NEWS

Cyber-Attacken im Mittelstand nehmen zu

Studie zur Cyber Security unter Mitwirkung der Hochschule Aalen veröffentlicht

24.06.2020 | Die Digitalisierung verändert die Unternehmenspraxis auch im Mittelstand umfassend. Immer mehr Bereiche des Alltags sind digital vernetzt. Es entstehen neue digitale Produkte, Geschäftsmodelle und Ertragsmöglichkeiten für mittelständische Unternehmen. Einher damit geht aber auch eine kontinuierliche Zunahme des Bedrohungspotenzial durch Cyber-Attacken. In diesem Spannungsfeld der gestiegenen Chancen und zugenommen Risiken bewegt sich der Mittelstand. In der Deloitte--Studie „Cyber Security im Mittelstand“, der neuesten Publikation aus der Studienserie „Erfolgsfaktoren im Mittelstand“, wurden diese Herausforderungen nun einmal genauer untersucht. Dafür wurden 353 mittelständische Unternehmen in einer Online-Erhebung befragt und die gewonnenen Erkenntnisse um vertiefende Experteninterviews ergänzt.

Die Studie ergibt, dass sich viele mittelständische Unternehmen der Bedrohung durch Cyber-Angriffe nicht hinreichend bewusst sind und diese ggf. sogar unterschätzen. Attacken werden nicht schnell genug erkannt und es gibt nur in wenigen Unternehmen Notfall-Reaktionspläne. „Nachlässigkeit und Unkenntnis auf dem Gebiet der Cyber-Sicherheit können in zunehmendem Maße eine Gefahr für Leib und Leben darstellen“, so Prof. Roland Hellmann, IT-Sicherheitsexperte an der Hochschule Aalen im Studiengang Informatik.

„Einige aktuelle Beispiele von erfolgreichen Cyber-Angriffen auf Unternehmen und andere Organisationen haben gezeigt, dass Unternehmen im Notfall in der Lage sein müssen, alternative IT-Systeme einzusetzen, um den Betrieb aufrechtzuerhalten und Kunden weiter zu bedienen“, ergänzt Prof. Dr. habil. Patrick Ulrich, Sprecher des Direktoriums des Aalener Instituts für Unternehmensführung (AAUF). Täten sie dies nicht, entstünde ein irreparabler Schaden – sowohl im direkten wirtschaftlichen Sinne als auch für die Reputation des Unternehmens.

In der Studie wurden auch Verteidigungsmöglichkeiten wie z.B. organisatorische Sicherungsmaßnahmen und automatisierte Routinen untersucht. Die befragten Unternehmen sehen jedoch den größten Nachholbedarf im Bereich Aus- und Weiterbildung der eigenen Mitarbeiter. „Verbreitete Cyber-Angriffsvarianten wie CEO-Fraud (Business E-mail Compromise), Ransomware und Trojaner kommen häufig durch kompromittierte E-Mails ins System. Ein falscher Click kann genügen, um den Angreifern die Tür zu öffnen“, so Ulrich. Die Mails seien oft so gut gestaltet, dass kaum zwischen Original und Fälschung zu unterscheiden sei. Insofern müssten mittelständische Unternehmen neben den IT-seitigen und organisatorischen Rahmenbedingungen auch ein besonderes Augenmerk auf die Sensibilisierung der Mitarbeiter für Cyber-Risiken legen.

Die vollständige Studie kann direkt bei Deloitte eingesehen werden.