Gefahren der Digitalisierung kennen und erkennen

Mithilfe manipulierter IP-Pakete lassen sich E-Mail-Accounts attackieren und Code aus der Ferne ausführen, ohne dass eine Aktion des Empfängers vonnöten ist – also ohne Öffnen der Mail oder Anzeige im Vorschaufenster. Was sich wie eine Szene aus einem schlechten Science-Fiction-Film anhört, ist eine kritische Sicherheitslücke im Mail-Programm Outlook, die Anfang 2023 behoben werden musste. Unter den Cybersicherheitswarnungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) findet sich auch ein VPN-System von Cisco, aus dem sensible Daten im Klartext ausgelesen werden konnten.

Diese Beispiele bekannter Anbieter zeigen, dass die Digitalisierung neben all ihren Vorteilen auch Gefahren mit sich bringt. Das BSI hat eine rund zehnprozentige Zunahme von Schwachstellen in Software-Produkten im Vergleich zum Vorjahr feststellen können. Ebenso ist im »Lagebericht der IT-Sicherheit in Deutschland 2022« von über 116 Millionen neuen Schadprogramm-Varianten die Rede. Einige davon können den Zugriff auf Daten oder Systeme einschränken oder sogar blockieren. 15 Millionen Meldungen zu Schadprogramm-Infektionen komplettieren das Lagebild.

Auch an der Sicherheitstechnik und der Gebäudeautomation gehen diese Entwicklungen nicht spurlos vorbei. Ansatzpunkte für mögliche Cyber-Attacken gibt es genug: Sicherheitstechnische Anlagen geben ihre Daten und Meldungen an Software-basierte Gefahrenmanagementsysteme weiter, Zutrittskontrolle wird beim Mobile Access vom Smartphone unterstützt, Videoüberwachungskameras senden Datenanalysen für zusätzliche Auswertungen, der Zugriff auf Brandmeldeanlagen erfolgt aus der Ferne und Fluchtwegsteuerungen reagieren dynamisch auf aktuelle Sensormeldungen. Auch ein fehlgeleiteter Code in IoT-Geräten (Internet of Things) oder die Manipulation von Datensätzen, mit denen Künstliche Intelligenz angelernt wird, sind Fehlerquellen, die moderne Datennetze schnell aus der geplanten Bahn werfen können.

Präventive IT-Sicherheitsmaßnahmen sind die Basis einer funktionsfähigen, digital vernetzten Gesellschaft, und unvorhergesehene (politische) Krisen können die Bedrohungslage rasch ändern. Staat, Verbände und Unternehmen sind daher in der Pflicht, hier Rahmenbedingungen zu setzen, diese technisch einzuhalten und die potenzielle Schwachstelle Mensch entsprechend zu schulen.

Im beruflichen Umgang mit High-End-Tools, vernetzter Technik und digitalen Infrastrukturen sollten trotz allem die Sicherheits-Basics keinesfalls vernachlässigt werden. So sind für IoT-Devices mit Bluetooth- oder WLAN-Schnittstellen, IP-Videoüberwachungskameras, Smartphones genauso wie für Router sichere Passwörter, Software-Updates, Firewalls und aktueller Virenschutz ein Muss.

Sicherheitsfachfirmen, die sich der Gefahren bewusst sind und sich proaktiv damit befassen, können inzwischen nach entsprechender Schulung und Prüfung Cybersecurity-Zertifikate verschiedener seriöser Anbieter erhalten. Damit zeigen sie auch nach außen hin ihren Kunden Kompetenz und dass sie Sicherheitsrisiken kennen, erkennen und beseitigen können.

Britta Kalscheuer, Redaktion »de«