**IT-Sicherheit:**

**Prinzip Hoffnung im Mittelstand**

**(November 2020) Den meisten kleinen und mittelständischen Unternehmen in Deutschland wissen, dass Cyberkriminalität eine Gefahr darstellt. Doch das Risiko, selbst einmal Opfer eines Cyberangriffs zu werden, verdrängen viele – es trifft ja immer nur die anderen.**

Betriebsunterbrechungen sind eine der häufigsten und in der Regel die teuersten Folgen von Cyberattacken – und können Unternehmen quer über alle Branchen ins Mark treffen. In der Produktion stehen die Bänder still, Händler können weder liefern noch Zahlungen abwickeln, Ärzte haben keinen Zugriff auf Patientendaten, Hoteliers keinen Überblick über Gäste und die noch freien Zimmer. Dieser Zustand ist in den wenigsten Fällen innerhalb kurzer Zeit behoben: Wie aus der diesjährigen Forsa-Umfrage zur Cybersicherheit des deutschen Mittelstandes hervorgeht, braucht die Hälfte der Betroffenen bis zu drei Tage, bis alle Systeme wieder laufen, bei 22 Prozent dauerte es sogar noch länger. Je größer die Unternehmen, desto größer ist auch die Abhängigkeit von funktionierenden IT-Systemen: Unter den Firmen mit 50 oder mehr Mitarbeitern wären 87 Prozent bei einem mehrtägigen Ausfall der IT voraussichtlich lahmgelegt.

Das Risikobewusstsein ist dabei durchaus vorhanden – immerhin 69 Prozent erkennen ein hohes Risiko durch Cyberkriminalität für die mittelständische Wirtschaft. Erstaunlicherweise bewerten aber die gleichen Befragten die Gefahr für sich selbst ganz anders: Hier sehen auf einmal nicht mehr 69 Prozent ein hohes Risiko, sondern nur noch 28 Prozent. Anders ausgedrückt: 41 Prozent meinen, es gibt ein hohes Risiko für andere, aber nicht für sie. Hiervon meinen 70 Prozent, dass ihre Daten für Hacker nicht interessant wären, 60 Prozent halten ihr Unternehmen für zu klein, um in den Fokus von Cyberkriminellen zu gelangen. 58 Prozent machen geltend, dass sie bisher schließlich noch nie Opfer einer erfolgreichen Cyberattacke waren – und ganze 81 Prozent halten ihr Unternehmen für umfassend geschützt

Gerade einmal etwas mehr als die Hälfte der befragten Unternehmen wird in den kommenden zwei Jahren in die Sicherheit ihrer Systeme investieren – obwohl die Investition von Zeit und Geld in vielen Fällen angebracht wäre. Vielerorts fehlt es schon an den notwendigen Strukturen: In 44 Prozent der Unternehmen ist niemand explizit für die IT-Sicherheit verantwortlich, 48 Prozent bereiten sich auf eine Cyberattacke auch nicht vor. Geradezu folgerichtig werden auch die Mitarbeiter nicht für die Gefahren sensibilisiert: Nicht mal in einem Drittel der befragten Unternehmen gibt es entsprechende Schulungen.

Dabei sind IT-Präventionsmaßnahmen nahezu immer die Voraussetzung, um sich überhaupt gegen die finanziellen Folgen von Cyber-Kriminalität versichern zu können, so die SIGNAL IDUNA. Der digitale Schutzschild der SIGNAL IDUNA für Gewerbekunden bietet ein wirksames Instrument gegen Cyber-Attacken. Er umfasst drei Verteidigungslinien: Vorkehrungen zur IT-Sicherheit, Präventionsmaßnahmen sowie einen leistungsstarken Cyber-Versicherungsschutz.