# 12. Wichtige Hinweise zur IT-Organisation im Errichter-Betrieb

## 12.1 Allgemeines

Ohne die entsprechenden IT-Systeme ist die Arbeit in den meisten Betrieben gar nicht mehr denkbar. Doch hier ist Vorsicht geboten: der sorglose Umgang mit der Technik kann großen Schaden anrichten, wenn Daten verloren oder gestohlen werden – oder rechtliche Vorgaben nicht eingehalten werden.

## 12.2 Die 10 wichtigsten Schritte

Im Folgenden wird eine Auswahl der 10 wichtigsten Schritte für mehr IT-Sicherheit in Ihrem Betrieb vorgestellt.

### 1. Musterleitlinie zur Informationssicherheit formulieren

Die wesentlichen Aussagen zur internen Sicherheitsstrategie sollten in einer Leitlinie zur Informationssicherheit zusammengefasst werden, um die Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter zu dokumentieren und Zuständigkeiten zu definieren (wer, wie wann, wo was). Mit der Sicherheitsleitlinie bekennt sich die Unternehmensleitung sichtbar zu ihrer Verantwortung für Informationssicherheit.

### 2. Inventur der IT-Systeme durchführen

Erst eine Inventur der vorhandenen Technik verschafft einen Überblick über alle stationären und mobilen Geräte (Laptops, Tablet-PCs und Smartphones etc.), aber auch Server und Router. Für sie ist jeweils zu dokumentieren, welchen Stand die vorhandene Software hat und wie der Zugriff geregelt ist. Zu beachten ist auch, mit welchen privaten Geräten die Mitarbeiter das Firmennetzwerk nutzen.

*Tipp*: Hilfreich kann als Basis ein LAN-Scan sein, der alle mit dem Netzwerk verbundenen Geräte anhand ihrer MAC- und IP-Adressen erfassen kann.

### 3. Datenzugriff regeln

Der Zugang zum IT-System, bspw. zum Serverraum, unbelegten Netzwerksteckdosen, dem internen WLAN oder freien USB-Ports, sollte klar geregelt und kommuniziert werden. Dies gilt selbstverständlich auch für alle anderen sensiblen internen Bereiche und bspw. den Zugriff auf personenbezogene Daten.

*Tipp:* Wichtige Daten werden zunehmend in der Cloud gespeichert. Die kostenlose Software Nextcloud ermöglicht das Speichern und Teilen von Daten auf dem eigenen Server. Dadurch behält der Nutzer die vollständige Kontrolle über seine Daten.

### 4. Firewall und Virenschutz aktuell halten

Firewall und Virenschutz sind bedeutende Bestandteile der IT-Sicherheit. Neue Updates sollten frühestmöglich installiert werden, um einen besseren Schutz gegen neue Bedrohungen zu gewährleisten. Für den Daten-Zugriff aus der Ferne, bspw. durch den Techniker, sollte ein VPN-Zugang eingerichtet werden.

*Tipp:* Praktikable Software-Lösungen sind z.B. hier zu finden

- *Physikalische Firewall von Securepoint: www.securepoint.de/produkte/utm-firewalls/black-dwarf-utm.html*
- *Virenschutz von Trendmicro: www.trendmicro.de/kleinunternehmen/virus-und-bedrohungsschutz*
- *Software zur physikalischen Netzwerksicherheit: www.barox.ch/produkte/ip-produkte/switche*

Unbekannte bzw. ungewünschte Dateien in Mails direkt sperren und das Ausführen von Programmen und das Öffnen von Dateien regeln. Sensible Daten bzw. ganze Laufwerke könnten ggf. zusätzlich durch Verschlüsselung geschützt werden.

### 5. Betriebssysteme und installierte Programme regelmäßig updaten

Auch die eingesetzten Betriebssysteme und installierten Programme sollten stets auf die neueste Version aktualisiert werden, da sonst Sicherheitslücken entstehen. Um zu verhindern, dass