



IT-Sicherheit im Betrieb

Köln, 27. August 2021

Das Thema IT-Sicherheit wird mit zunehmender Digitalisierung immer komplexer, damit steigen die Anforderungen für Betriebe, aber auch für Privatpersonen. So wurde jüngst eine Sicherheitslücke bei Millionen Smart-Home-Geräten entdeckt. Sie betrifft die Software des Herstellers ThroughTek, die aktuell in 83 Millionen IoT-Geräten verbaut ist. „IoT“ steht für „Internet of Things“ (Internet der Dinge). Gemeint sind damit Geräte im oder am Haus, die sich mit dem Internet und untereinander vernetzen. Sie werden aus der Ferne gesteuert, zum Beispiel über Apps. Von der Schwachstelle sollen aktuell vor allem IP-Überwachungskameras und digitale Videorekorder betroffen sein. Nutzen Angreifer die Sicherheitslücke aus, können sie die Steuerung des Smart-Home-Geräts übernehmen und zum Beispiel die IP-Überwachungskamera aktivieren, das Haus überwachen oder die Kamera sogar ferngesteuert ausschalten. Die Schwachstelle wird daher als „kritisch“ eingestuft. Experten raten daher dringend, die Aktualisierung für die Software der Geräte zu überprüfen. Die Updates sollten direkt installiert werden, um vor Angriffen geschützt zu sein. Mehr Infos unter <https://www.sicher-im-netz.de>

Angriffe von innen

Betriebe sind mittlerweile sensibilisiert, wenn es um Cyberangriffe von außen geht und schützen ihre Daten. Doch oft sind sie weniger gut gegen Datendiebstahl aus den eigenen Reihen gewappnet. Neben sensiblen Daten, wie beispielsweise vertraulichen Dokumenten oder betrieblichen Informationen, können auch personenbezogene Daten entwendet werden. Je nachdem, worum es sich handelt, liegt dann nicht nur eine Datenschutzverletzung nach der DSGVO vor, sondern auch ein Verstoß, der zivil- oder strafrechtlich von Bedeutung sein kann.

Auch wenn man Angriffe von innen nicht hundertprozentig verhindern kann, erschweren vorsorgliche Maßnahmen und ein sicheres Datenschutzmanagement den Datenklau. Auch können klare Regelungen abschreckend wirken. Oft sind es innerbetriebliche Nachlässigkeiten, unklare Regelungen und fehlende Zuständigkeiten, die den Datendiebstahl erleichtern. So haben ehemalige Mitarbeitern:innen noch Zugang zu internen Informationen, weil beispielsweise Passwörter nicht geändert wurden. Mehr dazu: <https://bit.ly/DSIN-Blog>

IT-Sicherheit für den Mittelstand

Es gibt viele Möglichkeiten, die IT-Sicherheit in Unternehmen zu verbessern. Maßnahmen sind die Absicherung des Unternehmensnetzwerks, der Schutz zentraler Systeme wie das CRM-Tool zur Kundendatenpflege oder die Absicherung der E-Mail-Kommunikation. Die große Bedeutung der IT-Sicherheit kennen zwar viele Unternehmen, allerdings sind gerade kleine und mittelständische Unternehmen oft verunsichert, was zu tun ist, oder scheuen vor aufwendigen Beratungsprojekten zurück. Einen neuen Ansatz hat das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO gerade auch für Handwerksbetriebe entwickelt. Es bietet Unternehmen die Möglichkeit durch die Beantwortung weniger, nicht-technischer Fragen in kürzester Zeit eine schnelle Analyse durchzuführen und neben einem Aktionsplan auch direkt passende Handlungsempfehlungen zu erhalten. Somit wird Unternehmen eine schnelle und unkomplizierte Hilfestellung auf dem Weg zu mehr IT-Sicherheit geboten. Hier geht es zum Aktionsplan: <https://www.tisim.de>