DIGITALE UNTERNEHMENSWERTE SCHÜTZEN

Mitarbeiter und Unternehmensmarke bilden nach Innen und Außen zumeist die wichtigsten Stützen im Betrieb. Direkt danach folgen die Unternehmenswerte: Interne Produktinformationen, Konzeptionsdaten sowie Kundendaten bestimmen über zukünftigen und nachhaltigen Geschäftserfolg. Cyber-Kriminelle haben sich genau diese Daten als Fokus gesetzt

Der Autor Benjamin Richter ist Geschäftsführer der Procova UG. Er beschäftigt sich seit mehr als einem Jahrzehnt mit dem Thema Datenschutz, berät internationale Konzerne bei der IT-Security und bildet als zertifizierter Trainer u.a. Datenschutzbeauftragte aus.

Von Praktikern für Praktiker

Im Jahr 2019 wird Benjamin Richter regelmäßig aktuelle Datenschutz-Fragen aus der beruflichen Praxis aufgreifen und diese in Unternehmertum Südwestfalen beantworten. Stellen Sie Ihre Fragen gerne bereits heute per Mail an: *fragen@procova.de*

Aktuelle Zahlen geben Anlass zur Sorge! In den letzten 24 Monaten wurde fast jedes zweite deutsche Unternehmen (46 Prozent) Opfer einer Cyber-Attacke. Dazu hat sich das althergebrachte Bild des Hackers gewandelt. Sprach man früher von zurückgezogenen und spätpubertierenden Nerds, ist aus den damaligen „Script-Kiddies“ heute eine so komplexe Schattenwirtschaft geworden, das Fachleute bereits von „Cybercrime as a Service“ sprechen. Also der Möglichkeit gezielte Angriffe, wie auf einem digitalen Basar, an den Meistbietenden zu verkaufen. Gerade aufgrund dieser neuen Professionalisierung der Internetkriminalität sollte die Unternehmensführung handeln. Der Punkt „IT-Security“ und alles was damit zusammen hängt muss als einer der wichtigsten zukünftigen Management-Bereiche betrachtet werden. Aufgrund der schnell voranschreitenden Digitalisierung werden Services immer mehr automatisiert. Somit werden sich auch in Zukunft immer wieder neue Chancen für Cyber-Kriminelle bieten.

IT-SICHERHEIT UND DATENSCHUTZ SIND MANAGEMENTAUFGABEN

Natürlich setzt die IT-Sicherheit mehr voraus als reine technische Maßnahmen für das Unternehmen. Denn noch immer gilt der Mensch als größtes Sicherheitsrisiko. Über 90 Prozent der vermeintlichen IT-Angriffe werden, bewusst oder unbewusst, von den eigenen Mitarbeitern ermöglicht. Sei es der einfache Sachbearbeiter, der bei der Vielzahl von IT-Systemen im Eifer des Geschäfts die falsche E-Mail öffnet oder der Vertriebsmitarbeiter, der das Thema aufgrund des Umsatzdruckes nicht im Fokus sieht. Wer auch immer einen IT-Sicherheitsvorfall ausgelöst hat, es bleibt dabei: Der Unternehmer bzw. die Führungskraft trägt am Ende des Tages die Verantwortung. Hier spielt die Sensibilisierung der Beschäftigten eine Schlüsselrolle: Wissen und Bewusstsein lassen sich auch im 21. Jahrhundert nicht Outsourcen! Daher verlangt auch die neue Datenschutzgrundverordnung (DSGVO) in Art. 39 eine Sensibilisierung und Schulung, welche regelmäßig für alle Mitarbeiter stattfinden soll. Dabei geht es vor allem um alltägliche Dinge wie den Umgang mit Handakten, dem Verwenden von sicheren Passwörtern und das allgemeine Bewusstsein der Daten als Unternehmenswerte.