Maßnahmenplan

Das Internet der Dinge und seine Sicherheit: Maßnahmen für unternehmerischen IT-Grundschutz

- ✓ Robusten Grundschutz einführen: Oft scheitert ein Basisschutz bereits am mangelnden Patch-Management und einer entsprechenden Mitarbeitersensibilisierung – dabei sind diese Maßnahmen bereits kostengünstig umzusetzen und decken den größten Teil der aktuellen Schwachstellen ab. Zu ihnen gehören: Sicherheitsupdates mit neuester Version für das Betriebssystem, ein gutes Virenschutzprogramm und eine Firewall, die das Netzwerk vor Angriffen schützt.
- ✓ Sicheres WLAN bedenken: Durch die Verbindung von Geräten innerhalb eines Netzwerkes ist vor allem ein sicheres WLAN wichtig. Damit sich das Internet der Dinge mittels WLAN unternehmensweit durchsetzen kann, müssen die Netzwerksicherheit einhundertprozentig gewährleistet und Zugriffskontrollen, wie u. a. Netzwerkschlüssel, gegeben sein.
- ✓ Vorhandene Sicherheits-Infrastruktur pflegen: Das meint nicht nur das Aktualisieren von Softwares und Sicherheitsmanagement-Anwendungen, sondern auch das Durchführen von Back-ups aller Unternehmensdaten. Dies ist vor allem auch in der Anwendung von IoT-Lösungen wichtig, um Prozesse, Störungen oder auch Schwankungen bei Produktionen nachvollziehen und auswerten zu können. Auch die Einführung und Aufrechterhaltung von Passwörtern für physische Geräte ist notwendig.
- ✓ Security-by-Design-Konzept erstellen: Je nach technischen Aspekten und unter Berücksichtigung des unternehmerischen Basisschutzes sollte ein individuell entwickeltes Sicherheits-Konzept für die IoT-Lösungen zusammengestellt werden. Dieses beinhaltet einen mit IT-Experten erarbeiteten Investitionsplan für nötige Sicherheits-Technologien und Maßnahmen.
- ✓ Verantwortlichkeit planen: Einzelnen Geschäftsbereichen sollte Verantwortung für die IT-Sicherheit übertragen werden. Das heißt, dass jeder Mitarbeiter und Verantwortliche im Umgang mit sensiblen Daten geschult werden sollte. Ebenso müssen Prozesse, Produkte und Dienste in enger Abstimmung mit der IT-Abteilung geplant werden, um mögliche Schwachstellen bereits in der Planung zu beheben. Auch für strategische Partner, die mittel- oder unmittelbar mit den digitalen Anwendungen zu tun haben, sollte eine formale Handlungsanleitung, ein sogenanntes Framework, in der Zusammenarbeit aufgestellt werden, um externe Sicherheitsrisiken von vornherein zu minimieren.