Sicherheit inmitten der Digitalisierung

Das Thema Cybersicherheit wird heftig diskutiert. In den vergangenen Monaten verursachte eine Welle von Hackerangriffen weltweit enorme Schäden. Steigen die Risiken? Die Dresdner Gesellschaft für IT Management unterstützt gemeinsam mit dem Leipziger Dienstleister Tilia Unternehmen und Kommunen in IT-Sicherheitsfragen. Die Fachleute geben einen Überblick zum aktuellen Stand der Dinge.

Ende 2016 diskutierten die Teilnehmer des 33. Chaos Communication Congress in Hamburg über Sicherheitsmängel in der IT und Cyberangriffe. Topthemen waren u. a. aufgedeckte Lücken bei Flugbuchungs- und Reiseportalen sowie Angriffe auf Banken, Banking Apps und digitale Währungen wie BitCoins. Im Fokus stand auch die Sicherheit der Energie-Infrastruktur. So hatten Hackerangriffe auf den Stromversorger Calpine zu mehreren Blackouts in Nordamerika geführt.

„In Deutschland gab es 2016 ebenfalls medienwirksame Cyberangriffe", sagt Dr. Ralf Cordes, Geschäftsführer der Gesellschaft für IT Management (ITM) in Dresden, ein zertifizierter IT-Sicherheitsberater, der Kommunen, Unternehmen und Privatpersonen unterstützt. „Im Herbst war bspw. die Telekom Ziel von Attacken auf DSL-Router und Cloud-Rechenzentren. Die Ausfälle betrafen tausende Haushalte sowie zahlreiche kleine und mittlere Unternehmen. Später erwies sich eine Sicherheitslücke im Wartungszugang der Router als Einfallstor für die Schadsoftware."

Etwa zur gleichen Zeit stahlen Datendiebe Millionen Kundendatensätze bei Google. Noch kritischer waren die Angriffe auf mehrere Krankenhäuser im Frühjahr. Hacker hatten die IT der Kliniken lahmgelegt, ohne die auch in OP-Sälen fast nichts mehr geht.

Woher kommen die Gefahren? Fachleute sehen vor allem drei wesentliche Quellen für Cyberangriffe. Ralf Cordes: "Hacker nutzen immer wieder Schwachstellen in handelsüblicher Standardsoftware – Betriebssysteme, Browser, Apps. Zudem verwenden die Kriminellen spezifische Angriffsmuster wie Botnetze, oder aber infiltrieren bestehende Kommunikationsbeziehungen, indem sie Router und Modems manipulieren. Und nicht zuletzt knacken Angreifer als sicher geglaubte Verschlüsselungen, bspw. das sogenannte SSL."

Und die Risiken steigen: In den vergangenen Jahren beobachteten Experten bei typischen Softwarekomponenten eine deutliche Zunahme der Schwachstellen. Seit 2014 betraf dieser Trend vor allem Adobe-Produkte, Apple IOS sowie einige Microsoft-Produkte. Im Fall von Apple und Adobe registrieren nationale Prüfstellen aktuell fast 1,5 Sicherheitslücken pro Tag – Produktfamilien, die fast jedes deutsche Unternehmen verwendet.

Angreifer nutzen diese Schwachstellen und entwickeln gezielt Schadsoftwaren. Die Anzahl bekannter Programme hat sich zwischen 2011 und 2016 auf über 550 Millionen verzehnfacht, wie das Bundesministerium des Inneren (BMI) mitteilt.

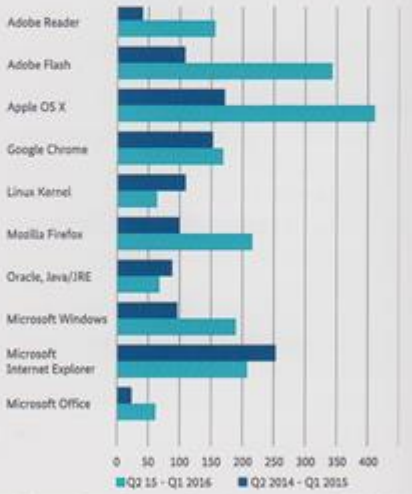
Die Entwicklung hat den Gesetzgeber aufgescheucht. So verabschiedete die Bundesregierung im Sommer 2015 das IT-Sicherheitsgesetz, das zahlreiche bestehende Gesetze erweitert: Kritische IT-Infrastrukturen (KRITIS) müssen nun ein besonderes IT-Sicherheitsmanagement aufweisen. Die Vorgabe betrifft u. a. Energieversorger, Banken, Hospitäler oder Telekommunikations- und Medienunternehmen. Voraussetzung für das IT-Sicherheitsmanagement ist ein intaktes Sicherheitssystem, z. B. nach dem ISO27001 Standard, eine mindestens zweijährige Überprüfung sowie konsequentes Melden von Angriffen und Sicherheitsvorfällen.

„Speziell für die Energieversorgung ist das IT-Sicherheitsgesetz ein Schritt in die richtige Richtung", meint Christophe Hug, Vorsitzender Geschäftsführer des Leipziger Dienstleister Tilia, der u. a. im Energiebereich tätig ist. „Die Maßnahmen sind grundsätzlich geeignet, Sicherheitsaspekte zu stärken und das Thema im Fokus zu halten. Die tatsächliche Wirkung der Vorgaben wird aber wahrscheinlich erst in ein paar Jahren abzuschätzen sein."

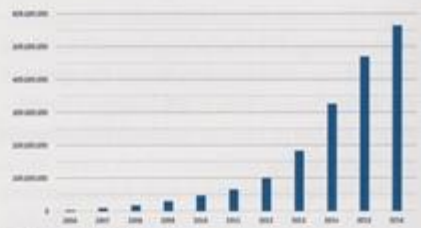
Das Gesetz definiert auch die Rolle des Bundesamtes für Informationssicherheit (BIS) neu. Bislang war das BIS vorrangig als Informationsgeber und Berater für IT-Probleme tätig – über das nationale Cyberabwehrzentrum sowie den CERT-Bund. Künftig wird das BIS zum nationalen Kontrollgremium für die Einhaltung des IT-Sicherheitsgesetzes.

In den kommenden Jahren sollen weitere nationale und europäische Gesetzesinitiativen in Kraft treten, z. B. 2018 die EU-Datenschutznovelle. Unberührt davon bleibt die Frage, wie Unternehmen und Privatpersonen sich gegen Cyberangriffe schützen können. „Ein technischer Basisschutz lässt sich schon mit überschaubaren Mitteln aufbauen", sagt ITM-Experte Ralf Cordes. „Er übersteigt allerdings die obligatorischen Mittel aus Virenschutz, Patchmanagement und Firewall, die heute jedes Unternehmen einsetzt."

Die Fachleute raten zu einer einfachen, aber detaillierte Analyse der kompletten digitalen Infrastruktur, um schützenswerte Daten und Systeme zu identifizieren. Anschließend



Schwachstellenaufkommen vo Q2/2014-Q1/2015 zu Q2/15-Q1/2016



Bekannte Schadprogramme
Quelle: AV-TEST GmbH

sind gezieltere Schutzmaßnahmen möglich. Unternehmen sollte zudem eine IT-Governance mit Vorschriften zur Nutzung der internen IT durch die Mitarbeiter einführen. Häufig müssen zuvor die Entscheidungsträger für das Thema sensibilisiert werden. Mangelnde IT-Compliance und IT-Governance können speziell für die Unternehmensleitung mit erheblichen Haftungs- und finanziellen Risiken verbunden sein.

Das Thema IT-Sicherheit wird weiter köcheln. Ralf Cordes: „Mit der fortschreitenden Digitalisierung werden auch Cyberangriffe allgegenwärtig bleiben. Unternehmen und Privatpersonen können die Attacken nicht verhindern, aber eben wirksam abwehren. Es gilt, in unruhigen Zeiten das richtige Fahrwasser zur IT-Cybersicherheit gemeinsam auszuloten."

Henning Groeger M.A.
Firmen: ITM Gesellschaft für IT-Management mbH www.itm-dl.de und Tilia GmbH www.tilia.info