschungsergebnisse auszuspähen, Geschäftsprozesse und Verwaltungsprozesse zu sabotieren oder um sich international auf Kosten Dritter zu bereichern.

Die Zahlen sind erschreckend: Zurzeit sind in der PC-Welt etwa 620 Millionen Varianten von Schadprogrammen bekannt, zu denen täglich rund 280.000 neue Varianten hinzukommen. Cyber-Angriffe haben bereits im Jahr 2016 in Deutschland Schäden in zweistelliger Milliardenhöhe verursacht.

Voller Werkzeugkasten der Angreifer ▸ Die Angreifer nutzen diverse technische oder organisatorische Schwachstellen in Unternehmen. Die Bandbreite reicht vom Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (Identitätsraub) über die Ausspähung und Fälschung von Daten bis zur Computersabotage. Sorge bereiten vor allem groß angelegte Cyber-Angriffe mit Schadsoftware. Mitte 2017 wurden über 200.000 Rechner weltweit mit der Malware »WannaCry« und »NotPetya« infiziert. Die Schadenschätzungen reichen von einigen Hundert Millionen bis zu vier Milliarden Dollar.

Auch der sogenannte »CEO-Fraud« tritt häufig auf. Dabei fordert eine (gefälschte) E-Mail mit Absenderadresse aus einem Unternehmen und mit korrekter Signatur ausführungsfähige Mitarbeiter zu einer finanziellen Transaktion auf. Diese Methode kombiniert gut gemachtes »Spear-Phishing« mit professionellem »Social Engeneering«.

Arne Schönbohm

Die Angreifer legen es darauf an, mit »Advanced Persistent Threats« (APT), sukzessive in die IT-Infrastruktur von Unternehmen einzudringen, um sensible Informationen längere Zeit auszuspähen. Ziel ist nicht nur die klassische Büro-IT, sondern betroffen sind auch Systeme in der Fabrikautomatisierung, in der Prozessautomatisierung und Steuerungsanlagen in der Industrie (»Industrial Control Systems«, ICS), speziell in kritischen Infrastrukturen.

Die Angreifer verfügen über leistungsfähige, flexibel einsetzbare Angriffsmittel und verbessern ihre Methoden kontinuierlich. Sie sind international organisiert und profitieren von der globalen Vernetzung sowie von den Möglichkeiten des Internets, Aktivitäten tarnen zu können. Ihre Spur ist oft schwer aufzunehmen und zu verfolgen, zumal die Ermittler rasch an nationale Grenzen stoßen. Die Offenheit und die Ausdehnung des Cyber-Raums erlaubt es den raffinierten Tätern auch, verschleierte Angriffe durchzuführen und verwundbare Opfersysteme als Werkzeug für Angriffe zu missbrauchen. Daher kann bei Angriffen häufig weder auf die Identität noch auf den Background der Angreifer geschlossen werden.

Mittelstand im Fokus der Angriffe ▸ Bei alledem sind sich Mittelständler oft genug gar nicht wirklich bewusst, wie wertvoll die Informationen, Konstruktionspläne oder Formeln sind, die sie in ihrem Firmennetzwerk speichern. Zugleich fehlt das Bewusstsein, die Sicherheit seiner IT stets auf dem letzten Stand zu halten. Beispielsweise nutzen viele KMU unverdrossen immer noch Windows XP. Das 17 Jahre alte Betriebssystem wird von seinem Hersteller Microsoft seit geraumer Zeit nicht mehr unterstützt. Es gibt keine Aktualisierungen mehr und keinen Support, falls heute noch Sicherheitslücken bekannt werden. Eine hat die Erpressungssoftware »Wannacry« jedenfalls 2017 genutzt.

Werden Altsysteme in der IT also zu lange genutzt, sind auch ungezielte Angriffe mit Schadsoftware oft erfolgreich, und zwar um so mehr, je weniger Vorkehrungen getroffen wurden und je weniger einschlägiges IT-Know-how gegeben ist. Auf der anderen Seite erhalten Hersteller aus Unternehmen keine ausreichenden Informationen in Bezug auf deren Anforderungen an die Sicherheit ihrer IT, da das Thema nicht im Fokus steht. Zudem haben die Hersteller selbst Probleme mit ihren Prozessen, um mit Schwachstellen in ihren Produkten umzugehen, diese zu kommunizieren und für eine zuverlässige Fehlerbeseitigung zu sorgen. Hinzu kommt, dass KMU anders als Konzerne in ihrer IT nicht nur personelle Engpässe haben, sondern meist auch knappe Budgets. Die IT-Abteilung soll aber dennoch die technische Infrastruktur mit allen gewünschten Funktionalitäten bereitstellen. Hinzu kommt stets auch der Faktor Mensch. Die fehlende Sensibilisierung im Hinblick auf IT-Sicherheitsrisiken und Einfallstore ist eine Hauptursache für Datendiebstahl und kompromittierte Systeme.

Sensibilisierung stärken ▸ Vor diesem Hintergrund schärft das BSI die Sensibilität für das brisante Thema als nationale Cyber-Sicherheitsbehörde vor allem auch in KMU. Immerhin schätzen rund 92 % der in unserer Studie befragten Unternehmen die Gefahren aus dem Cyber-Raum als kritisch für ihre Betriebsfähigkeit ein. Doch nur knapp 42 % gehen davon aus, dass der Betrieb im Fall eines Cyber-Angriffs durch Ersatzmaßnahmen aufrechterhalten werden könnte.

Dabei beurteilen KMU die Lage durchaus weniger kritisch als Konzerne. Während fast 74 % der Großunternehmen erwarten, dass die Gefahren im Cyber-Raum zunehmen, erwarten dies nur gut 62 % der KMU. Hier muss also noch mehr getan werden.

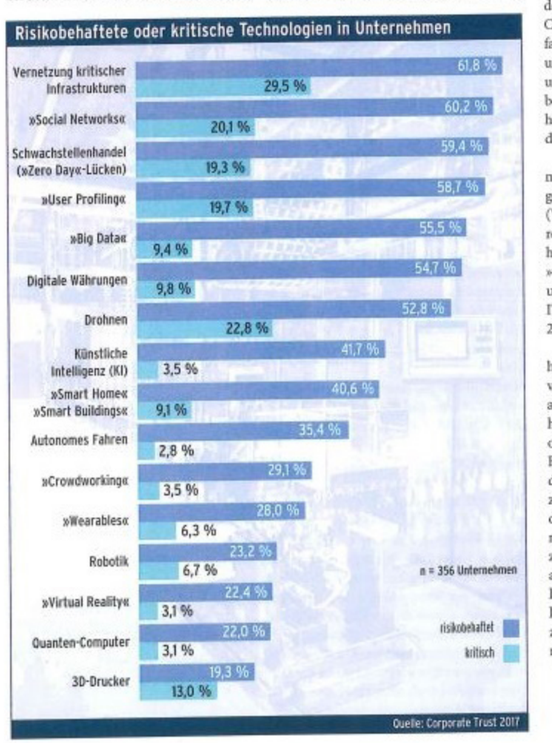
▸ *Fortsetzung auf Seite 14*

▸ *Fortsetzung von Seite 13*

Sowohl die technologische Entwicklung als auch die immer neuen Angriffswege und Angriffstechniken in der Cyber-Kriminalität und die rechtlichen Rahmenbedingungen führen dazu, dass Cyber Security heute eine zentrale Rolle in der Risikoabschätzung jedes mittelständischen Unternehmens spielen sollte. Die Sensibilisierung der Mitarbeiter, die Implementierung einer zeitgemäßen IT-Strategie und ein umsetzbarer Maßnahmenplan sind zentrale Erfolgsfaktoren einer zukunftsstabilen IT-Sicherheit.

Für die Realisierung dieser Aufgabe gibt es verschiedene Möglichkeiten, die sich in der Praxis miteinander kombinieren lassen:

- Die Definition zukunftsorientierter »Compliance«-Pflichten und deren Delegierung in die eigene »Compliance«-Organisation.
- Der Entwurf einer IT-Sicherheitsrichtlinie mit Vorgaben zur Verschlüsselung von Informationsflüssen laut IT-Grundschutz des BSI.
- Die Bestellung eines IT-Sicherheitsbeauftragten, wobei die Stelle je nach Betriebsgröße von einem Mitarbeiter, von mehreren oder in Teilzeit ausgefüllt werden kann.
- Die Anwendung von Frameworks (NIST-Rahmenwerk, ISO 27001/27002, COBIT).
- Die Beauftragung eines externen Datenschutzbeauftragten, um die datenschutzspezifischen Vorschriften zu überwachen.
- Die Einrichtung eines Managementsystems für die Informationssicherheit (ISMS).



Das BSI macht KMU diverse Angebote und es bietet Rat und praktische Handlungsempfehlungen an. Dazu zählt vor allem der modernisierte, praxisorientierte IT-Grundschutz, aber auch die Mitwirkung in der Allianz für Cyber-Sicherheit (www.allianz-fuer-cybersicherheit.de). KMU können sich dort in Erfahrungskreisen (ERFA-Kreise) vertrauensvoll austauschen, offen diskutieren und vom Erfahrungsschatz der anderen Teilnehmer profitieren. Die regelmäßig stattfindenden Cyber-Sicherheits-Tage befassen sich mit aktuellen Themen, die in Vorträgen vielseitig beleuchtet und in Kurzworkshops oder in Diskussionen vertieft werden.

Als Mitglied in der Allianz für Cyber-Sicherheit können Unternehmen auch auf den vom BSI und vom »ISACA Germany Chapter« e. V. gemeinsam entwickelten Leitfaden »Cyber-Sicherheits-Check« zugreifen, um ihren aktuellen Status zu bestimmen und aktuellen Bedrohungen aus dem Cyber-Raum wirksam zu begegnen. Darüber hinaus erhalten die Mitglieder Zugriff auf die »Cyber-Sicherheits-Warnungen« des BSI.

Des Weiteren stellt das BSI Informationen über Schwachstellen im externen Angebot des Warn- und Informationsdienstes (WID) vom CERT-Bund bereit. Für kleinere Unternehmen können auch die Hinweise hilfreich sein, die das BSI im Internet unter »www.bsi-fuer-buerger.de« anbietet. Zudem unterhält das BSI für Bürgeranfragen zur IT-Sicherheit eine Helpline (Telefon 0800/2741000 oder mail@bsi-fuer-buerger.de).

Welche Maßnahmen zu ergreifen sind, hängt vom jeweiligen Unternehmen sowie von der Gefährdungslage ab. Generell kann auch wichtig sein, das betriebliche Know-how vor der Entwendung durch Mitarbeiter oder Dritte zu schützen. In einem anderen Fall wird im Vordergrund stehen, die Produktionsanlagen oder die IT-Systeme jederzeit verfügbar zu halten. Außerdem kann es darum gehen, personenbezogene Daten gemäß den Datenschutz-Anforderungen aufzubewahren und zu sichern. In jedem Fall aber muss der Fokus im Mittelstand darauf liegen, unternehmensweit ein professionelles IT-Sicherheitsniveau zu erreichen. Ohne zeitgemäße Cyber-Sicherheit gibt es keinen nachhaltigen Erfolg der Digitalisierung. ■

Arne Schönbohm,
Präsident Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn