CYBER-GEFAHREN UND ONLINE-BETRUG – RISIKOMANAGEMENT UND VERSICHERBARKEIT

Dass mit steigender Technologisierung von Prozessen, Arbeitsabläufen und ganzen Produktionsstätten das Risiko von Hacker-Angriffen steigt, ist nicht neu. Aktuell ist die Gefahr aber überproportional groß. Der Grund: Während der Corona-Krise rüsteten viele Unternehmen in kürzester Zeit auf Homeoffice und Remote-Zugänge um – oft zulasten der Sicherheit. Risikomanager Markus Oswald weiß, wo Gefahren lauern und was schützt.

Cyber-Angriffe können jedes Unternehmen treffen. Gerade jetzt haben Hacker leichtes Spiel, Firmen zu schaden und Gewinne zu erpressen. Denn: „Eine große Schwachstelle ist Homeoffice. Die privaten Internetzugänge von Mitarbeitenden sind häufig unzureichend geschützt und somit leichter hackbar als ein unternehmensinternes Firmennetzwerk", informiert Markus Oswald. Das Problem: Durch die schnelle Umstellung auf das Arbeiten von zuhause, sind die Mitarbeiterinnen und Mitarbeiter oftmals nicht genügend geschult, organisatorische Abläufe wurden nicht ausreichend vorbereitet und definiert. Viele Dienstleistungsfirmen sind derzeit mit dem großen Andrang überfordert. Der erfahrene IT-Risikomanager von risk on mind ® zeigt auf, dass ein Hacker oder eine Hacker-Gruppe nur wenige Stunden brauchen, um sich die Tür zu einem Betrieb – zum Beispiel durch den privaten Internetzugang eines Mitarbeitenden – zu öffnen. Dann komme es darauf an, wie gut die zweite und dritte Sicherheitsschicht im Unternehmen wirken. Der Schaden reicht von Viren am Laptop bis hin zur Stilllegung der gesamten Informationstechnologie und Maschinensteuerung. „Hat ein Hacker Zugang zum Firmennetzwerk, kann er sich häufig weitere Zugangsrechte verschaffen. Ist dies geschehen, kann er Schadenssoftware einschleusen, Daten verschlüsseln, Dienste ausschalten und gegebenenfalls die Produktion stilllegen und damit Geld erpressen. Ist in einer Firma die Wertschöpfungskette unterbrochen, braucht es viel Geld und Zeit, den Schaden zu beheben. Meist wird dadurch auch der Ruf des Unternehmens stark geschädigt", warnt der Cyber-Risiko-Experte.

Risiken kennen und gegensteuern

Das Um und Auf ist, Risiken im Vorfeld zu identifizieren, sie zu bewerten und ihnen zielgerichtet entgegenzusteuern. „Mit einem systematischen Risikomanagement können wir Gefahrenpotenziale in der IT- und OT-Struktur ausschalten oder minimieren und die reibungslose Umsetzung der erforderlichen Sicherheitsmaßnahmen steuern. Das schützt Daten, senkt die Wahrscheinlichkeit von Cyber-Crime-Vorfällen und reduziert das Ausmaß von Schäden, wenn doch etwas passiert", rät Markus Oswald: „Ein Restanteil der Cyber-Gefahren kann auch durch Abschluss einer Cyber-Versicherung abgesichert werden."

Markus Oswald, Cyber-Risiko-Manager

„Private Mitarbeiter-Laptops sind die Eintrittskarte für Hacker, um mit wenig Aufwand großen Schaden anzurichten."